Σχολή Θετικών Επιστημών και Τεχνολογίας

Διαχείριση και Τεχνολογία Ποιότητας

Διπλωματική Εργασία

Η προσέγγιση της διακινδύνευσης στο πρότυπο ISO 27001:2022. Μελέτη περίπτωσης διαχείρισης της διακινδύνευσης στη διαχείριση δεδομένων ενός Πανεπιστημιακού Ιδρύματος.

Ηλίας Κ. Σταυρόπουλος

Επιβλέπων καθηγητής: Γεώργιος Μπαλωμένος

Πάτρα,Μάιος 2024

Η προσέγγιση της διακινδύνευσης στο πρότυπο ISO 27001:2022. Μελέτη περίπτωσης διαχείρισης της διακινδύνευσης στη διαχείριση δεδομένων ενός Πανεπιστημιακού Ιδρύματος.

Ηλίας Κ. Σταυρόπουλος

Επιτροπή Επίβλεψης Διπλωματικής Εργασίας

Επιβλέπων Καθηγητής:

Δρ. Γεώργιος Μπαλωμένος

Αν. Καθηγητής Σχολής Θετικών Επιστημών και Τεχνολογίας

Ελληνικό Ανοικτό Πανεπιστήμιο

Συν-Επιβλέπων Καθηγητής:

Δρ. Γεώργιος Χατζηγεωργίου

Καθηγητής Σχολής Θετικών Επιστημών και Τεχνολογίας

Ελληνικό Ανοικτό Πανεπιστήμιο

Πάτρα, Μάιος 2024

Ευχαριστίες

Θερμές ευχαριστίες στον επιβλέποντα καθηγητή μου Γεώργιο Μπαλωμένο, όπου χωρίς την κατανόηση, την ενθάρρυνση και την υποστήριξη του δεν θα είχε ολοκληρωθεί η εκπόνηση της παρούσας διπλωματικής εργασίας. Ευχαριστίες και στον συν-επιβλέποντα καθηγητή Γεώργιο Χατζηγεωργίου για την υποστήριξη. Εύχομαι την συνέχιση της συνεργασία μας σε διάφορα επίπεδα. Ένα μεγάλο ευχαριστώ και στον Κοσμά Πιπύρο, για την σύντομη αλλά ουσιαστική επικοινωνία μας και την διάθεση χρήσιμων δημοσιεύσεων και πηγών πληροφόρησης.

Η ολοκλήρωση της εκπόνησης της παρούσας διπλωματικής εργασίας έρχεται να κλείσει τον κύκλο των μεταπτυχιακών σπουδών στο πρόγραμμα της Διασφάλισης και Τεχνολογίας Ποιότητας του Ελληνικού Ανοικτού Πανεπιστημίου. Ένας κύκλος που άνοιξε πριν αρκετά χρόνια από προσωπικό ενδιαφέρον και ευχαρίστηση για ζητήματα και τεχνικές που αφορούσαν τη διασφάλιση της ποιότητας και έκλεισε με προσανατολισμό την ασφάλεια των πληροφοριών.

Ένας κύκλος που δεν θα είχε ολοκληρωθεί χωρίς την καθημερινή συμπαράσταση της συζύγου μου Βασιλικής, και της παρότρυνσης της να συνεχίζω παρά τις υποχρεώσεις και τις δυσκολίες που συναντούσαμε, την κόρη μου Θεοδώρα που μου έδινε χαρά και ενέργεια, και την κόρη μου Δέσποινα που με γέμιζε αγάπη και ανέδειξε αόρατες πτυχές μου ως γονέας και ως άνθρωπος. Σε αυτές αφιερώνεται.

… στην Βασιλική, στην Θεοδώρα, στην Δέσποινα

Περίληψη

Η συγκεκριμένη ΜΔΕ αφορά την προσέγγιση της έννοιας της διακινδύνευσης όπως αυτή ορίζεται στο πρότυπο ISO/IEC 27001:2022. Το πρότυπο ISO/IEC 27001:2022 αποτελεί το πιο αναγνωρισμένο διεθνές πρότυπο Ασφάλειας Πληροφοριών, το οποίο παρέχει σε επιχειρήσεις και οργανισμούς, ανεξαρτήτου μεγέθους, ένα πλαίσιο διαχείρισης και καθορισμού των απαιτήσεων για την εφαρμογή και συνεχή βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και διαθεσιμότητας των πληροφοριών τους. Η εκτίμηση της διακινδύνευσης αποτελεί εδάφιο του προτύπου, με συγκεκριμένα σημεία στα οποία μια επιχείρηση ή οργανισμός οφείλει να συμμορφώνεται.

Σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων, για κάθε είδος επεξεργασία που ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας υποχρεούται στην εκτίμηση του αντικτύπου των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία των δεδομένων προσωπικού χαρακτήρα. Στην παρούσα ΜΔΕ περιγράφονται τεχνικές εκτίμησης της διακινδύνευσης (η εκτίμηση του αντικτύπου είναι μία από αυτές). Στη συνέχεια, δίνεται μια μελέτη περίπτωσης όπου τεχνικές εκτίμησης της διακινδύνευσης εφαρμόζονται για την διαχείριση της διακινδύνευσης σε ένα πληροφοριακό σύστημα με εκπαιδευτικά δεδομένα ενός πανεπιστημιακού ιδρύματος, μέρος των οποίων χαρακτηρίζονται ως δεδομένα προσωπικού χαρακτήρα.

Η ΜΔΕ δομείται ως εξής: αρχικά παρουσιάζεται η έννοια της διακινδύνευσης όπως αυτή ορίζεται στο πρότυπο ISO/IEC 27001:2022. Στη συνέχεια περιγράφεται η διαδικασία της εκτίμησης της διακινδύνευσης σύμφωνα με τα πρότυπα που υποστηρίζουν το ISO/IEC 27001:2022 (το πρότυπο ISO/IEC 27005:2018 που παρέχει οδηγίες για την διαχείριση της διακινδύνευσης, το γενικό διεθνές πρότυπο ISO/IEC 31000:2018 που περιλαμβάνει αρχές και οδηγίες για τη διαχείριση της διακινδύνευσης καθώς και το γενικό διεθνές πρότυπο ISO/IEC 31010:2019 που περιλαμβάνει τεχνικές εκτίμησης της διακινδύνευσης). Η ΜΔΕ επικεντρώνεται στην παρουσίαση των τεχνικών για τα διάφορα στάδια εκτίμησης της διακινδύνευσης σύμφωνα με το διεθνές πρότυπο ISO/IEC 31010:2019 καθώς βρίσκουν

γενική εφαρμογή για την εκτίμηση της διακινδύνευσης. Στη συνέχεια, γίνεται αναφορά στον Γενικό Κανονισμό Προστασίας Δεδομένων και στα άρθρα που αφορούν τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και την υποχρέωση για εκπόνηση μελέτης εκτίμησης αντικτύπου προστασίας δεδομένων. Τέλος, δίνεται ως περίπτωση μελέτης η εκπόνηση μελέτης εκτίμησης αντικτύπου προσωπικών δεδομένων στην επεξεργασία εκπαιδευτικών δεδομένων που αφορούν χαρακτηριστικά των υποκειμένων στο εικονικό περιβάλλον μάθησης που χρησιμοποιεί ένα πανεπιστημιακό ίδρυμα για την παροχή εκπαίδευσης από απόσταση.

Λέξεις – Κλειδιά

Διαχείριση Διακινδύνευσης, Εκπαιδευτικά Δεδομένα, ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 31000, ISO/IEC 31010, ΓΚΠΔ.

The risk approach in ISO 27001:2022 standard. A case study of risk management in data management of a University Institution

Elias C. Stavropoulos

Abstract

This master thesis deals with the concept of risk as defined in the ISO/IEC 27001:2022 standard. The ISO/IEC 27001:2022 standard is the most recognized international Information Security standard, which provides businesses and organizations, regardless of size, with a framework for managing and defining the requirements for the implementation and continuous improvement of an Information Security Management System, ensuring the confidentiality, integrity and availability of their information. The risk assessment is a subsection of the standard, with specific points that a business or organization must comply with.

According to the General Data Protection Regulation, for any type of data processing that may pose a high risk to the rights and freedoms of natural persons, the data controller is required to assess the impact of the planned processing operations on the protection of personal data. This thesis describes risk assessment techniques (data processing impact assessment is one of them). Then, a case study is given where risk assessment techniques are applied for risk management in an information system with educational data of a university institution, part of which is characterized as personal data.

The thesis is structured as follows: initially the concept of risk as defined in the ISO/IEC 27001:2022 standard is presented. The process of risk assessment is then described according to the standards that support ISO/IEC 27001:2022 (the ISO/IEC 27005:2018 standard that provides guidelines for risk management, the general international standard ISO/IEC 31000:2018 which includes principles and guidelines for risk management as well as the general international standard ISO/IEC 31010:2019 which includes risk assessment techniques). The thesis focuses on presenting the techniques for the various stages of risk

assessment according to the international standard ISO/IEC 31010:2019 as they are applicable in general. Then, a reference is made to the General Data Protection Regulation and the articles concerning the rights and freedoms of natural persons and the obligation to prepare a data protection impact assessment study. Finally, as a case study, a data processing impact assessment study is conducted for processing educational data of the subjects in the virtual learning environment utilized by a university institution to provide distance education to tis students.

Keywords

Risk Management, Educational Data, ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 31000, ISO/IEC 31010, GDPR.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Ορολογία

Για την ορολογία χρησιμοποιήθηκε ο οδηγός ISO Guide 73:2009 [1] που παρέχει ένα βασικό λεξιλόγιο για την κατανόηση εννοιών και όρων της διαχείρισης της διακινδύνευσης. Ο οδηγός έχει σκοπό να προωθήσει μια συνεκτική προσέγγιση στην περιγραφή των ενεργειών για τη διαχείρισης της διακινδύνευσης και τη χρήση της ορολογίας διακινδύνευσης, καθώς και να συμβάλει στην κοινή κατανόηση της διαχείρισης διακινδύνευσης μεταξύ των οργανισμών που αναπτύσσουν πρότυπα.

Η ορολογία αυτή υιοθετείται και στο πρότυπο ISO/IEC 27000:2018 [2] το οποίο παρέχει μια επισκόπηση των Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών καθώς επίσης τους όρους και τους ορισμούς που χρησιμοποιούνται στην οικογένεια προτύπων ISO/IEC 270xx που αφορούν τα Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών.

Συντομογραφίες & Ακρωνύμια

ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
ΔΠΧ	Δεδομένα Προσωπικού Χαρακτήρα
ΕΑΠΔ	Εκτίμηση Αντικτύπου Προστασίας Δεδομένων
ΕΣΥΔ	Εθνικό Σύστημα Διαπίστευσης
ΣΔΑΠ	Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
ΥΠΔ	Υπεύθυνος Προστασίας Δεδομένων
CNIL	Commission Nationale de l'Informatique et des Libertés
CNSS	Committee on National Security Systems
DPIA	Data Protection Impact Assessment
GDPR	General Data Protection Regulation
ENISA	European Union Agency for Network and Information Security
ICO	Information Commissioner's Office
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
LMS	Learning Management System
PIA	Privacy Impact Assessment
VLE	Virtual Learning Environment

Ελληνοαγγλικό γλωσσάριο

Αβεβαιότητα	Uncertainty
Αγαθό	Asset
Ακεραιότητα	Integrity
Αναγνώριση Διακινδύνευσης	Risk Identification
Ανάλυση Διακινδύνευσης	Risk Analysis
Αντιμετώπιση Διακινδύνευσης	Risk Treatment
Απειλή	Threat
Αποδοχή Διακινδύνευσης	Risk Acceptance
Αποτίμηση Διακινδύνευσης	Risk Evaluation
Ασφάλεια Πληροφοριών	Information Security
Αυθεντικότητα	Authenticity
Δεδομένα Προσωπικού Χαρακτήρα	Personal Data
Διαθεσιμότητα	Availability
Διακινδύνευση	Risk
Διακυβέρνηση	Governance
Διαμεσολαβητής	Facilitator
Διαπίστευση	Accreditation
Διαχείριση Διακινδύνευσης	Risk Management
Διεθνής Επιτροπή Ηλεκτροτεχνίας	International Electrotechnical Commission
Διεθνής Οργανισμός Τυποποίησης	International Organization for Standardization
Διοίκηση	Management
Δομημένη συνέντευξη	Structured interview
Εκτελών την επεξεργασία	Processor
Εκτίμηση Αντικτύπου	Impact Assessment
Εκτίμηση Διακινδύνευσης	Risk Assessment
Εμπιστευτικότητα	Confidentiality
Επεξεργασία δεδομένων	Data processing
Επικινδυνότητα	Risk
Εργαστήριο	Workshop
Έρευνα	Survey
Ευκαιρία	Opportunity
Ευπάθεια	Vulnerability

Ημι-δομημένη συνέντευξη	Semi-structured interview
Θεωρία Παιγνίων	Game Theory
Καταιγισμός ιδεών	Brainstorming
Κατηγοριοποίηση	Classification
Κατοχή	Possession
Κίνδυνος	Hazard
Λίστα ελέγχου	Checklist
Οδηγός Διακινδύνευσης	Risk driver
Παραβίαση Δεδομένων	Data Breach
Περιβάλλον Εικονικής Μάθησης	Virtual Learning Environment
Πηγή Επικινδυνότητας	Risk Source
Πιθανότητα	Likelihood, Probability
Πίνακας επικινδυνότητας	Risk Matrix
Πληροφορία	Information
Πληροφοριακό Σύστημα	Information System
Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών	Information Security Management System
Σύστημα Διαχείρισης Μάθησης	Learning Management System
Ταξινομία	Taxonomy
Τρωτότητα	Vulnerability
Υπεύθυνος επεξεργασίας	Controller
Υπολογιστικό νέφος	Cloud
Χρηστικότητα	Utility

Αγγλοελληνικό γλωσσάριο

Accreditation	Διαπίστευση
Asset	Αγαθό
Authenticity	Αυθεντικότητα
Availability	Διαθεσιμότητα
Brainstorming	Καταιγισμός ιδεών
Checklist	Λίστα ελέγχου
Classification	Κατηγοριοποίηση
Cloud	Υπολογιστικό νέφος
Confidentiality	Εμπιστευτικότητα
Controller	Υπεύθυνος επεξεργασίας
Data Breach	Παραβίαση Δεδομένων
Data Processing	Επεξεργασία δεδομένων
Facilitator	Διαμεσολαβητής
Game Theory	Θεωρία Παιγνίων
Governance	Διακυβέρνηση
Hazard	Κίνδυνος
Impact Assessment	Εκτίμηση Αντικτύπου
Information	Πληροφορία
Information Security	Ασφάλεια Πληροφοριών
Information Security Management System	Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
Information System	Πληροφοριακό Σύστημα
Integrity	Ακεραιότητα
International Electrotechnical Commission	Διεθνής Επιτροπή Ηλεκτροτεχνίας
International Organization for Standardization	Διεθνής Οργανισμός Τυποποίησης
Learning Management System	Σύστημα Διαχείρισης Μάθησης
Likelihood	Πιθανότητα
Management	Διοίκηση
Opportunity	Ευκαιρία
Personal Data	Δεδομένα Προσωπικού Χαρακτήρα
Probability	Πιθανότητα
Possession	Κατοχή
Processor	Εκτελών την επεξεργασία

Risk	Διακινδύνευση, Επικινδυνότητα
Risk Acceptance	Αποδοχή Διακινδύνευσης
Risk Analysis	Ανάλυση Διακινδύνευσης
Risk Assessment	Εκτίμηση Διακινδύνευσης
Risk Driver	Οδηγός Διακινδύνευσης
Risk Evaluation	Αποτίμηση Διακινδύνευσης
Risk Identification	Αναγνώριση Διακινδύνευσης
Risk Management	Διαχείριση Διακινδύνευσης
Risk Matrix	Πίνακας Επικινδυνότητας
Risk Source	Πηγή Επικινδυνότητας
Risk Treatment	Αντιμετώπιση Διακινδύνευσης
Semi-structured interview	Ημι-δομημένη συνέντευξη
Structured interview	Δομημένη συνέντευξη
Survey	Έρευνα
Taxonomy	Ταξινομία
Thread	Απειλή
Uncertainty	Αβεβαιότητα
Utility	Χρηστικότητα
Virtual Learning Environment	Περιβάλλον Εικονικής Μάθησης
Vulnerability	Ευπάθεια, Τρωτότητα
Workshop	Εργαστήριο

1. Εισαγωγή

Ζούμε σε μια εποχή όπου εκατομμύρια χρήστες διαμοιράζονται δεδομένα καθημερινά μέσω συσκευών και εφαρμογών πραγματικού χρόνου, εμπορικών και τραπεζικών συναλλαγών, κοινωνικών δικτύων, ιατρικών πράξεων, εκπαιδευτικών και ψυχαγωγικών δραστηριοτήτων κ.α. Η τεράστια πρόοδος στην τεχνολογία δίνει τη δυνατότητα συλλογής και αποθήκευσης, με πολύ χαμηλό κόστος, μεγάλου όγκου δεδομένων που προέρχονται από διαφορετικές πηγές και σε διάφορες μορφές. Δημιουργούνται έτσι μεγάλα κέντρα αποθήκευσης δεδομένων που διασυνδέονται μεταξύ τους για να δημιουργηθεί μια τεράστια δεξαμενή δεδομένων που στο χώρο της Πληροφορικής καλείται «μεγάλα δεδομένα». Τα δεδομένα αυτά μπορούν υπόκεινται σε επεξεργασία μέσω ισχυρών τεχνικών εξόρυξης δεδομένων και εξελιγμένων διαδικασιών ανάλυσης δεδομένων προκειμένου να εξαχθούν συμπεράσματα για ομάδες ατόμων ή και αναδειχθούν χαρακτηριστικά για τα υποκείμενα των δεδομένων.

Τα δεδομένα μπορούν να χρησιμοποιούνται από επιχειρήσεις και οργανισμούς για διάφορους σκοπούς, όπως επικοινωνία, μάρκετινγκ, ανάπτυξη προϊόντων. Η ανάλυση μεγάλων δεδομένων βοηθά τις επιχειρήσεις και τους οργανισμούς να λειτουργούν με πιο έξυπνο και αποτελεσματικό τρόπο, διότι προσφέρει αξιόπιστα αποτελέσματα σε πραγματικά προβλήματα, βρίσκοντας τάσεις, πρότυπα, συσχετίσεις και πολλά άλλα χαρακτηριστικά που υπάρχουν μεταξύ των δεδομένων. Το ίδιο ισχύει και για τον τομέα της υγείας, των κοινωνικών υπηρεσιών και φυσικά της εκπαίδευσης. Συνδυάζοντας πληροφορίες που βασίζονται στα δεδομένα των μαθητών, των ασθενών και, γενικά, των υποκειμένων των δεδομένων, και με την εφαρμογή προηγμένων υπολογιστικών εργαλείων μαζί με μεγάλες αναλυτικές δεξιότητες, η επιστήμη των δεδομένων μπορεί να παρέχει προγνωστικά μοντέλα και έτσι να οδηγήσει σε καλύτερες και ταχύτερες αποφάσεις (δείτε ενδεικτικά στο [3]).

Υπάρχουν ωστόσο ζητήματα που θα πρέπει να απασχολούν τις επιχειρήσεις και τους οργανισμούς που επεξεργάζονται δεδομένα υποκειμένων. Ένα τέτοιο ζήτημα είναι η ασφάλεια των δεδομένων και ευρύτερα των πληροφοριακών συστημάτων του

οργανισμού. Αυτό που ονομάζεται «ασφάλεια πληροφοριών» και αφορά την προστασία των πληροφοριακών συστημάτων που διαχειρίζονται τις πληροφορίες εντός του οργανισμού από ευπάθειες, απειλές, εισβολείς, κακόβουλο λογισμικό, εξαπάτηση των χρηστών κ.α. Η ασφάλεια τω πληροφοριών στοχεύει στην προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων ενώ για τη διασφάλιση αυτής οι οργανισμοί καλούνται υιοθετούν ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών και να συμμορφώνονται με το διεθνές πρότυπο ISO/IEC 27001 το οποίο καθορίζει τις απαιτήσεις για την καθιέρωση, υλοποίηση, συντήρηση και διαρκή βελτίωση ενός ΣΔΑΠ και προσφέρει ένα ολοκληρωμένο πλαίσιο διαχείρισης και καθορισμού των απαιτήσεων για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών τους. Το πρότυπο ISO/IEC 27001 επιβάλει μια σειρά σταδίων για την εκτίμηση της επικινδυνότητας στην επεξεργασία της πληροφορίας, καθώς και ελέγχων και μέτρων για την αντιμετώπιση του κινδύνου.

Η διατήρηση της ιδιωτικότητας των δεδομένων είναι ένα άλλο σοβαρό ζήτημα που οφείλει να απασχολεί οργανισμούς και επιχειρήσεις. Η ανάλυση μεγάλων δεδομένων θεωρείται ως ένας τρόπος κεφαλαιοποίησης των εμπορικών δραστηριοτήτων και των μεταποιητικών, λιανικών και χρηματοοικονομικών υπηρεσιών κ.λ.π., επειδή προσφέρει αξιόπιστες πληροφορίες για τα πραγματικά προβλήματα με την εύρεση τάσεων, προτύπων, συσχετίσεων και άλλων χαρακτηριστικών που υπάρχουν μεταξύ των δεδομένων. Επίσης τα δεδομένα και ιδιαίτερα τα προσωπικά δεδομένα παρέχουν πληροφορίες και γεγονότα που αποτελούν ισχυρή πηγή γνώσης για πολλές πτυχές της κοινωνικής και οικονομικής μας ζωής, ωστόσο δεν μπορεί να αγνοηθεί το απόρρητο των υποκειμένων των δεδομένων. Οι σύγχρονες κοινωνίες πρέπει να εφαρμόζουν αυστηρούς κανονισμούς και νόμους για την προστασία των υποκειμένων και των δικαιωμάτων τους. Για το σκοπό αυτό, τον Μάιο του 2018, η Ευρωπαϊκή Ένωση έφερε σε ισχύ τον Γενικό Κανονισμό για την Προστασία Δεδομένων (General Data Protection Regulation), ο οποίος είναι μακράν το πληρέστερο κανονιστικό πλαίσιο που ισχύει για όλους τους πολίτες της ΕΕ σε σχέση με την προστασία δεδομένων. Ο ΓΚΠΔ εισήγαγε κανονιστικές αρχές για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων

προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, δίνει έμφαση στο «δικαίωμα στην ιδιωτική ζωή» και επιβάλλει την έννοια της συναίνεσης. Επιπλέον, επιβάλει την εφαρμογή διαδικασιών για την ασφάλεια των δεδομένων και την εκτίμηση του αντικτύπου σχετικά με την προστασία των δεδομένων (Data Protection Impact Assessment, DPIA).

1.1. Δομή και περιεχόμενο εργασίας

Η παρούσα εργασία εισάγει τον αναγνώστη στις περιοχές που αναφέρθηκαν παραπάνω, περιγράφοντας μοντέλα, διαδικασίες και τεχνικές που χρησιμοποιούνται για την ασφάλεια της πληροφορίας και τη διαχείριση της επικινδυνότητας και κλείνει με την εκτίμηση του αντικτύπου στην επεξεργασία εκπαιδευτικών δεδομένων. Συγκεκριμένα, η εργασία δομείται ως εξής:

Στο Κεφάλαιο 2 γίνεται μια σύντομη αναφορά στα μοντέλα ασφάλειας πληροφοριών, στις απαιτήσεις του ΓΚΠΔ, στα Συστήματα Διαχείρισης Ασφάλειας Πληροφορικών και στο διεθνές πρότυπο ISO/IEC 27701 που αφορά στην ασφάλεια της πληροφορίας.

Στο Κεφάλαιο 3 παρουσιάζεται και περιγράφεται η διαδικασία της διαχείρισης της διακινδύνευσης, σύμφωνα με το γενικό πρότυπο ISO 31000 καθώς και με το ISO/IEC 27005. Το Κεφάλαιο 4 επικεντρώνεται στα στάδια της εκτίμησης της διακινδύνευσης (αναγνώριση, ανάλυση και αποτίμηση) ενώ στο κεφάλαιο 5 παρουσιάζονται επιγραμματικά οι τεχνικές εκτίμησης της διακινδύνευσης για κάθε στάδιο αυτής.

Στο Κεφάλαιο 6 γίνεται αναφορά στις κανονιστικές αρχές του ΓΚΠΔ και στην υλοποίηση της διαδικασίας ασφάλειας της επεξεργασίας των δεδομένων μέσω της μελέτης εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

Τέλος, στο κεφάλαιο 7, ως μελέτη περίπτωσης, παρουσιάζεται η μελέτη εκτίμησης αντικτύπου για την επεξεργασία εκπαιδευτικών δεδομένων ενός πανεπιστημιακού ιδρύματος που παρέχει εκπαίδευση από απόσταση.

Η εργασία ολοκληρώνεται με κάποια συμπεράσματα και προτάσεις για μελλοντικές προσεγγίσεις.

2. Ασφάλεια πληροφορίας και προστασία δεδομένων

2.1. Ασφάλεια πληροφοριών & πληροφοριακών συστημάτων

Η Ασφάλεια Πληροφοριών (Information Security, InfoSec) αναφέρεται στις διαδικασίες και τις μεθοδολογίες που σχεδιάζονται και εφαρμόζονται για την προστασία έντυπων, ηλεκτρονικών ή οποιασδήποτε άλλης μορφής εμπιστευτικών, ιδιωτικών και ευαίσθητων πληροφοριών ή δεδομένων από μη εξουσιοδοτημένη πρόσβαση, χρήση, κακή χρήση, αποκάλυψη, καταστροφή, τροποποίηση ή διακοπή. Περιλαμβάνει την πρόληψη για τη μη εξουσιοδοτημένη πρόσβαση ή χρήση πληροφοριών ή δεδομένων ή τη μείωση της πιθανότητας αυτής, καθώς επίσης την εκτίμηση των συνεπειών και τη μείωση αυτών σε περίπτωση τέτοιου συμβάντος.

Η ασφάλεια πληροφοριών σχετίζεται άμεσα με (συνεπάγεται) την προστασία των πληροφοριακών συστημάτων που διαχειρίζονται τις πληροφορίες εντός ενός οργανισμού. Ως Πληροφοριακό Σύστημα (Information System) θεωρούμε το οργανωμένο σύνολο από λογισμικό, υλικό, δεδομένα, δίκτυα, χρήστες, διαδικασίες, και εγκαταστάσεις [4]. Τα στοιχεία αυτά βρίσκονται σε μια συνεχή αλληλεπίδραση μεταξύ τους, αλλά και με το περιβάλλον, με σκοπό την παραγωγή και διαχείριση της πληροφορίας. Η πληροφορία, στο πλαίσιο ενός οργανισμού, θεωρείται αγαθό, έχει αξία και πιθανόν και κόστος απόκτησης. Κάθε οργανισμός οφείλει να προστατεύει τα δεδομένα του λόγω της αξίας και της φύσης αυτών. Οι ειδικοί σε θέματα ασφάλειας πληροφοριών είναι υπεύθυνοι για τη διατήρηση της πληροφορίας εντός του οργανισμού ασφαλή από απειλές και κακόβουλες επιθέσεις από τον κυβερνοχώρο που συχνά προσπαθούν να αποκτήσουν κρίσιμες ιδιωτικές πληροφορίες ή να αποκτήσουν τον έλεγχο των εσωτερικών συστημάτων.

2.1.1. Απειλές και τρωτότητες

Απειλή (threat) είναι οτιδήποτε μπορεί να εκμεταλλευτεί μια ευπάθεια ενός πληροφοριακού συστήματος για να παραβιάσει την ασφάλεια του και να τροποποιήσει, να διαγράψει ή να βλάψει γενικότερα αυτό και τα δεδομένα του. Οι απειλές πραγματοποιούνται με τη χρήση κακόβουλου λογισμικού (malicious software) που σκοπός του είναι να διακόψει ή να καταστρέψει τα δεδομένα. Τα πιο

γνωστά είδη κακόβουλου λογισμικού είναι τα virus, worm, trojan horse και bot. Ανάλογα με τον τρόπο που λειτουργεί το κακόβουλο λογισμικό χαρακτηρίζεται ως adware, spyware, ransomware, scareware, rootkit ή zombie. Ανεξάρτητα από τον τρόπο που λειτουργεί, ο αντίπαλος (αυτός που απειλεί το πληροφοριακό σύστημα μέσω του κακόβουλου λογισμικού) έχει ως στόχο κάτι από τα παρακάτω [5]:

- Κλοπή πνευματικής ιδιοκτησίας (πνευματικά δικαιώματα, διπλώματα ευρεσιτεχνίας κ.ά.).
- Κλοπή ταυτότητας (κτήση προσωπικών στοιχείων ενός ατόμου ή πρόσβαση σε ζωτικές πληροφορίες όπως η πρόσβαση στον υπολογιστή ή τον λογαριασμό μέσων κοινωνικής δικτύωσης ενός ατόμου μέσω σύνδεσης στον λογαριασμό χρησιμοποιώντας τα διαπιστευτήρια σύνδεσής του).
- Κλοπή εξοπλισμού και πληροφοριών αυτού (φορητών συσκευών και δεδομένων αυτών).
- Σαμποτάζ (καταστροφή του ιστότοπου του οργανισμού για την πρόσκληση απώλειας εμπιστοσύνης από μέρους των πελατών του).
- Εκβιασμός (κλοπή πληροφοριών και χρηματικό αντάλλαγμα για την επιστροφή αυτών). Για παράδειγμα, το ransomware μπορεί να κλειδώσει τα αρχεία του θύματος, καθιστώντας τα απρόσιτα, αναγκάζοντας έτσι το θύμα να πληρώσει ως αντάλλαγμα προκειμένου να ξεκλειδωθούν τα αρχεία του.

Με την πρόοδο της τεχνολογίας, το κακόβουλο λογισμικό εξελίσσεται κι αυτό με αποτέλεσμα να δημιουργούνται νέας γενιάς απειλές [5]:

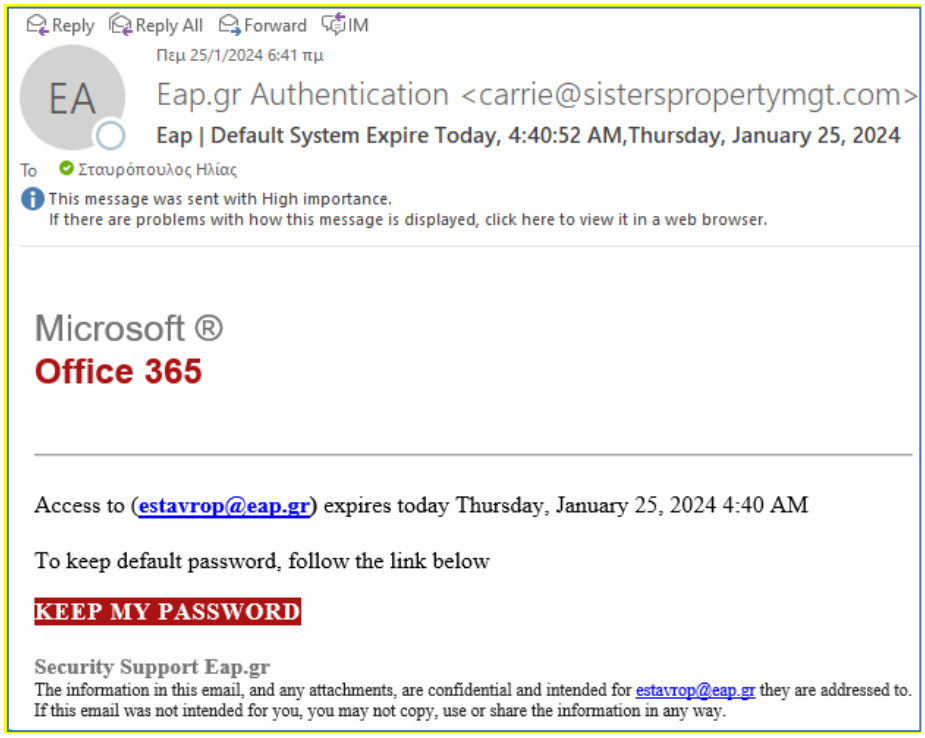
- Τεχνολογία με ασθενή ασφάλεια: τα νέα gadget που κυκλοφορούν στην αγορά παρέχουν κάποιου είδους δυνατότητες δικτύωσης ή απομακρυσμένης πρόσβασης χωρίς ωστόσο οι κατασκευαστές τους να έχουν ακολουθήσει τις αρχές ασφάλειας πληροφοριών.
- Επιθέσεις μέσων κοινωνικής δικτύωσης: ο αντίπαλος προσδιορίζει και μολύνει ένα σύμπλεγμα ιστοσελίδων που επισκέπτονται χρήστες ενός συγκεκριμένου οργανισμού, ώστε να μπορεί να υποκλέψει πληροφορίες.
- Κακόβουλο λογισμικό για κινητές συσκευές: το κακόβουλο λογισμικό δεν περιορίζεται σε συστήματα επιτραπέζιων ή φορητών υπολογιστών. Με την

πληθώρα των εφαρμογών που είναι διαθέσιμες για κινητές συσκευές, είναι πολύ πιθανό οι χρήστες να εγκαταστήσουν κατά λάθος κακόβουλο λογισμικό στις κινητές συσκευές τους.

- Ξεπερασμένο λογισμικό ασφαλείας: με νέες απειλές να εμφανίζονται καθημερινά, η ενημέρωση ενός συστήματος με τις πιο πρόσφατες ενημερώσεις σε επίπεδο λειτουργικού συστήματος, ειδικά σε ότι αφορά ενημερώσεις ασφαλείας, θα πρέπει να αποτελεί υψηλή προτεραιότητα προκειμένου να διατηρηθεί ένα πλήρως ασφαλές περιβάλλον.
- Εταιρικά δεδομένα σε προσωπικές συσκευές: πολλοί οργανισμοί επιτρέπουν στους υπαλλήλους τους να «φέρουν τη δική τους συσκευή» (BYOD). Συσκευές όπως φορητοί υπολογιστές, ταμπλέτες, ακόμη και η χρήση μονάδων USB και η αποθήκευση στο υπολογιστικό νέφος (cloud) στο χώρο εργασίας μπορούν να δημιουργήσουν σοβαρές παραβιάσεις ασφάλειας.
- Κοινωνική Μηχανική: είναι η τέχνη της χειραγώγησης των ανθρώπων ώστε να παραιτηθούν από τις εμπιστευτικές τους πληροφορίες, όπως στοιχεία τραπεζικού λογαριασμού, κωδικούς πρόσβασης κ.λ.π. Οι αντίπαλοι ξεγελούν τους χρήστες ώστε να λάβουν προσωπικές και εμπιστευτικές πληροφορίες ή να κερδίζουν την εμπιστοσύνη τους ώστε να εγκαταστήσουν ένα κακόβουλο λογισμικό που θα τους δώσει τον έλεγχο του υπολογιστή τους.

Στην Εικόνα 1 δίνεται ένα παράδειγμα «ψαρέματος» (phishing) εμπιστευτικών στοιχείων μέσω ηλεκτρονικού ταχυδρομείου. Ο χρήστης εξαπατάται και σπεύδει να εισάγει να αναγνωριστικά του, προκειμένου να μην διακοπεί η πρόσβαση του στην ηλεκτρονική του θυρίδα.

Τρωτότητα ή ευπάθεια (vulnerability) είναι μια αδυναμία που έχει ένα πληροφοριακό σύστημα, η οποία δίνει την ευκαιρία στους αντιπάλους να αποκτήσουν περιουσιακά στοιχεία του. Όλα τα συστήματα έχουν τρωτά σημεία. Παρόλο που οι τεχνολογίες και τα εργαλεία βελτιώνονται, ο αριθμός των τρωτών σημείων αυξάνεται. Τα τρωτά σημεία προέρχονται κυρίως από τέσσερεις πηγές, ήτοι, το υλικό, το λογισμικό, τα δίκτυα και τις διαδικασίες, όπου [5]:



Εικόνα 1 Παράδειγμα ψαρέματος ιδιωτικών στοιχείων χρήστη

- οι ευπάθειες υλικού αναφέρονται σε επιθέσεις στο υλικό του συστήματος είτε φυσικά είτε εξ αποστάσεως (ξεπερασμένη έκδοση συστημάτων ή συσκευών, μη προστατευμένη αποθήκευση, μη κρυπτογραφημένες συσκευές κ.ά.),
- οι ευπάθειες λογισμικού αναφέρονται σε σφάλματα λογισμικού που δημιουργήθηκαν κατά την ανάπτυξη ή τη διαμόρφωση του (μη επικύρωση της εισόδου, μη επαληθευμένες μεταφορτώσεις, cross-site scripting, μη κρυπτογραφημένα δεδομένα κ.ά.),
- οι ευπάθειες δικτύων που παρουσιάζονται είτε στο υλικό είτε στο λογισμικό (απροστάτευτη επικοινωνία, κακόβουλο λογισμικό, επιθέσεις κοινωνικής μηχανικής, εσφαλμένα διαμορφωμένα τείχη προστασίας κ.ά.),
- οι ευπάθειες διαδικασιών που αφορούν τις μεθόδους λειτουργίας του οργανισμού (π.χ., στη διαδικασία κωδικών πρόσβασης, οι κωδικοί πρόσβασης πρέπει να ακολουθούν την τυπική πολιτική κωδικών πρόσβασης, στη διαδικασία εκπαίδευσης, οι εργαζόμενοι πρέπει να γνωρίζουν τις ενέργειες που πρέπει να κάνουν για να χειριστούν την ασφάλεια, να μην διαμοιράζουν

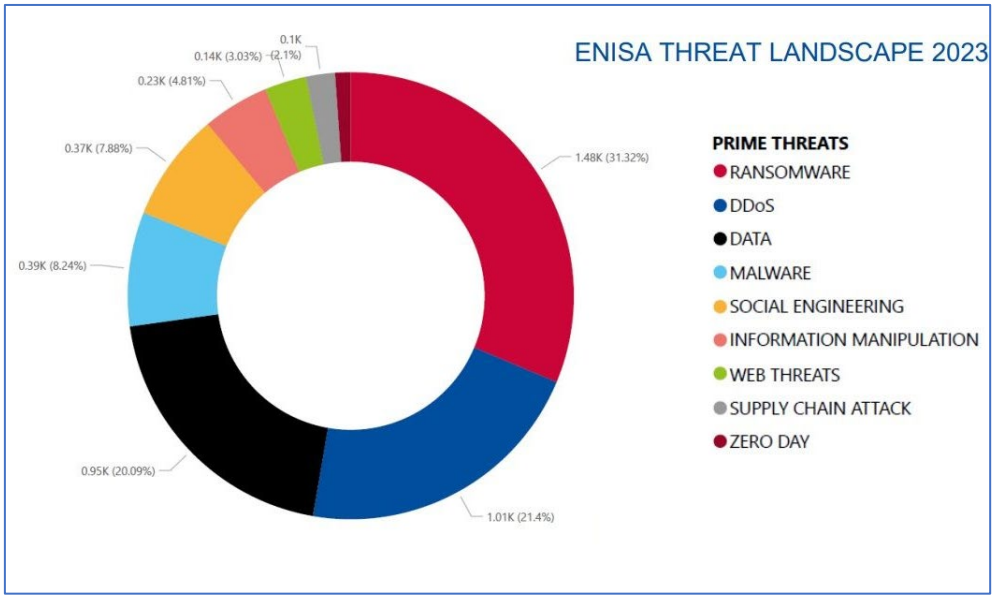
τα διαπιστευτήρια τους, να είναι ενημερωμένοι για την κοινωνική μηχανική και τις απειλές εξαπάτησης).

Αντιλαμβανόμαστε λοιπόν ότι μια απειλή μπορεί να είναι οτιδήποτε μπορεί να βλάψει τις πληροφορίες ή τα συστήματα ενός οργανισμού. Μπορεί να είναι ένα δίκτυο εισβολέων μέσω μιας θύρας στο τείχος προστασίας, μια διαδικασία πρόσβασης στα δεδομένα με τρόπο που παραβιάζει την πολιτική ασφαλείας, ένας υπάλληλος που ακούσια θα μπορούσε να αποκαλύψει εμπιστευτικές πληροφορίες ή να καταστρέψει την ακεραιότητα ενός αρχείου ή ακόμα και ένα ακραίο καιρικό φαινόμενο (μια πλημύρα ή ένας ανεμοστρόβιλος που προκαλεί καταστροφές στις εγκαταστάσεις του οργανισμού). Ένα τέτοιο παράδειγμα αποτελεί η κακοκαιρία Daniel που έπληξε στις αρχές Σεπτεμβρίου του 2023 τον Θεσσαλικό κάμπο, με αποτέλεσμα να προκληθούν σημαντικές ζημιές στα κτήρια, στα δίκτυα και στις υποδομές του Πανεπιστημίου Θεσσαλίας (δείτε στο [6] τη δήλωση του Πρύτανη του Πανεπιστημίου λίγες ημέρες μετά).

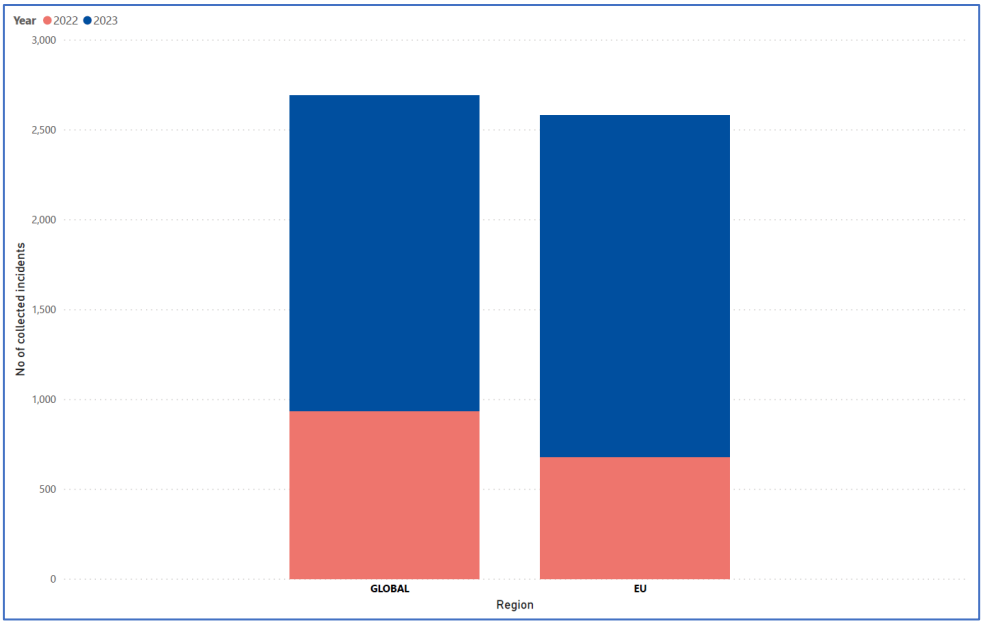
Στο [7] δίνεται μια πρόσφατη λίστα από συνήθεις απειλές και τρωτά σημεία για ένα σύστημα πληροφοριών. Πρέπει να αναφέρουμε ότι οι απειλές που μπορεί να δεχθεί ένα σύστημα πληροφοριών δεν είναι μόνο τεχνικές αλλά μπορεί να είναι και μη τεχνικές, όπως για παράδειγμα απειλές που αφορούν την κλοπή ή τον βανδαλισμό του εξοπλισμού, ακραία καιρικά φαινόμενα και φυσικές καταστροφές που φέρνουν σε κίνδυνο τις εγκαταστάσεις του οργανισμού, εξαπάτηση από υπαλλήλους ή συνεργάτες, μη ασφαλείς διαδικασίες απόρριψης ευαίσθητων δεδομένων κ.ά. Είναι σημαντικό για την ασφάλεια των πληροφοριών του ο οργανισμός να εντοπίσει τις πιθανές απειλές και τις ευπάθειες, να τις ομαδοποιήσει ανά κατηγορία και να αξιολογήσει την πιθανή ζημία από αυτές. Μια λίστα με απειλές καθώς και σημεία ελέγχου αυτών των απειλών είναι διαθέσιμες στο [8].

Σύμφωνα με πρόσφατη αναφορά του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (European Union Agency for Cybersecurity – ENISA) [9], το τοπίο της κυβερνοασφάλειας σημείωσε σημαντική αύξηση τόσο στην ποικιλία όσο και στην ποσότητα των κυβερνοεπιθέσεων και στις συνέπειές τους (το τοπίο επηρέασε και ο πόλεμος μεταξύ Ουκρανίας και Ρωσίας). Στην Εικόνα 2

βλέπουμε τις κύριες απειλές και τα ποσοστά εμφάνισης της κατά τη χρονικό διάστημα 7ος 2022 – 6ος 2023, όπου οι απειλές τύπου Ransomware (οι αντίπαλοι αναλαμβάνουν τον έλεγχο των περιουσιακών στοιχείων και απαιτούν λύτρα με αντάλλαγμα την επιστροφή της διαθεσιμότητας τους) και DDoS (επιθέσεις όπου οι χρήστες ενός συστήματος ή μιας υπηρεσίας δεν έχουν πρόσβαση σε σχετικά δεδομένα, υπηρεσίες ή άλλους πόρους) ξεπέρασαν το 50% των περιπτώσεων που είχαν καταγραφεί.



Εικόνα 2 Κύριες απειλές κυβερνοασφάλειας

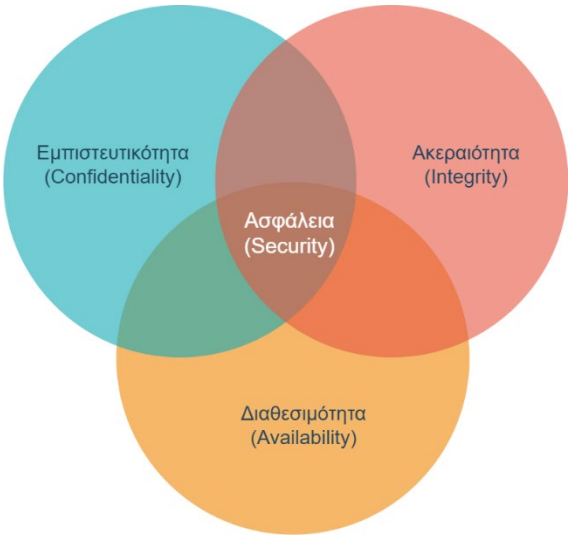


Εικόνα 3 Αύξηση των απειλών κυβερνοασφάλειας στην Ε.Ε. και παγκοσμίως

Σύμφωνα με την αναφορά του ENISA [9], όπως παρατηρούμε στην Εικόνα 3, οι απειλές αυξήθηκαν σε σχέση με το προηγούμενο έτος αναφοράς τόσο στην ευρωπαϊκή ένωση όσο και παγκοσμίως.

2.1.2. Μοντέλα ασφάλειας πληροφοριών

Σύμφωνα με την Επιτροπή Εθνικής Ασφάλειας Συστημάτων των Ηνωμένων Πολιτειών (Committee on National Security Systems, CNSS), πρωταρχικός στόχος της ασφάλειας πληροφοριών είναι η ισόρροπη προστασία της εμπιστευτικότητας (Confidentiality), της ακεραιότητας (Integrity) και της διαθεσιμότητας (Availability) των δεδομένων (Εικόνα 4). Η τριάδα C.I.A. αποτελεί το πιο διαδεδομένο μοντέλο ασφάλειας πληροφοριών το οποίο παρέχει μια ολοκληρωμένη προσέγγιση για την ασφάλεια των συστημάτων πληροφοριών, αντιμετωπίζοντας τις βασικές πτυχές της προστασίας ευαίσθητων πληροφοριών, τη διατήρηση της ακεραιότητας των δεδομένων και τη διασφάλιση της διαθεσιμότητας του συστήματος.



Εικόνα 4 Το μοντέλο ασφάλειας πληροφοριών C.I.A.

Η εμπιστευτικότητα αναφέρεται στην προστασία ευαίσθητων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση ή αποκάλυψη. Διασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα ή οντότητες μπορούν να έχουν πρόσβαση και να δουν τις πληροφορίες. Για τη διατήρηση της εμπιστευτικότητας οι καλύτερες τεχνικές που μπορούν να χρησιμοποιηθούν είναι η κρυπτογράφηση δεδομένων (data encryption), η

αυθεντικοποίηση δύο παραγόντων (two-factor authentication) και η περιορισμένη έκθεση της ευαίσθητης πληροφορίας.

Η ακεραιότητα διασφαλίζει ότι η πληροφορία παραμένει ακριβής, πλήρης και αναλλοίωτη καθώς μεταδίδεται και δεν μπορεί να τροποποιηθεί χωρίς εξουσιοδότηση. Περιλαμβάνει την προστασία δεδομένων από μη εξουσιοδοτημένη τροποποίηση, διαγραφή ή καταστροφή. Η μη εξουσιοδοτημένη πρόσβαση μπορεί να αποφευχθεί μέσω περιορισμών πρόσβασης χρηστών και με δικαιώματα αρχείων. Για την διατήρηση της ακεραιότητας χρησιμοποιούνται τεχνικές όπως η επικύρωση δεδομένων (data validation), οι συναρτήσεις αθροισμάτων ελέγχου (checksums) και οι ψηφιακές υπογραφές (digital signatures).

Η διαθεσιμότητα διασφαλίζει ότι οι πληροφορίες και τα συστήματα είναι προσβάσιμα και χρησιμοποιήσιμα όταν απαιτηθεί χωρίς περιορισμούς ή παρεμβάσεις. Περιλαμβάνει την πρόληψη διακοπών που θα μπορούσαν να επηρεάσουν τη διαθεσιμότητα των πόρων. Για τη διασφάλιση της διαθεσιμότητας εφαρμόζονται τεχνικές όπως πλεονασμός (redundancy), ανοχή σφαλμάτων (fault tolerance) και σχέδιο αποκατάστασης καταστροφών (Disaster Recovery Plan, DRP).

Το μοντέλο ασφαλείας CNSS παρέχει μια ολοκληρωμένη προσέγγιση για την ασφάλεια των συστημάτων πληροφοριών, αντιμετωπίζοντας τις βασικές πτυχές της προστασίας ευαίσθητων πληροφοριών, της διατήρησης της ακεραιότητας των δεδομένων και της διασφάλισης της διαθεσιμότητας του συστήματος.

Ένα άλλο μοντέλο ασφάλειας πληροφοριών είναι το εξαγωνικό μοντέλο του Parker (Parkerian hexan model) [10]). Το μοντέλο αυτό, που δεν είναι τόσο διαδεδομένο όσο η τριάδα C.I.A., περιλαμβάνει τις τρεις αρχές του C.I.A. μαζί με ακόμα τρεις: την Αυθεντικότητα (Authenticity), την Κατοχή (Possession) και την Χρηστικότητα (Utility) (Εικόνα 4).

Εικόνα 5 Το εξαγωνικό μοντέλο του Parker

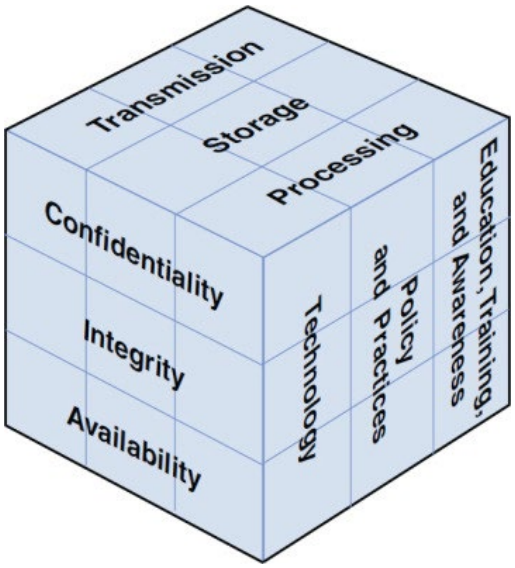
Η αυθεντικότητα αναφέρεται στην ακρίβεια του ισχυρισμού προέλευσης ή γνησιότητας της πληροφορίας. Για παράδειγμα, μια μέθοδος για την επαλήθευση της γνησιότητας ενός χειρόγραφου εγγράφου είναι η σύγκριση των χειρόγραφων χαρακτηριστικών του εγγράφου με ένα δείγμα άλλων που έχουν ήδη επαληθευτεί. Για την επαλήθευση της γνησιότητας ενός ψηφιακού εγγράφου θα μπορούσε να χρησιμοποιηθεί μια ψηφιακή υπογραφή χρησιμοποιώντας κρυπτογραφία δημόσιου κλειδιού (θα μπορούσε επίσης να χρησιμοποιηθεί για την επαλήθευση της ακεραιότητας του εγγράφου).

Η Κατοχή (ή έλεγχος) αναφέρεται σε μία κατάσταση η οποία δείχνει απώλεια ελέγχου ή κατοχής πληροφοριών, αλλά δεν συνεπάγεται παραβίαση του απορρήτου. Αν, για παράδειγμα, ένας κλέφτης έπρεπε να κλέψει έναν σφραγισμένο φάκελο που περιείχε μια τραπεζική χρεωστική κάρτα και τον προσωπικό της αριθμό αναγνώρισης, ακόμα κι αν ο κλέφτης δεν άνοιξε αυτόν τον φάκελο, είναι λογικό για το θύμα να ανησυχεί ότι ο κλέφτης θα μπορούσε να το κάνει ανά πάσα στιγμή.

Η χρηστικότητα αναφέρεται στη χρησιμότητα των πληροφοριών. Αν για παράδειγμα κάποιος κρυπτογραφούσε τα δεδομένα του για να αποτρέψει μη εξουσιοδοτημένη πρόσβαση ή μη ανιχνευμένες τροποποιήσεις αυτών, και στη συνέχεια έχανε το κλειδί αποκρυπτογράφησης, τότε αυτό θα ήταν παραβίαση της χρηστικότητας. Τα δεδομένα θα ήταν μεν εμπιστευτικά, ελεγχόμενα, ολοκληρωμένα, αυθεντικά και

διαθέσιμα, αλλά δεν θα ήταν χρήσιμα σε αυτή τη μορφή. Ομοίως, η μετατροπή δεδομένων ή η αποθήκευση τους σε μορφή ακατάλληλη για μια συγκεκριμένη αρχιτεκτονική υπολογιστή θα αποτελούσε παραβίαση της χρηστικότητας των δεδομένων. Αναλυτική περιγραφή των χαρακτηριστικών του εξαγωνικού μοντέλου του Parker δίνεται στο [9], μαζί με μια συγκριτική παρουσίαση του με τα χαρακτηριστικά της τριάδας C.I.A.

Ο κύβος McCumber αποτελεί μια πολύπλευρη προσέγγιση της ασφάλειας της πληροφορίας, ο οποίος εισήχθη το 1991 [11], παρουσιάστηκε αναλυτικά το 2004 [12] και θεωρεί την ασφάλεια ως έναν κύβο, όπου οι διαστάσεις του είναι οι στόχοι, οι καταστάσεις και οι διασφαλίσεις (Πηγή: [13]). Ο κύβος McCumber αποτελεί φυσική επέκταση του τριγώνου της C.I.A. σε τρεις διαστάσεις, το οποίο είναι σημαντικό πλεονέκτημα καθώς το τρίγωνο της C.I.A. είναι ευρέως γνωστό και κατανοητό στην κοινότητα της κυβερνοασφάλειας. Αυτό κάνει τη μετάβαση στον κύβο McCumber, και στη συνέχεια μια ταξινόμηση που βασίζεται στον κύβο McCumber, ευκολότερη.



Εικόνα 6 Ο κύβος του McCumber.

2.2. Ο Γενικός Κανονισμός Προστασίας Δεδομένων

Οι πληροφορίες και τα δεδομένα που διαχειρίζεται ένας οργανισμός αποτελούν τα περιουσιακά στοιχεία ή αλλιώς τα αγαθά (assets) του οργανισμού. Είναι εκείνα τα στοιχεία που χρήζουν προστασίας, ανάλογα με την σημαντικότητα τους και τον

βαθμό ευαισθησία τους. Έτσι, ο οργανισμός μπορεί να χαρακτηρίσει τα δεδομένα του ως δημόσια, εσωτερικής χρήσης, περιορισμένης χρήσης ή εμπιστευτικά, ανάλογα με την αξία τους, την κρισιμότητα τους στη λειτουργία του οργανισμού, καθώς επίσης και απαιτήσεις που διέπει η νομοθεσία.

Στο πλαίσιο των δραστηριοτήτων τους, κεντρική εργασία των οργανισμών είναι η επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η «*επεξεργασία*» καλύπτει ευρύ φάσμα πράξεων που πραγματοποιούνται σε δεδομένα προσωπικού χαρακτήρα, είτε με χειροκίνητα είτε με αυτοματοποιημένα μέσα. Περιλαμβάνει τη συλλογή, καταχώριση, οργάνωση, διάρθρωση, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση, χρήση, κοινολόγηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμό, περιορισμό, διαγραφή ή καταστροφή δεδομένων προσωπικού χαρακτήρα. Τα «*δεδομένα προσωπικού χαρακτήρα* – ΔΠΧ» είναι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο. Διαφορετικές πληροφορίες οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, αποτελούν επίσης δεδομένα προσωπικού χαρακτήρα. Οποιοδήποτε φυσικό πρόσωπο είναι υποκείμενο των δεδομένων που επεξεργάζεται ο οργανισμός.

Παραδείγματα δεδομένων προσωπικού χαρακτήρα είναι το όνομα και επώνυμο ενός ατόμου, η διεύθυνση κατοικίας και η διεύθυνση ηλεκτρονικού ταχυδρομείου, ο αριθμός της ταυτότητας του, η διεύθυνση διαδικτυακού πρωτοκόλλου (IP) του υπολογιστή μου, ο αναγνωριστικός αριθμός της πιστωτικής του κάρτας, δεδομένα θέσης που προκύπτουν από το κινητό του τηλέφωνο, ιατρικά δεδομένα που φυλάσσονται από νοσοκομείο ή γιατρό, κ.ά. Τα δεδομένα προσωπικού χαρακτήρα μπορεί να είναι γενετικά (αφορούν γενετικά χαρακτηριστικά που προκύπτουν από την ανάλυση βιολογικού δείγματος), βιομετρικά (προκύπτουν από την επεξεργασία φυσικών, βιολογικών ή συμπεριφορικών χαρακτηριστικών όπως εικόνες προσώπου, ίριδα οφθαλμού ή δακτυλικό αποτύπωμα) ή δεδομένα που αφορούν την υγεία (σχετίζονται με τη σωματική ή ψυχική υγεία και αποκαλύπτουν πληροφορίες για την κατάσταση της υγείας) του ατόμου [14].

Παραδείγματα επεξεργασίας δεδομένων είναι η διαχείριση προσωπικού και η μισθοδοσία, η προσπέλαση/αναζήτηση πληροφοριών σε βάση δεδομένων επαφών που περιλαμβάνει δεδομένα προσωπικού χαρακτήρα, η δημοσίευση/ανάρτηση φωτογραφίας ενός ατόμου σε κάποια ιστοσελίδα, η αποστολή διαφημιστικών ηλεκτρονικών μηνυμάτων, η καταστροφή εγγράφων που περιέχουν δεδομένα προσωπικού χαρακτήρα, η αποθήκευση διαδικτυακών διευθύνσεων, η μαγνητοσκόπηση μέσω κλειστού κυκλώματος τηλεόρασης (CCTV), κ.ά. [14].

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων – ΓΚΠΔ (General Data Protection Regulation – GDPR) της Ευρωπαϊκής Ένωσης (κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 [15] [16]), που τέθηκε σε εφαρμογή την 25η Μαΐου 2018, ρυθμίζει την επεξεργασία από άτομο, εταιρεία ή οργανισμό των δεδομένων προσωπικού χαρακτήρα που αφορούν άτομα στην ΕΕ. Ο ΓΚΠΔ αφορά την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και καταργεί την προγενέστερη οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995 [17]. Ορίζει τα δικαιώματα των πολιτών (υποκειμένων των δεδομένων): ενημέρωση, διόρθωση, διαγραφή, περιορισμός της επεξεργασίας, φορητότητα των δεδομένων και εναντίωση την επεξεργασία. Επιπρόσθετα, ο ΓΚΠΔ επιβάλλει μια σειρά υποχρεώσεων στους υπεύθυνους επεξεργασίας, οι οποίες απορρέουν από τις βασικές αρχές και ιδίως την ενισχυμένη αρχή της διαφάνειας στον τρόπο συλλογής, επεξεργασίας και τήρησης δεδομένων και την αρχή της λογοδοσίας, σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωσή του με όλες τις αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων.

Μία από τις βασικές υποχρεώσεις του υπευθύνου επεξεργασίας (καθορίζει τους σκοπούς και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα) είναι η Εκτίμηση Αντικτύπου σχετικά με την Προστασία των Δεδομένων - ΕΑΠΔ (Data Protection Impact Assessment – DPIA) όταν η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα των ατόμων, ιδίως επειδή είναι συστηματική,

μεγάλης κλίμακας, αφορά ειδικές κατηγορίες δεδομένων και βασίζεται στη χρήση νέων τεχνολογιών. Όταν βάσει της διενεργηθείσας εκτίμησης αντικτύπου και παρά την πρόβλεψη μέτρων προστασίας παραμένει υψηλή η επικινδυνότητα της επεξεργασίας, ο υπεύθυνος επεξεργασίας υποχρεούται να προβεί σε προηγούμενη διαβούλευση με την Εποπτική Αρχή, όπου στην Ελλάδα η αρχή αυτή ονομάζεται Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).

Η ΕΑΠΔ είναι μια διαδικασία που έχει σχεδιαστεί για να περιγράψει την επεξεργασία, να αξιολογήσει την αναγκαιότητα και την αναλογικότητά της και να συνδράμει στη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που συνεπάγεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, με την αξιολόγησή τους και τον καθορισμό μέτρων για την αντιμετώπισή τους. Για τους σκοπούς του ΓΚΠΔ έχουν εκδοθεί κατευθυντήριες γραμμές για την ΕΑΠΔ και τον καθορισμό του κατά πόσον η επεξεργασία «*ενδέχεται να επιφέρει υψηλό κίνδυνο*» [18]. Επίσης, η ΕΑΠΔ αποτελεί:

α. σημαντικό εργαλείο για την πλήρωση της υποχρέωσης λογοδοσίας, καθώς παρέχει συνδρομή στους υπεύθυνους επεξεργασίας όχι μόνον προκειμένου να συμμορφώνονται με τις προδιαγραφές του ΓΚΠΔ, αλλά και για να αποδεικνύουν ότι έχουν ληφθεί τα ενδεδειγμένα μέτρα για τη διασφάλιση της συμμόρφωσης προς τον ΓΚΠΔ,

β. μία από τις τεχνικές ανάλυσης της διακινδύνευσης (risk analysis), όπου ένα από τα στάδια της εκτίμησης της διακινδύνευσης (risk assessment) αποτελεί κεντρικό θέμα της παρούσης εργασίας, και

γ. τεχνική που εφαρμόζεται για τη διαχείριση της διακινδύνευσης (risk management) ενός οργανισμού, η οποία απαιτείται για την ασφάλεια των πληροφοριών.

2.3. Αρχές νομιμότητας επεξεργασίας

Σύμφωνα με το άρθρο 5 του ΓΚΠΔ, η επεξεργασία προσωπικών δεδομένων (απλών και ειδικών κατηγοριών) χαρακτηρίζεται ως νόμιμη εφόσον διέπεται από

συγκεκριμένες αρχές. Παραθέτουμε τις αρχές αυτές όπως παρουσιάζονται από την Αρχή Προστασίας Δεδομένων στο [19]:

- Η αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας: Τα δεδομένα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία, με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Η διαφάνεια απαιτεί η ενημέρωση του υποκειμένου να είναι συνοπτική, εύκολα προσβάσιμη, κατανοητή, με σαφή και απλή διατύπωση.
- Η αρχή του περιορισμού του σκοπού: Τα δεδομένα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με τους σκοπούς αυτούς.
- Η αρχή της αναλογικότητας («ελαχιστοποίηση των δεδομένων»): Τα δεδομένα θα πρέπει να είναι πρόσφορα, συναφή και αναγκαία για τους επιδιωκόμενους σκοπούς επεξεργασίας.
- Η αρχή της ακρίβειας των δεδομένων: Τα δεδομένα θα πρέπει να είναι ακριβή, να επικαιροποιούνται και να λαμβάνονται τα κατάλληλα μέτρα για την άμεση διόρθωση ή διαγραφή ανακριβών σε σχέση με τους επιδιωκόμενους σκοπούς επεξεργασίας δεδομένων.
- Η αρχή του καθορισμού της χρονικής διάρκειας της επεξεργασίας («περιορισμός της περιόδου αποθήκευσης»): Τα δεδομένα πρέπει να τηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για την επίτευξη των σκοπών της επεξεργασίας.
- Η αρχή της «ακεραιότητας και εμπιστευτικότητας»: Τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ασφάλεια και προστασία τους από παράνομη επεξεργασία, απώλεια, καταστροφή ή φθορά τους.
- Η αρχή της λογοδοσίας του υπευθύνου επεξεργασίας: Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωσή του με τον ΓΚΠΔ ενώπιον των εποπτικών αρχών και των δικαστηρίων.

2.4. Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών

Με βάση την Ενότητα 2.1, η «ασφάλεια πληροφοριών» περιλαμβάνει τη διαχείριση της ασφάλειας των πληροφοριών καθώς και την ασφάλεια των υπολογιστών και των δικτύων. Επίσης, περιλαμβάνει πολιτικές και διαδικασίες του οργανισμού, ρόλους και αρμοδιότητες των χρηστών αυτού, νομικό και θερμικό πλαίσιο λειτουργίας του

οργανισμού κ.ά., για τα οποία απαιτείται η συμβολή πολλών επιστημών [20]. Κατά συνέπεια, δεν αρκεί μόνο η υιοθέτηση και αξιοποίηση σύγχρονων τεχνολογιών και επικοινωνιών αλλά είναι απαραίτητη και η οργανωμένη διακυβέρνηση και διοίκηση της ασφάλειας πληροφοριών.

Ως διακυβέρνηση ασφάλειας πληροφοριών (information security governance) ορίζεται η επιχειρησιακή διεργασία της εγκαθίδρυσης και διατήρησης ενός πλαισίου και μιας διοικητικής δομής που διασφαλίζει ότι οι στρατηγικές ασφάλειας πληροφοριών υποστηρίζουν και εναρμονίζονται με τους στόχους του οργανισμού, αναθέτουν υπευθυνότητες και είναι συνεπείς με το νομικό και θεσμικό πλαίσιο, εφαρμόζοντας τις κατάλληλες πολιτικές και μέτρα, σε μια προσπάθεια να διαχειριστούν τους κινδύνους ασφάλειας [21].

Ενώ η διακυβέρνηση ασφάλειας πληροφοριών ασχολείται με την στρατηγική ασφάλειας πληροφοριών, δηλαδή με το τι πρέπει να γίνει, η διοίκηση ασφάλειας πληροφοριών (information security management) ασχολείται με το πώς θα υλοποιηθεί η στρατηγική. Η διοίκηση ασφάλειας πληροφοριών ορίζει τους στόχους ασφάλειας και διαμορφώνει πολιτικές, διαδικασίες και οδηγίες για την επίτευξη των στόχων. Επιπλέον, καθοδηγεί και επιβλέπει τη λήψη αποφάσεων που σχετίζονται με την ασφάλεια πληροφοριών σε όλα τα επίπεδα του οργανισμού, από το επίπεδο της καθημερινής λειτουργίας (π.χ. αποφάσεις για την εκχώρηση δικαιωμάτων πρόσβασης σε χρήστες) μέχρι το επίπεδο της ανώτερης διοίκησης (π.χ. αποφάσεις για την προμήθεια συστημάτων) [20]. Σχεδιάζει ένα σύνολο κανόνων, διαδικασιών, μέτρων και πολιτικών το οποίο καλείται να εφαρμόζει ο οργανισμός προκειμένου να οργανώσει τη διοίκηση της ασφάλειας των πληροφοριών του. Το σύνολο των παραπάνω καλείται Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών – ΣΔΑΠ (Information Security Management System – ISMS).

Ένα σύστημα διαχείρισης χρησιμοποιεί ένα πλαίσιο από πόρους για την επίτευξη των στόχων του οργανισμού. Το σύστημα διαχείρισης περιλαμβάνει την οργανωτική δομή, πολιτικές, προγραμματισμένες δραστηριότητες, ευθύνες, πρακτικές, διαδικασίες, διεργασίες και πόρους. Όσον αφορά την ασφάλεια των πληροφοριών, ένα ΣΔΑΠ επιτρέπει στον οργανισμό να [2]:

- ικανοποιεί τις απαιτήσεις ασφάλειας πληροφοριών των πελατών και άλλων ενδιαφερομένων,
- βελτιώσει τα σχέδια και τις δραστηριότητες του οργανισμού,
- ανταποκρίνεται στους στόχους ασφάλειας πληροφοριών του οργανισμού,
- συμμορφώνονται με τους κανονισμούς, τη νομοθεσία και τις κλαδικές εντολές
- διαχειρίζεται τα περιουσιακά στοιχεία του οργανισμού με οργανωμένο τρόπο που διευκολύνει τη συνεχή βελτίωση και προσαρμογή στους τρέχοντες οργανωτικούς στόχους.

Η υιοθέτηση ενός ΣΔΑΠ είναι σημαντική τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα προκειμένου ο οργανισμός να προστατέψει τα περιουσιακά του στοιχεία. Η ασφάλεια πληροφοριών απαιτεί τη διαχείριση της επικινδυνότητας (risk management) η οποία περιλαμβάνει κινδύνους από φυσικές, ανθρώπινες και τεχνολογικές απειλές που σχετίζονται με το σύνολο των πληροφοριών που παράγονται ή χρησιμοποιούνται από τον οργανισμό. Όπως είδαμε σε προηγούμενη ενότητα, τα συστήματα πληροφοριών και τα δίκτυα ενός οργανισμού αντιμετωπίζουν απειλές ασφαλείας που προέρχονται από ένα ευρύ φάσμα πηγών. Δυστυχώς, η ασφάλεια πληροφοριών δεν λαμβάνεται πάντα υπόψη κατά το σχεδιασμό και την ανάπτυξη των πληροφοριακών συστημάτων. Επιπλέον, η ασφάλεια των πληροφοριών δεν απαιτεί μόνο τεχνικές λύσεις. Η ασφάλεια που μπορεί να επιτευχθεί μόνο με τεχνικά μέσα είναι περιορισμένη και θα είναι μη αποτελεσματική αν δεν υποστηριχθεί από κατάλληλη διαχείριση και διαδικασίες μέσω ενός ΣΔΑΠ.

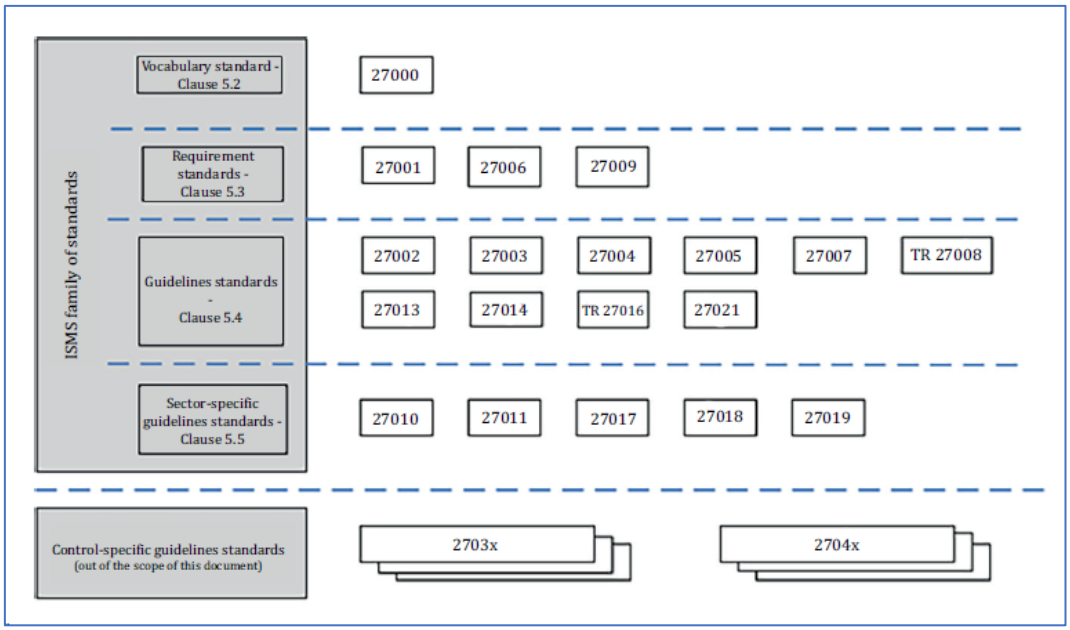
Η υιοθέτηση ενός ΣΔΑΠ αποτελεί μια στρατηγική απόφαση για τον οργανισμό. Ο σχεδιασμός και η εφαρμογή του ΣΔΑΠ ενός οργανισμού εξαρτάται από τις ανάγκες και τους στόχους του οργανισμού, τις απαιτήσεις ασφάλειας, τις επιχειρηματικές διαδικασίες και το μέγεθος και τη δομή του οργανισμού. Ο σχεδιασμός και η λειτουργία ενός ΣΔΑΠ πρέπει να αντανακλά τα ενδιαφέροντα και τις απαιτήσεις ασφάλειας πληροφοριών όλων των ενδιαφερόμενων μερών του οργανισμού, συμπεριλαμβανομένων των πελατών, των προμηθευτών, των επιχειρηματικών εταίρων, των μετόχων και άλλων τρίτων μερών. Η επιτυχής υιοθέτηση ενός ΣΔΑΠ επιτρέπει στον οργανισμό να [2]:

- έχει μεγαλύτερη βεβαιότητα ότι τα περιουσιακά της στοιχεία προστατεύονται επαρκώς από απειλές σε συνεχή βάση,
- διατηρήσει ένα δομημένο και περιεκτικό πλαίσιο για τον αναγνώριση και την αξιολόγηση των κινδύνων ασφάλειας πληροφοριών, την επιλογή και την εφαρμογή των εφαρμόσιμων ελέγχου και τη μέτρηση και τη βελτίωση της αποτελεσματικότητάς τους,
- βελτιώνει διαρκώς το περιβάλλον ελέγχου του,
- επιτύχει αποτελεσματική νομική και κανονιστική συμμόρφωση.

Τα ΣΔΑΠ ακολουθούν συγκεκριμένο πρότυπο που προδιαγράφει τις απαιτήσεις που πρέπει να ικανοποιούν. Πρόκειται για το πρότυπο ISO/IEC 27001 [22] (περιγράφεται αναλυτικά στην επόμενη ενότητα) το οποίο εκδίδεται από τον Διεθνή Οργανισμό Τυποποίησης (International Organization for Standardization, ISO) σε συνεργασία με τη Διεθνή Επιτροπή Ηλεκτροτεχνίας (International Electrotechnical Commission, IEC). Το πρότυπο ISO/IEC 27001 καθορίζει τις απαιτήσεις για την καθιέρωση, υλοποίηση, συντήρηση και διαρκή βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών ενός οργανισμού και προσφέρει ένα ολοκληρωμένο πλαίσιο διαχείρισης και καθορισμού των απαιτήσεων για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών. Ανήκει στην ευρύτερη οικογένεια προτύπων ISO/IEC 270xx (Εικόνα 7, Πηγή [2]) που παρέχουν ένα οδηγό βέλτιστων πρακτικών για τις απαιτήσεις ενός ΣΔΑΠ, γενικές οδηγίες και την υλοποίηση ενός ΣΔΑΠ καθώς και ειδικές οδηγίες ανάλογα με τον τομέα δραστηριοποίησης ενός οργανισμού.

Οι οργανισμοί οι οποίοι συμμορφώνονται με τις αιτήσεις του προτύπου ISO/IEC 27001 πιστοποιούνται μετά από επιθεώρηση που πραγματοποιείται από ανεξάρτητους διαπιστευμένους φορείς πιστοποίησης. Η διαπίστευση των φορέων διενεργείται από το Εθνικό Σύστημα Διαπίστευσης (Ε.ΣΥ.Δ.) που αποτελεί τον Εθνικό Οργανισμό Διαπίστευσης της Ελλάδας. Στην Εικόνα 8 δίνεται ένα παράδειγμα πιστοποιητικού οργανισμού από διαπιστευμένο φορέα, όπου η διαπίστευση πραγματοποιείται σύμφωνα με το πρότυπο ISO/IEC 17065 [23] και των

συμπληρωματικών απαιτήσεων διαπίστευσης που ορίζονται από την αρμόδια εποπτική αρχή.



Εικόνα 7 Η οικογένεια προτύπων Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών

Το πρότυπο ISO/IEC 27000:2018 [2] παρέχει μια επισκόπηση των ΣΔΑΠ καθώς επίσης τους όρους και τους ορισμούς που χρησιμοποιούνται στην οικογένεια προτύπων ISO/IEC 270xx που αφορούν τα ΣΔΑΠ. Σύμφωνα με αυτό, για την καθιέρωση, την παρακολούθηση, την συντήρηση και την βελτίωση ενός ΣΔΑΠ, ένας οργανισμός θα πρέπει να αναλάβει τα παρακάτω βήματα:

α. να προσδιορίζει τα περιουσιακά στοιχεία πληροφοριών και τις σχετικές απαιτήσεις ασφάλειας πληροφοριών,
β. να αξιολογεί και να αντιμετωπίζει τους κινδύνους για την ασφάλεια των πληροφοριών,
γ. να επιλέγει και να εφαρμόζει σχετικούς ελέγχους για τη διαχείριση των κινδύνων,
δ. να παρακολουθεί, να συντηρεί και να βελτιώνει την αποτελεσματικότητα των ελέγχων.

Το βήμα (β) αφορά την εκτίμηση της διακινδύνευσης (risk assessment), που αποτελεί ένα από τα στάδια της διαχείρισης της διακινδύνευσης (risk management). Οι έννοιες

αλλά και οι τεχνικές αυτών θα αναφερθούν σε επόμενες ενότητες, καθώς αποτελούν κεντρικό θέμα της παρούσας εργασίας.

TÜVNORD

Πιστοποιητικό

Σύστημα Διαχείρισης σύμφωνα με

ΕΛΟΤ ISO/IEC 27001 : 2013

Ο Φορέας Πιστοποίησης TÜV HELLAS (TÜV NORD) S.A. επιβεβαιώνει με το παρόν ότι, ως αποτέλεσμα επιθεώρησης, αξιολόγησης και απόφασης πιστοποίησης σύμφωνα με το ISO/IEC 17021-1 : 2015 ο οργανισμός

ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
Τμήμα Εγκαταστάσεων και Εκτέλεσης Έργων
Πάροδος Αριστοτέλους 18
263 35 Πάτρα
Ελλάδα

εφαρμόζει ένα Σύστημα Διαχείρισης σύμφωνα με τις απαιτήσεις του προτύπου ΕΛΟΤ ISO/IEC 27001 : 2013, του οποίου η συμμόρφωση θα αξιολογείται κατά τη διάρκεια της τριετούς ισχύος

Πεδίο Εφαρμογής

- **Εξ Αποστάσεως Παροχή ΠροΠτυχιακής και ΜεταΠτυχιακής ΕκΠαίδευσης και ΕπιμόρφωσηΣ**
- **ΑνάΠτυξη ΚατάλληλΟυ ΕκΠαιδευτικΟύ ΥλικΟύ**
- **ΑνάΠτυξη ΤεχνολογίΑς και ΜεθοδολογίΑς στη ΜετάδοΣη της ΓνώσηΣ απο ΑπόσταΣη**

S.o.A.: Έκδοση 6, με Ημερομηνία από: 20.07.2021

Αριθμός Μητρώου Πιστοποιητικού 048 20 0012
Αρ. Αναφοράς Επιθεώρησης IS-0037/2023

Λήξη Προηγούμενου Πιστοποιητικού 2023-09-10
Ισχύει από 2023-12-20
Ισχύει μέχρι 2025-10-31
(Μέχρι 2026-09-09 σε περίπτωση Αναβάθμισης στο ISO 27001:2022)
Αρχική Πιστοποίηση 2020

Αθήνα, 20.12.2023

TÜV HELLAS (TÜV NORD) A.E. Φορέας Πιστοποίησης

TÜV HELLAS (TÜV NORD) A.E.
Λ. Μεσογείων 282
155 62 Αθήνα, Ελλάδα
tuvhellas.gr

TÜV®

TÜVNORDGROUP

Εικόνα 8 Παράδειγμα πιστοποιητικού σύμφωνα με το πρότυπο ISO/IEC 27001[1]

Για να διασφαλιστεί ότι το ΣΔΑΠ προστατεύει αποτελεσματικά τα πληροφοριακά περιουσιακά στοιχεία του οργανισμού σε συνεχή βάση, είναι απαραίτητο τα παραπάνω βήματα να επαναλαμβάνονται διαρκώς για τον εντοπισμό αλλαγών στους κινδύνους ή στις στρατηγικές ή τους επιχειρηματικούς στόχους του οργανισμού. Το

[1] https://www.eap.gr/wp-content/uploads/2024/01/EAP-27001-GR-RE-1.pdf

πρότυπο ISO/IEC 27001 που θα περιγράψουμε στην επόμενη ενότητα, καθορίζει τις απαιτήσεις για την καθιέρωση ενός ΣΔΑΠ. Η συμμόρφωση ενός οργανισμού στις απαιτήσεις του προτύπου ISO/IEC 27001 και η πιστοποίηση του από διαπιστευμένο φορέα, αυξάνει το κύρος και την αξιοπιστία του οργανισμού στο χώρο δραστηριοποίησης του και αποτελεί σημαντικό πλεονέκτημα συγκριτικά με άλλους μη πιστοποιημένους οργανισμούς.

2.5. Το πρότυπο ISO/IEC 27001

Το πρότυπο ISO/IEC 27001 είναι παγκοσμίως το πιο δημοφιλές πρότυπο για την ασφάλεια πληροφοριών. Καθορίζει τις απαιτήσεις που πρέπει να πληροί ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών. Ανεξάρτητα από το μέγεθος και τον τομέα δραστηριότητας, το πρότυπο ISO/IEC 27001 παρέχει στους οργανισμούς καθοδήγηση για τη δημιουργία, την εφαρμογή, τη συντήρηση και τη συνεχή βελτίωση ενός ΣΔΑΠ.

Με το έγκλημα στον κυβερνοχώρο να αυξάνεται και νέες απειλές να αναδύονται συνεχώς, μπορεί να φαίνεται δύσκολο ή ακόμα και αδύνατο να διαχειριστεί κανείς τους κινδύνους στον κυβερνοχώρο. Το ISO/IEC 27001 βοηθά τους οργανισμούς να συνειδητοποιήσουν τους κινδύνους και να εντοπίσουν και να αντιμετωπίσουν προληπτικά τις αδυναμίες τους προκειμένου να διασφαλίσουν τα δεδομένα που κατέχουν ή διαχειρίζονται. Ένα ΣΔΑΠ που εφαρμόζεται σύμφωνα με αυτό το πρότυπο είναι ένα εργαλείο για τη διαχείριση κινδύνων, την ανθεκτικότητα στον κυβερνοχώρο και τη λειτουργική αριστεία.

Η τρέχουσα έκδοση του προτύπου είναι η ISO/IEC 27001:2022 [22], η οποία ανακοινώθηκε πρόσφατα (πριν ένα χρόνο περίπου) για να αντικαταστήσει την έκδοση ISO/IEC 27001:2013 [24]. Συμμόρφωση (conformity) με το ISO/IEC 27001:2022 σημαίνει ότι ένας οργανισμός έχει θέσει σε εφαρμογή ένα ΣΔΑΠ το οποίο σέβεται όλες τις απαιτήσεις και τις βέλτιστες πρακτικές και αρχές που κατοχυρώνονται σε αυτό το πρότυπο. Το ISO/IEC 27001:2022 περιλαμβάνει 93 σημεία ελέγχου που αφορούν τις επιχειρησιακές λειτουργίες, το ανθρώπινο δυναμικό, τη φυσική ασφάλεια και την τεχνολογική ασφάλεια. Οι έλεγχοι αυτοί

εφαρμόζονται στο πλαίσιο της εφαρμογής διεργασιών για τη διαχείριση της επικινδυνότητας. Οδηγίες για τη διαχείριση της επικινδυνότητας παρέχονται στο πρότυπο ISO/IEC 27005:2018 [25] το οποίο υποστηρίζει τις γενικές έννοιες του προτύπου ISO/IEC 27001:2022 και είναι σχεδιασμένο για να υποβοηθά την ικανοποιητική υλοποίηση ενός ΣΔΑΠ. Εκτενής αναφορά στο πρότυπο ISO/IEC 27005:2015 θα πραγματοποιηθεί στην επόμενη ενότητα που αφορά την διαχείριση της διακινδύνευσης, τα διάφορα στάδια της και τις τεχνικές αυτών.

3. Η διαχείριση της διακινδύνευσης

3.1. Βασικοί ορισμοί

Διακινδύνευση ή επικινδυνότητα (risk) είναι η επίδραση της αβεβαιότητας στην επίτευξη των στόχων.

Στόχος (objective) είναι ένα αποτέλεσμα που επιθυμούμε να επιτευχθεί.

Διαχείριση της διακινδύνευσης (risk management) είναι οι συντονισμένες ενέργειες για την καθοδήγηση και τον έλεγχο ενός οργανισμού αναφορικά με την διακινδύνευση.

Η διεργασία της διαχείρισης της διακινδύνευσης (risk management process) είναι η συστηματική εφαρμογή πολιτικών, διαδικασιών και πρακτικών στις δραστηριότητες της επικοινωνίας, διαβούλευσης, καθορισμού πλαισίου και εντοπισμού, ανάλυσης, αξιολόγησης, αντιμετώπισης, παρακολούθησης και επανεξέτασης της διακινδύνευσης [2].

3.2. Η διαχείριση της διακινδύνευσης και το πρότυπο ISO 31000

Όλοι οι οργανισμοί, ανεξαρτήτως του τύπου, του μεγέθους, της θέσης τους και του αντικειμένου τους, αντιμετωπίζουν μια σειρά από κινδύνους που μπορεί να επηρεάσουν την επίτευξη των στόχων τους. Οι στόχοι αυτοί μπορεί να σχετίζονται με διάφορες δραστηριότητες του οργανισμού, δηλαδή, από τις στρατηγικές πρωτοβουλίες μέχρι τις λειτουργίες, τις διαδικασίες και τα έργα του οργανισμού. Επίσης, οι στόχοι μπορεί να έχουν κοινωνικά, περιβαλλοντικά, και τεχνολογικά αποτελέσματα καθώς και αποτελέσματα που αφορούν την ασφάλεια, να μετριούνται με εμπορικά και οικονομικά μέτρα και να έχουν αντίκτυπο κοινωνικό, πολιτιστικό, πολιτικό καθώς και στην φήμη του οργανισμού.

Όλες οι δραστηριότητες ενός οργανισμού εμπεριέχουν κινδύνους που πρέπει ο οργανισμός να διαχειριστεί. Η διαδικασία της διαχείρισης διακινδύνευσης (risk management) βοηθά στη λήψη αποφάσεων λαμβάνοντας υπόψη την αβεβαιότητα και την πιθανότητα για μελλοντικά γεγονότα ή περιστάσεις (σκόπιμα ή ακούσια) και

τις επιπτώσεις τους στους συμφωνημένους στόχους του οργανισμού. Η ενσωμάτωση της διαχείρισης διακινδύνευσης βασίζεται στην κατανόηση των οργανωτικών δομών και του πλαισίου λειτουργίας του οργανισμού. Οι δομές διαφέρουν ανάλογα με τον σκοπό, τους στόχους και την πολυπλοκότητα του οργανισμού. Η διαχείριση της διακινδύνευσης γίνεται σε κάθε τμήμα της δομής του οργανισμού. Όλοι σε έναν οργανισμό έχουν την ευθύνη για τη διαχείριση της διακινδύνευσης. Η διακυβέρνηση καθοδηγεί την πορεία του οργανισμού, τις εξωτερικές και εσωτερικές του σχέσεις και τους κανόνες, τις διαδικασίες και τις πρακτικές που απαιτούνται για την επίτευξη του σκοπού του. Οι δομές διαχείρισης μεταφράζουν την κατεύθυνση της διακυβέρνησης στη στρατηγική και τους σχετικούς στόχους που απαιτούνται για την επίτευξη των επιθυμητών επιπέδων βιώσιμης απόδοσης και μακροπρόθεσμης βιωσιμότητας. Ο καθορισμός της ευθύνης διαχείρισης κινδύνου και των ρόλων εποπτείας εντός ενός οργανισμού αποτελούν αναπόσπαστα μέρη της διακυβέρνησης του οργανισμού. Η ενσωμάτωση της διαχείρισης κινδύνου σε έναν οργανισμό είναι μια δυναμική και επαναλαμβανόμενη διαδικασία και θα πρέπει να προσαρμόζεται στις ανάγκες και την κουλτούρα του οργανισμού. Η διαχείριση επικινδυνότητας πρέπει να είναι μέρος και όχι ξεχωριστή από τον οργανωτικό σκοπό, τη διακυβέρνηση, την ηγεσία και τη δέσμευση, τη στρατηγική, τους στόχους και τις λειτουργίες. Η διαδικασία διαχείρισης επικινδυνότητας πρέπει να αποτελεί αναπόσπαστο μέρος της διαχείρισης και της λήψης αποφάσεων και να ενσωματώνεται στη δομή, τις λειτουργίες και τις διαδικασίες του οργανισμού. Μπορεί να εφαρμοστεί σε στρατηγικό, επιχειρησιακό, πρόγραμμα ή επίπεδο έργου.

Αν και η διαδικασία διαχείρισης επικινδυνότητας παρουσιάζεται συχνά ως διαδοχική, στην πράξη είναι επαναληπτική και περιλαμβάνει την εφαρμογή λογικών και συστηματικών μεθόδων για την:

- επικοινωνία και διαβούλευση καθ’ όλη τη διάρκεια της,
- καθιέρωση του πλαισίου για τον εντοπισμό, την ανάλυση, την αξιολόγηση, την αντιμετώπιση του κινδύνου που σχετίζεται με οποιαδήποτε δραστηριότητα, διαδικασία, λειτουργία ή προϊόν,
- παρακολούθηση και επανεξέταση των κινδύνων,

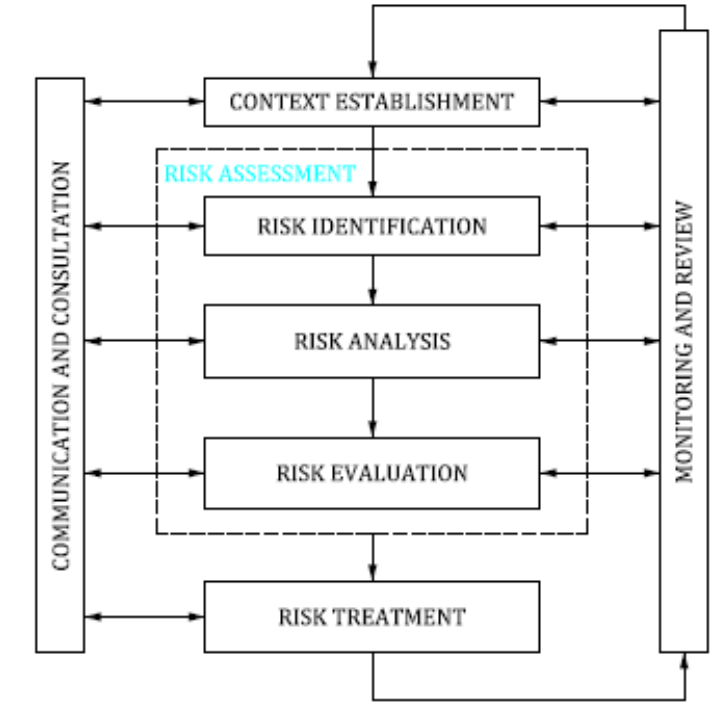
- αναφορά και καταγραφή των αποτελεσμάτων κατάλληλα.

Το διεθνές πρότυπο ISO 31000:2018 [26] παρέχει οδηγίες για το πώς ένας οργανισμός μπορεί να ενσωματώσει τη λήψη αποφάσεων που βασίζεται στη διακινδύνευση, στη διακυβέρνηση, τον σχεδιασμό, τη διαχείριση, την πολιτική, τις αξίες και την κουλτούρα του. Είναι ένα ανοιχτό σύστημα που βασίζεται σε αρχές, που σημαίνει ότι δίνει τη δυνατότητα στους οργανισμούς να εφαρμόζουν τις αρχές του προτύπου στο οργανωτικό τους πλαίσιο. Βοηθάει τους οργανισμούς να αναπτύξουν μια στρατηγική διαχείρισης επικινδυνότητας για τον αποτελεσματικό εντοπισμό και τον μετριασμό των κινδύνων, ενισχύοντας έτσι την πιθανότητα επίτευξης των στόχων τους και αύξησης της προστασίας των περιουσιακών τους στοιχείων. Ο πρωταρχικός στόχος του προτύπου είναι να αναπτύξει στους οργανισμούς μια κουλτούρα διαχείρισης της διακινδύνευσης, όπου οι εργαζόμενοι και τα ενδιαφερόμενα μέρη να γνωρίζουν τη σημασία της παρακολούθησης και της διαχείρισης του κινδύνου. Η εφαρμογή του προτύπου ISO 31000:2018 βοηθά επίσης τους οργανισμούς να αναγνωρίσουν τόσο τις θετικές ευκαιρίες όσο και τις και αρνητικές συνέπειες που συνδέονται με την επικινδυνότητα και επιτρέπει πιο ενημερωμένη, και συνεπώς πιο αποτελεσματική, λήψη αποφάσεων στην δέσμευση και κατανομή των πόρων. Επιπρόσθετα, αποτελεί ένα ενεργό συστατικό για τη βελτίωση της διακυβέρνησης και, τελικά, της απόδοσης ενός οργανισμού.

Στην Εικόνα 9 βλέπουμε τη διαδικασία της διαχείρισης της διακινδύνευσης σύμφωνα με το πρότυπο ISO 31000:2018 όπως παρουσιάζεται στο πρότυπο ISO/IEC 27005:2018 [25] (χρησιμοποιούμε το ISO/IEC 27005:2018 προκειμένου να το αντιπαραβάλουμε με το ISO 31000:2018 καθώς το πρότυπο ISO/IEC 27005:2018 έχει υιοθετήσει το γενικό πρότυπο ISO 31000:2018 για τη διαχείριση της διακινδύνευσης στην ασφάλεια πληροφοριών) το οποίο περιλαμβάνει τα εξής:

Επικοινωνία και διαβούλευση (communication and consultation): Σκοπός της επικοινωνίας και της διαβούλευσης είναι να βοηθήσει τα ενδιαφερόμενα μέρη να κατανοήσουν την επικινδυνότητα, τη βάση στην οποία λαμβάνονται οι αποφάσεις και τους λόγους για τους οποίους απαιτούνται συγκεκριμένες ενέργειες. Η επικοινωνία επιδιώκει να προωθήσει την ευαισθητοποίηση και την κατανόηση της

επικινδυνότητας ενώ η διαβούλευση περιλαμβάνει τη λήψη ανατροφοδότησης και πληροφοριών για την υποστήριξη της λήψης αποφάσεων. Ο στενός συντονισμός μεταξύ των δύο θα πρέπει να διευκολύνει την πραγματική, έγκαιρη, σχετική, ακριβή και κατανοητή ανταλλαγή πληροφοριών, λαμβάνοντας υπόψη την εμπιστευτικότητα και την ακεραιότητα των πληροφοριών καθώς και τα δικαιώματα ιδιωτικής ζωής των ατόμων.



Εικόνα 9 Η διαδικασία διαχείρισης της διακινδύνευσης σύμφωνα με το πρότυπο ISO 31000:2018

Καθορισμός πεδίου εφαρμογής (content establishment): Ο σκοπός του καθορισμού του πεδίου εφαρμογής, του πλαισίου και των κριτηρίων είναι η προσαρμογή της διαδικασίας διαχείρισης διακινδύνευσης, επιτρέποντας την αποτελεσματική αξιολόγηση της διακινδύνευσης και την κατάλληλη αντιμετώπιση της. Το πεδίο εφαρμογής, το πλαίσιο και τα κριτήρια περιλαμβάνουν τον καθορισμό του εύρους της διαδικασίας και την κατανόηση του εξωτερικού και εσωτερικού πλαισίου.

Εκτίμηση διακινδύνευσης (risk assessment): Η εκτίμηση διακινδύνευσης είναι η συνολική διαδικασία αναγνώρισης, ανάλυσης και αξιολόγησης της διακινδύνευσης.

Η εκτίμηση της διακινδύνευσης θα πρέπει να διεξάγεται συστηματικά, επαναληπτικά και συλλογικά, βασιζόμενη στις γνώσεις και τις απόψεις των ενδιαφερομένων. Θα πρέπει να χρησιμοποιεί τις καλύτερες διαθέσιμες πληροφορίες, συμπληρωμένες με περαιτέρω έρευνα, όπως απαιτείται.

Αντιμετώπιση διακινδύνευσης (risk treatment): Ο σκοπός της αντιμετώπισης της διακινδύνευσης είναι η επιλογή και η εφαρμογή διαφόρων δυνατοτήτων για την αντιμετώπιση της διακινδύνευσης η οποία περιλαμβάνει:

- τη διαμόρφωση και την επιλογή δυνατοτήτων για την αντιμετώπιση της διακινδύνευσης,
- τον προγραμματισμό και την εφαρμογή της επιλογής αντιμετώπισης της διακινδύνευσης,
- την αξιολόγηση της αποτελεσματικότητας αυτής της επιλογής αντιμετώπισης της διακινδύνευσης,
- την απόφαση του κατά πόσο η εναπομένουσα διακινδύνευση είναι αποδεκτή, και
- εάν δεν είναι αποδεκτή, τη λήψη επιπρόσθετης αντιμετώπισης.

Παρακολούθηση και αναθεώρηση (monitoring and review): σκοπός της παρακολούθησης και της αναθεώρησης είναι να διασφαλίσει και να βελτιώσει την ποιότητα και την αποτελεσματικότητα του σχεδιασμού, της υλοποίησης και των αποτελεσμάτων. Η συνεχής παρακολούθηση και η περιοδική επανεξέταση της διαδικασίας διαχείρισης κινδύνου και των αποτελεσμάτων της θα πρέπει να αποτελούν προγραμματισμένο μέρος της διαδικασίας διαχείρισης κινδύνου, με σαφώς καθορισμένες ευθύνες. Η παρακολούθηση και η επανεξέταση θα πρέπει να πραγματοποιούνται σε όλα τα στάδια της διαδικασίας. Περιλαμβάνουν τον σχεδιασμό, τη συλλογή και την ανάλυση πληροφοριών, την καταγραφή αποτελεσμάτων και την παροχή ανατροφοδότησης. Τα αποτελέσματα αυτών θα πρέπει να ενσωματώνονται σε όλες τις δραστηριότητες διαχείρισης, μέτρησης και αναφοράς του οργανισμού.

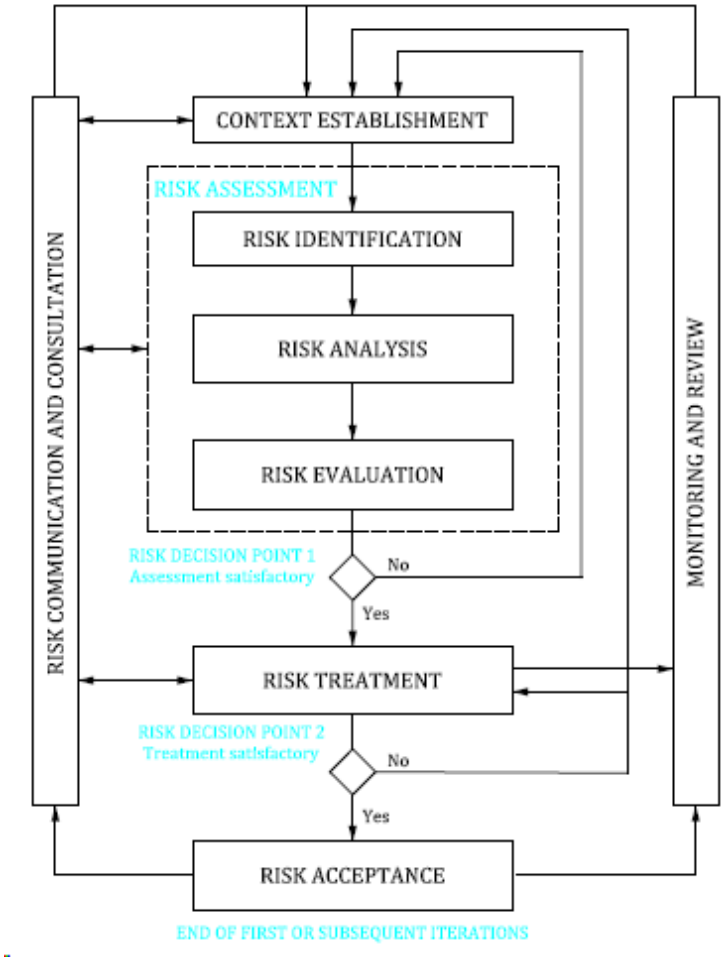
Καταγραφή και αναφορά (Recording and reporting): Η καταγραφή και η αναφορά στοχεύουν:

- στην κοινοποίηση των δραστηριοτήτων και των αποτελεσμάτων διαχείρισης διακινδύνευσης σε ολόκληρο τον οργανισμό,
- στην παροχή πληροφοριών για τη λήψη αποφάσεων,
- στη βελτίωση των δραστηριοτήτων διαχείρισης διακινδύνευσης,
- στην υποβοήθηση της αλληλεπίδρασης με τα ενδιαφερόμενα μέρη, συμπεριλαμβανομένων εκείνων που έχουν ευθύνη και υπευθυνότητα για δραστηριότητες διαχείρισης της επικινδυνότητας.

3.3. Η διαχείριση της διακινδύνευσης και το πρότυπο ISO/IEC 27005

Το πρότυπο ISO/IEC 27005 [25] υποστηρίζει τις γενικές έννοιες που καθορίζονται στο ISO/IEC 27001 και έχει σχεδιαστεί για την υποβοήθηση της ικανοποιητικής εφαρμογής της ασφάλειας πληροφοριών σύμφωνα με την διεργασία διαχείρισης της διακινδύνευσης. Το πρότυπο ISO/IEC 27005 ισχύει για όλους τους τύπους οργανισμών (π.χ. εμπορικές επιχειρήσεις, κρατικούς φορείς, μη κερδοσκοπικούς οργανισμούς) που σκοπεύουν να διαχειριστούν τους κινδύνους που αφορούν την ασφάλεια των πληροφοριών τους.

Στην Εικόνα 9 είδαμε σε υψηλό επίπεδο τη διαδικασία της διαχείρισης της διακινδύνευσης σύμφωνα με το πρότυπο ISO 31000:2018 [26]. Στην Εικόνα 10 βλέπουμε πως η διαδικασία αυτή εφαρμόζεται στην ασφάλεια πληροφοριών, όπως παρουσιάζεται στο πρότυπο ISO/IEC 27005:2018 [25]. Σύμφωνα με αυτήν, η διαδικασία διαχείρισης διακινδύνευσης στην ασφάλεια πληροφοριών μπορεί να είναι επαναληπτική για τη δραστηριότητα εκτίμησης της διακινδύνευσης και αντιμετώπισης της διακινδύνευσης. Η επαναληπτική προσέγγιση δίνει η δυνατότητα της εκτίμησης της διακινδύνευσης εις βάθος και με μεγαλύτερη λεπτομέρεια σε κάθε επανάληψη. Επίσης, παρέχει μια εξισορρόπηση μεταξύ της ελαχιστοποίησης του χρόνου και της προσπάθειας που δαπανάται για τον εντοπισμό των ελέγχων και της διασφάλισης ότι οι υψηλοί κίνδυνοι αξιολογούνται κατάλληλα.



Εικόνα 10 Η διαδικασία διαχείρισης της διακινδύνευσης στην ασφάλεια πληροφοριών σύμφωνα με το πρότυπο ISO/IEC 27005:2018

3.3.1. Καθορισμός Πλαισίου (content establishment)

Αρχικά πραγματοποιείται ο καθορισμός του πλαισίου εφαρμογής της διαχείρισης της διακινδύνευσης ως εξής:

Είσοδος: Η συλλογή όλων των πληροφοριών σχετικά με τον οργανισμό που σχετίζονται με τη δημιουργία πλαισίου διαχείρισης κινδύνου ασφάλειας πληροφοριών.

Ενέργεια: Η δημιουργία του πλαισίου για τη διαχείριση της διακινδύνευσης ασφάλειας πληροφοριών του οργανισμού, το οποίο θα περιλαμβάνει τον καθορισμό των βασικών κριτηρίων που είναι απαραίτητα για τη διαχείριση της επικινδυνότητας, τον καθορισμό του πεδίου εφαρμογής και των ορίων, καθώς επίσης και η δημιουργία

ενός κατάλληλου συστήματος που θα διαχειρίζεται την διαδικασία διαχείρισης διακινδύνευσης.

Έξοδος: Ο προσδιορισμός των βασικών κριτηρίων, το πεδίο εφαρμογής και τα όρια και η οργάνωση για τη διαδικασία διαχείρισης διακινδύνευσης ασφάλειας πληροφοριών.

Είναι σημαντικό σε αυτό το στάδιο να καθοριστεί ο σκοπός του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ), καθώς αυτός επηρεάζει τη συνολική διαδικασία και ειδικότερα τον καθορισμό του πλαισίου. Ο σκοπός αυτός μπορεί να αφορά

- την ανάπτυξη και υποστήριξη ενός ΣΔΑΠ,
- τη νομική συμμόρφωση και τα αποδεικτικά στοιχεία που χρήζουν επιμέλειας,
- την προετοιμασία ενός σχεδίου επιχειρηματικής συνέχειας,
- την προετοιμασία ενός σχεδίου αντιμετώπισης περιστατικών· και
- την περιγραφή των απαιτήσεων ασφάλειας πληροφοριών για ένα προϊόν, μια υπηρεσία ή έναν μηχανισμό.

Ανάλογα με τον σκοπό και τους στόχους του ΣΔΑΠ, η προσέγγιση της διαχείρισης επικινδυνότητας που θα επιλεγεί θα πρέπει να λαμβάνει υπόψη της βασικά κριτήρια που αφορούν

- την αξιολόγηση της επικινδυνότητας (risk evaluation criteria)
- τη επίπτωση της επικινδυνότητας (risk impact criteria) και
- την αποδοχή της επικινδυνότητας (risk acceptance criteria).

Επιπρόσθετα, ο οργανισμός θα πρέπει να αξιολογήσει διαθέτει τους απαραίτητους πόρους για:

- τη διενέργεια εκτίμησης διακινδύνευσης και την κατάρτιση σχέδιο αντιμετώπισης της διακινδύνευσης,
- τον καθορισμό και την εφαρμογή πολιτικών και διαδικασιών, καθώς και την εφαρμογή των επιλεγμένων ελέγχων,
- την παρακολούθηση των ελέγχων, και

- την παρακολούθηση της διαδικασίας διαχείρισης επικινδυνότητας ασφάλειας πληροφοριών.

Για τον καθορισμό των κριτηρίων αξιολόγησης της διακινδύνευσης θα πρέπει να ληφθούν υπόψη:

- η στρατηγική αξία της διαδικασίας επιχειρηματικής πληροφόρησης,
- η κρισιμότητα των στοιχείων ενεργητικού που θα συμπεριληφθούν,
- η λειτουργική και επιχειρηματική σημασία της διαθεσιμότητας, της εμπιστευτικότητας και της ακεραιότητας, και
- οι προσδοκίες και οι αντιλήψεις των ενδιαφερομένων και αρνητικές συνέπειες για την καλή θέληση και τη φήμη του οργανισμού.

Τα κριτήρια επίπτωσης της διακινδύνευσης καθορίζονται ανάλογα με το βαθμό της καταστροφής ή του κόστους που θα προκαλέσει στον οργανισμό κάποιο γεγονός ασφάλειας πληροφοριών. Για τον καθορισμό τους θα πρέπει να λαμβάνονται υπόψη:

- το επίπεδο ταξινόμησης του επηρεαζόμενου περιουσιακού στοιχείου πληροφοριών,
- παραβιάσεις στην ασφάλεια των πληροφοριών (π.χ. απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας),
- περιορισμός δραστηριοτήτων (εσωτερικών ή τρίτων μερών),
- απώλεια επιχειρηματικής και οικονομικής αξίας,
- διακοπή σχεδίων και προθεσμιών, και
- καταστροφή της φήμης του οργανισμού.

Τα κριτήρια αποδοχής της διακινδύνευσης εξαρτώνται από τις πολιτικές, τους στόχους και τα συμφέροντα των ενδιαφερομένων του οργανισμού. Κάθε οργανισμός ορίζει τα δικά του επίπεδα αποδοχής. Για τον καθορισμό των κριτηρίων θα πρέπει να λαμβάνονται υπόψη τα εξής:

- Τα κριτήρια αποδοχής διακινδύνευσης μπορεί να περιλαμβάνουν πολλαπλά όρια, με ένα επιθυμητό επίπεδο διακινδύνευσης, αλλά με την πρόβλεψη για τα ανώτερα στελέχη να αποδέχονται τη διακινδύνευση πάνω από αυτό το επίπεδο κάτω από καθορισμένες συνθήκες.

- Τα κριτήρια αποδοχής διακινδύνευσης μπορούν να εκφραστούν ως το λόγος του εκτιμώμενου κέρδους (ή άλλου επιχειρηματικού οφέλους) προς την εκτιμώμενη διακινδύνευση.
- Διαφορετικά κριτήρια αποδοχής διακινδύνευσης μπορούν να ισχύουν για διαφορετικές κατηγορίες διακινδύνευσης.
- Τα κριτήρια αποδοχής διακινδύνευσης μπορεί να περιλαμβάνουν απαιτήσεις για μελλοντική πρόσθετη αντιμετώπιση, για παράδειγμα π.χ. η διακινδύνευση μπορεί να γίνει αποδεκτή εάν υπάρχει έγκριση και δέσμευση για λήψη μέτρων για τη μείωσή της σε αποδεκτό επίπεδο εντός μιας καθορισμένης χρονικής περιόδου.

Επίσης θα πρέπει να ληφθούν υπόψη επιχειρηματικά κριτήρια, λειτουργίες, τεχνολογία, χρηματοδότηση καθώς και κοινωνικοί και ανθρωπιστικοί παράγοντες.

Για τον καθορισμό του σκοπού και των ορίων της διαδικασίας διαχείρισης διακινδύνευσης ασφάλειας πληροφοριών, θα πρέπει να πραγματοποιηθεί μελέτη του οργανισμού, να καταγραφούν οι περιορισμοί που επηρεάζουν τον οργανισμό και τον σκοπό του οργανισμού.

3.3.2. Εκτίμηση διακινδύνευσης (risk assessment)

Ακολουθεί η εκτίμηση της διακινδύνευσης η οποία αποτελείται από τα στάδια της αναγνώρισης (identification), της ανάλυσης (analysis) και της αξιολόγησης (evaluation) της διακινδύνευσης. Αν η πληροφορία που παρέχει είναι επαρκής για τον αποτελεσματικό προσδιορισμό των ενεργειών που απαιτούνται για την αντιμετώπιση της διακινδύνευσης σε αποδεκτό επίπεδο, τότε η εργασία έχει ολοκληρωθεί και ακολουθεί το στάδιο της αντιμετώπιση της διακινδύνευσης. Διαφορετικά, πραγματοποιείται μια επανάληψη της εκτίμησης της διακινδύνευσης με αναθεωρημένο πλαίσιο (π.χ. κριτήρια αξιολόγησης, κριτήρια αποδοχής ή κριτήρια επιπτώσεων διακινδύνευσης) (βλ. Εικόνα 9, Σημείο απόφασης κινδύνου 1).

Είσοδος Τα βασικά κριτήρια, το πλαίσιο και τα όρια και η οργάνωση για τη διαδικασία διαχείρισης διακινδύνευσης ασφάλειας πληροφοριών.

Ενέργεια: Προσδιορισμός της επικινδυνότητας, ποσοτικοποίηση ή ποιοτική περιγραφή αυτής και διάταξη της σε σχέση με κριτήρια αξιολόγησης επικινδυνότητας και στόχους του οργανισμού.

Έξοδος: Κατάλογος κινδύνων με προτεραιότητα σύμφωνα με κριτήρια αξιολόγησης διακινδύνευσης του οργανισμού.

Για την εκτίμηση της διακινδύνευσης μπορεί να ακολουθηθεί μια υψηλού επιπέδου προσέγγιση ή μια λεπτομερής προσέγγιση. Περιγράφουμε συνοπτικά τα στάδια στις ενότητες που ακολουθούν ενώ αναλυτικά η διαδικασία καθώς και οι πιο χαρακτηριστικές τεχνικές για κάθε στάδιο περιγράφονται στα επόμενα κεφάλαια.

3.3.2.1. Αναγνώριση διακινδύνευσης (risk identification)

Ο σκοπός της αναγνώρισης της διακινδύνευσης είναι να προσδιορίσει τι μπορεί να συμβεί που να προκαλέσει μια πιθανή απώλεια, καθώς επίσης πώς, πού και γιατί μπορεί να προκληθεί αυτή η απώλεια. Στη διαδικασία αυτή θα πρέπει να λαμβάνονται υπόψη κίνδυνοι που η πηγή τους βρίσκεται υπό τον έλεγχο του οργανισμού, παρόλο που η πηγή ή η αιτία του κινδύνου ίσως να μην είναι προφανής.

Η αναγνώριση της διακινδύνευσης περιλαμβάνει τα αγαθά του οργανισμού, τις απειλές, τους ελέγχους, τα τρωτά σημεία καθώς επίσης και τις συνέπειες που μπορεί να προκληθούν. Τελική έξοδος της διαδικασίας είναι ένας κατάλογος από πιθανά συμβάντα με τις συνέπειες αυτών στα αγαθά και στις επιχειρηματικές διεργασίες του οργανισμού.

Αγαθά: Ένα αγαθό ή περιουσιακό στοιχείο (asset) είναι οτιδήποτε έχει αξία για τον οργανισμό και, ως εκ τούτου, απαιτεί προστασία. Για τον προσδιορισμό των περιουσιακών στοιχείων, θα πρέπει να ληφθεί υπόψη ότι ένα πληροφοριακό σύστημα αποτελείται όχι μόνο από υλικό αλλά και από λογισμικό.

Η αναγνώριση περιουσιακών στοιχείων θα πρέπει να εκτελείται σε κατάλληλο επίπεδο λεπτομέρειας που παρέχει επαρκείς πληροφορίες για την εκτίμηση της επικινδυνότητας. Το επίπεδο λεπτομέρειας που χρησιμοποιείται για την αναγνώριση των αγαθών επηρεάζει τη συνολική ποσότητα πληροφοριών που συλλέγονται κατά

την αξιολόγηση κινδύνου. Το επίπεδο μπορεί να βελτιωθεί σε περαιτέρω επαναλήψεις της αξιολόγησης κινδύνου.

Για κάθε περιουσιακό στοιχείο του οργανισμού θα πρέπει να ορίζεται ένας ιδιοκτήτης ο οποίος θα έχει την ευθύνη και θα λογοδοτεί για το περιουσιακό στοιχείο. Μπορεί να μην έχει δικαιώματα ιδιοκτησίας, όμως έχει την ευθύνη για την παραγωγή, την ανάπτυξη, τη συντήρηση, τη χρήση και την ασφάλειά του περιουσιακού στοιχείου. Ο ιδιοκτήτης ενός περιουσιακού στοιχείου είναι συχνά το πιο κατάλληλο άτομο για να καθορίσει την αξία του περιουσιακού στοιχείου για τον οργανισμό.

Τα αγαθά ενός οργανισμού διακρίνονται σε κύρια και υποστηρικτικά. Κύρια αγαθά είναι οι επιχειρηματικές διαδικασίες και οι δραστηριότητες, και οι πληροφορίες (τα δεδομένα). Υποστηρικτικά αγαθά (που βασίζονται στα κύρια αγαθά) είναι το υλικό, το λογισμικό, το δίκτυο, το προσωπικό, οι εγκαταστάσεις και η δομή του οργανισμού. Περισσότερα στοιχεία είναι διαθέσιμα στο Παράρτημα Β του [25].

Απειλές: Μια απειλή έχει τη δυνατότητα να βλάψει τα αγαθά ενός οργανισμού τις πληροφορίες, τις διαδικασίες και τα συστήματα και, επομένως, τον ίδιο τον οργανισμό. Οι απειλές μπορεί να είναι φυσικής ή ανθρώπινης προέλευσης και μπορεί να είναι τυχαίες ή εσκεμμένες. Θα πρέπει να προσδιορίζονται τόσο οι τυχαίες όσο και οι εσκεμμένες πηγές απειλής. Μια απειλή μπορεί να προκύψει από μέσα ή έξω από τον οργανισμό. Οι απειλές πρέπει να προσδιορίζονται γενικά και ανά είδος (π.χ. μη εξουσιοδοτημένες ενέργειες, σωματικές βλάβες, τεχνικές βλάβες). Στη συνέχεια, όπου ενδείκνυται, προσδιορίζονται μεμονωμένες απειλές εντός της γενικής κατηγορίας. Αυτό σημαίνει ότι δεν παραβλέπεται καμία απειλή, συμπεριλαμβανομένων των απροσδόκητων, αλλά ο όγκος της εργασίας που απαιτείται είναι περιορισμένος.

Στο Παράρτημα Γ του [25] δίνονται παραδείγματα εσκεμμένων απειλών για τις πληροφορίες (δεδομένα) ενός οργανισμού, τυχαίων απειλών που οφείλονται στον ανθρώπινο παράγοντα και φυσικών (περιβαλλοντικών) απειλών που δεν οφείλονται στον ανθρώπινο παράγοντα.

Έλεγχοι: Οι έλεγχοι πρέπει να είναι σύμφωνοι με τα σχέδια εφαρμογής αντιμετώπισης επικινδυνότητας, ώστε να αποφευχθεί η περιττή εργασία ή το κόστος, π.χ. λόγω διπλασιασμού των ελέγχων. Επιπλέον, κατά τον εντοπισμό των υφιστάμενων ελέγχων, θα πρέπει να διασφαλιστεί ότι οι έλεγχοι λειτουργούν σωστά. Εάν ένα στοιχείο ελέγχου δεν λειτουργεί όπως αναμένεται, αυτό μπορεί να προκαλέσει ευπάθειες. Αν ένας υφιστάμενος ή προγραμματισμένος έλεγχος αποτυγχάνει σε λειτουργία, απαιτούνται συμπληρωματικοί έλεγχοι για την αποτελεσματική αντιμετώπιση της επικινδυνότητας.

Για τον προσδιορισμό υφιστάμενων ή προγραμματισμένων ελέγχων, χρησιμεύουν οι παρακάτω δραστηριότητες:

- Επανεξέταση των εγγράφων που περιέχουν πληροφορίες σχετικά με τους ελέγχους (για παράδειγμα, σχέδια υλοποίησης αντιμετώπισης επικινδυνότητας). Εάν οι διαδικασίες διαχείρισης της ασφάλειας πληροφοριών είναι καλά τεκμηριωμένες, όλοι οι υφιστάμενοι ή προγραμματισμένοι έλεγχοι και η κατάσταση της εφαρμογής τους πρέπει να είναι διαθέσιμοι.
- Έλεγχος με τα πρόσωπα που είναι υπεύθυνα για την ασφάλεια των πληροφοριών (π.χ. υπεύθυνος ασφάλειας πληροφοριών και υπεύθυνος ασφάλειας συστημάτων πληροφοριών, διευθυντής κτιρίου ή διευθυντής λειτουργιών) και τους χρήστες σχετικά με το ποιοι έλεγχοι εφαρμόζονται πραγματικά για τη διαδικασία πληροφοριών ή το υπό εξέταση σύστημα πληροφοριών.
- Διεξαγωγή επιτόπιας επανεξέτασης των φυσικών ελέγχων, σύγκριση αυτών που εφαρμόζονται με τον κατάλογο των ελέγχων που πρέπει να υπάρχουν και έλεγχος αυτών που εφαρμόζονται ως προς το εάν λειτουργούν σωστά και αποτελεσματικά.
- Επανεξέταση των αναφορών των εξωτερικών επιθεωρήσεων του ΣΔΑΠ.

Τρωτότητες: Η παρουσία μιας ευπάθειας (τρωτότητας) δεν προκαλεί από μόνη της βλάβη. Μπορεί ωστόσο να χρησιμοποιηθεί από απειλές για να προκαλέσουν βλάβη

σε περιουσιακά στοιχεία ή στον οργανισμό. Τρωτά σημεία εντοπίζονται στους παρακάτω τομείς:

- οργάνωση,
- διεργασίες και διαδικασίες,
- ρουτίνες διαχείρισης,
- προσωπικό,
- φυσικό περιβάλλον,
- παραμετροποίηση πληροφοριακών συστημάτων,
- υλικό, λογισμικό, δικτυακός εξοπλισμός,
- εξάρτηση από εξωτερικά μέρη.

Στο Παράρτημα Δ του [25] δίνονται παραδείγματα για ευπάθειες σε διάφορους τομείς ασφάλειας, συμπεριλαμβανομένων παραδειγμάτων απειλών που μπορούν να εκμεταλλευτούν αυτές τις ευπάθειες.

Συνέπειες: Οι συνέπειες αφορούν την απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των αγαθών του οργανισμού. Μια συνέπεια μπορεί να είναι απώλεια αποτελεσματικότητας, δυσμενείς συνθήκες λειτουργίας, απώλεια επιχειρηματικής δραστηριότητας, φήμη, ζημιά κοκ.

Οι οργανισμοί θα πρέπει να προσδιορίζουν τις λειτουργικές συνέπειες των σεναρίων συμβάντων όσον αφορά τα ακόλουθα:

- χρόνος διερεύνησης και επισκευής,
- απώλεια χρόνου εργασίας,
- απώλεια ευκαιριών,
- υγεία και την ασφάλεια,
- οικονομικό κόστος ειδικών δεξιοτήτων για την αποκατάσταση της ζημίας,
- φήμη και καλή θέληση, κ.α.

3.3.2.2. Ανάλυση διακινδύνευσης (risk analysis)

Η ανάλυση διακινδύνευσης μπορεί να πραγματοποιηθεί με διάφορους βαθμούς λεπτομέρειας ανάλογα με την κρισιμότητα των αγαθών, την έκταση των γνωστών τρωτών σημείων και τα προηγούμενα περιστατικά που σχετίζονται με τον οργανισμό.

Μπορεί να είναι ποιοτική ή ποσοτική ή συνδυασμός αυτών, ανάλογα με τις περιστάσεις. Στην πράξη, η ποιοτική ανάλυση χρησιμοποιείται συχνά πρώτα για να ληφθεί μια γενική ένδειξη του επιπέδου επικινδυνότητας και να αποκαλυφθούν οι κύριοι κίνδυνοι. Στη συνέχεια μπορεί να χρειαστεί να γίνει πιο συγκεκριμένη ή ποσοτική ανάλυση για τους κύριους κινδύνους. Σκοπός της διαδικασίας είναι η αποτίμηση των αγαθών και εκτίμηση των επιπτώσεων. Τελική έξοδος είναι ένας κατάλογος με τις εκτιμώμενες συνέπειες των πιθανών σεναρίων (μαζί με την εκτιμώμενη πιθανότητα αυτών) αναφορικά με τα αγαθά και τα κριτήρια των επιπτώσεων.

3.3.2.3. Αξιολόγηση διακινδύνευσης (risk evaluation)

Για την αξιολόγηση της διακινδύνευσης οι οργανισμοί συγκρίνουν τους εκτιμώμενους κινδύνους με τα κριτήρια αξιολόγησης που ορίζονται κατά το στάδιο της δημιουργίας του πλαισίου. Τελική έξοδος είναι ένας κατάλογος των κινδύνων που ιεραρχούνται σύμφωνα με κριτήρια αξιολόγησης επικινδυνότητας σε σχέση με τα σενάρια συμβάντων που οδηγούν σε αυτούς τους κινδύνους.

3.3.3. Αντιμετώπιση διακινδύνευσης (risk treatment)

Η αποτελεσματικότητα της αντιμετώπισης της διακινδύνευσης εξαρτάται από τα αποτελέσματα της εκτίμησης της διακινδύνευσης. Η διαδικασία είναι κυκλική: εκτίμηση της αντιμετώπισης της επικινδυνότητας, απόφαση εάν τα επίπεδα της υπολειπόμενης διακινδύνευσης είναι αποδεκτά, δημιουργία νέας αντιμετώπισης επικινδυνότητας εάν τα επίπεδα διακινδύνευσης δεν είναι αποδεκτά και τέλος αξιολόγηση της αποτελεσματικότητας της νέας αντιμετώπισης. Είναι πιθανό η αντιμετώπιση της επικινδυνότητας να μην οδηγεί αμέσως σε ένα αποδεκτό επίπεδο υπολειπόμενης επικινδυνότητας. Σε αυτήν την περίπτωση, μπορεί να απαιτηθεί μια άλλη επανάληψη της εκτίμησης της επικινδυνότητας με διαφορετικές παραμέτρους πλαισίου (π.χ. εκτίμηση διακινδύνευσης, αποδοχή διακινδύνευσης, ή κριτήρια επιπτώσεων), ακολουθούμενη από περαιτέρω αντιμετώπιση επικινδυνότητας (βλ. Εικόνα 9, Σημείο απόφασης κινδύνου 2).

Είσοδος: Μια λίστα κινδύνων με σειρά προτεραιότητας σύμφωνα με κριτήρια αξιολόγησης κινδύνου σε σχέση με τα σενάρια συμβάντων που οδηγούν σε αυτούς τους κινδύνους.

Ενέργεια: Επιλογή ελέγχων για τη μείωση, τη διατήρηση, την αποφυγή ή τον επιμερισμό των κινδύνων και καθορισμός ενός σχεδίου αντιμετώπισης της επικινδυνότητας.

Έξοδος: Σχέδιο αντιμετώπισης της διακινδύνευσης και υπολειπόμενη επικινδυνότητα σύμφωνα με την απόφαση αποδοχής των διευθυντών του οργανισμού.

3.3.4. Αποδοχή διακινδύνευσης (risk acceptance)

Η δραστηριότητα της αποδοχής της διακινδύνευσης πρέπει να διασφαλίζει ότι η υπολειπόμενη διακινδύνευση γίνεται ρητά αποδεκτή από τους διευθυντές του οργανισμού. Αυτό είναι ιδιαίτερα σημαντικό σε μια κατάσταση όπου η εφαρμογή των ελέγχων παραλείπεται ή αναβάλλεται για παράδειγμα λόγω κόστους.

Είσοδος: Σχέδιο αντιμετώπισης επικινδυνότητας και αξιολόγηση υπολειπόμενου κινδύνου σύμφωνα με την απόφαση αποδοχής των διευθυντών του οργανισμού.

Ενέργεια: Λήψη απόφασης αποδοχής της επικινδυνότητας και των ευθυνών για την απόφαση αυτή, και επίσημη καταγραφή τους.

Έξοδος: Κατάλογος αποδεκτών κινδύνων με αιτιολόγηση για αυτούς που δεν πληρούν τα συνήθη κριτήρια αποδοχής διακινδύνευσης του οργανισμού.

Κάθε οργανισμός θα πρέπει να καθορίζει τα δικά του κριτήρια αποδοχής της διακινδύνευσης λαμβάνοντας υπόψη επιχειρηματικά κριτήρια, λειτουργίες, τεχνολογικά μέσα, οικονομικά στοιχεία καθώς επίσης και κοινωνικούς και ανθρωπιστικούς παράγοντες. Περισσότερα στοιχεία δίνονται στο Παράρτημα Α της πηγής [25].

3.3.5. Παρακολούθηση και αναθεώρηση (monitoring and review)

Καθ’ όλη τη διάρκεια της διαδικασίας διαχείρισης επικινδυνότητας της ασφάλειας πληροφοριών, είναι σημαντικό οι κίνδυνοι και η αντιμετώπισή τους να κοινοποιούνται στα κατάλληλα στελέχη και το επιχειρησιακό προσωπικό του

οργανισμού. Ακόμη και πριν από την αντιμετώπιση της διακινδύνευσης, οι πληροφορίες σχετικά με τους εντοπισμένους κινδύνους μπορεί να είναι πολύ πολύτιμες για τη διαχείριση συμβάντων και μπορούν να βοηθήσουν στη μείωση πιθανών ζημιών. Η επίγνωση των κινδύνων από τους διευθυντές και το προσωπικό, τη φύση των ελέγχων που εφαρμόζονται για τον μετριασμό των κινδύνων και τους τομείς που απασχολούν τον οργανισμό βοηθούν στην αντιμετώπιση περιστατικών και απροσδόκητων συμβάντων με τον πιο αποτελεσματικό τρόπο. Τα λεπτομερή αποτελέσματα κάθε δραστηριότητας της διαδικασίας διαχείρισης επικινδυνότητας στην ασφάλειας πληροφοριών και από τα δύο σημεία λήψης αποφάσεων κινδύνου θα πρέπει να τεκμηριώνονται.

Είσοδος: Όλες οι πληροφορίες που λαμβάνονται από τις δραστηριότητες διαχείρισης επικινδυνότητας.

Ενέργεια: Οι κίνδυνοι και οι παράγοντες τους (π.χ. η αξία των περιουσιακών στοιχείων, οι επιπτώσεις, οι απειλές, τα τρωτά σημεία, η πιθανότητα εμφάνισης τους) θα πρέπει να παρακολουθούνται και να επανεξετάζονται για τον εντοπισμό τυχόν αλλαγών στο πλαίσιο του οργανισμού σε πρώιμο στάδιο και για τη διατήρηση μιας επισκόπησης της πλήρους εικόνας της διακινδύνευσης. Επίσης, η διαδικασία διαχείρισης διακινδύνευσης για την ασφάλεια των πληροφοριών θα πρέπει να παρακολουθείται, να επανεξετάζεται και να βελτιώνεται διαρκώς όπως απαιτείται και ενδείκνυται.

Έξοδος: Διαρκής ευθυγράμμιση της διαχείρισης της διακινδύνευσης με τους επιχειρηματικούς στόχους του οργανισμού και με τα κριτήρια αποδοχής της διακινδύνευσης.

3.3.6. Επικοινωνία και διαβούλευση (risk communication and consulting)

Όλες οι πληροφορίες που αφορούν την διακινδύνευση θα πρέπει να διαμοιράζονται μεταξύ του υπευθύνου λήψης αποφάσεων και όλων των ενδιαφερομένων. Η αποτελεσματική επικοινωνία μεταξύ αυτών είναι σημαντική, καθώς μπορεί να έχει σημαντικό αντίκτυπο στις αποφάσεις που πρέπει να ληφθούν. Η επικοινωνία διασφαλίζει ότι οι υπεύθυνοι για την εφαρμογή της διαχείρισης επικινδυνότητας και

όσοι έχουν κεκτημένα συμφέροντα κατανοούν τη βάση στην οποία λαμβάνονται οι αποφάσεις και γιατί απαιτούνται συγκεκριμένες ενέργειες.

Είσοδος: Όλες οι πληροφορίες που λαμβάνονται από τις δραστηριότητες διαχείρισης επικινδυνότητας.

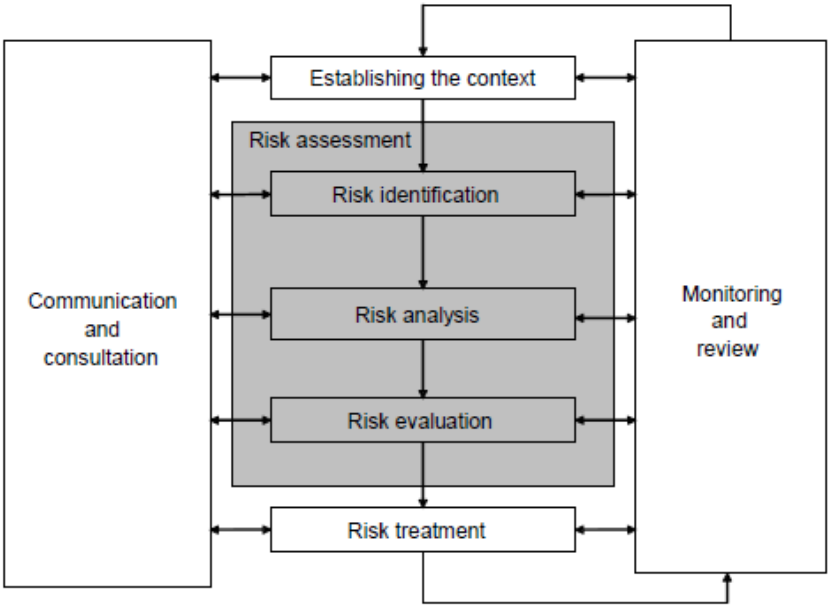
Ενέργεια: Ανταλλαγή πληροφοριών μεταξύ υπευθύνου λήψης αποφάσεων και όλων των ενδιαφερομένων.

Έξοδος: Διαρκής κατανόηση της διαδικασίας και των αποτελεσμάτων διαχείρισης διακινδύνευσης ασφάλειας πληροφοριών του οργανισμού.

4. Η εκτίμηση της διακινδύνευσης

4.1. Η εκτίμηση της διακινδύνευσης και το πρότυπο ISO/IEC 31010

Η εκτίμηση της διακινδύνευσης (risk assessment) αποτελεί τμήμα της διαδικασίας της διαχείρισης διακινδύνευσης (Εικόνα 11, Πηγή:[27]). Πρόκειται για μια δομημένη διαδικασία που προσδιορίζει πώς μπορεί να επηρεαστούν οι στόχοι και αναλύει τους κινδύνους ως προς την πιθανότητα να εμφανιστούν και τις συνέπειες τους, καθώς και τον τρόπο αντιμετώπισης της εμφάνισης τους.



Εικόνα 11 Η συνεισφορά της εκτίμησης διακινδύνευσης στη διαδικασία διαχείρισης διακινδύνευσης

Ο σκοπός της εκτίμησης της διακινδύνευσης είναι η κατανόηση της φύσης του κινδύνου και των χαρακτηριστικών του, συμπεριλαμβανομένου, κατά περίπτωση, του επιπέδου κινδύνου. Η εκτίμηση της διακινδύνευσης περιλαμβάνει μια λεπτομερή εξέταση των αβεβαιοτήτων, των πηγών κινδύνου, των συνεπειών, της πιθανότητας, των γεγονότων, των σεναρίων, των ελέγχων και της αποτελεσματικότητάς τους. Ένα γεγονός μπορεί να έχει πολλαπλές αιτίες και συνέπειες και μπορεί να επηρεάσει πολλούς στόχους. Έτσι, η εκτίμηση της διακινδύνευσης προσπαθεί να απαντήσει στα ακόλουθα θεμελιώδη ερωτήματα:

- τι μπορεί να συμβεί και γιατί;
- ποιες είναι οι συνέπειες;
- ποια είναι η πιθανότητα εμφάνισης;
- υπάρχουν παράγοντες που μετριάζουν τις συνέπειες ή που μειώνουν την πιθανότητα του κινδύνου;

Για την απάντηση των προηγουμένων, η εκτίμηση της διακινδύνευσης πρέπει να λαμβάνει υπόψη παράγοντες όπως:

- την πιθανότητα γεγονότων και συνεπειών,
- τη φύση και το μέγεθος των συνεπειών,
- την πολυπλοκότητα και τη συνδεσιμότητα,
- παράγοντες που σχετίζονται με το χρόνο και την αστάθεια,
- την αποτελεσματικότητα των υφιστάμενων ελέγχων, και
- τα επίπεδα ευαισθησίας και εμπιστοσύνης.

Η εκτίμηση της διακινδύνευσης μπορεί να επηρεαστεί από τυχόν αποκλίσεις απόψεων, προκαταλήψεις, αντιλήψεις για τον κίνδυνο και κρίσεις. Πρόσθετες επιρροές είναι η ποιότητα των πληροφοριών που χρησιμοποιούνται, οι υποθέσεις και οι αποκλεισμοί που έγιναν, τυχόν περιορισμοί των τεχνικών και ο τρόπος εκτέλεσής τους. Αυτές οι επιρροές θα πρέπει να εξετάζονται, να τεκμηριώνονται και να κοινοποιούνται στους υπεύθυνους λήψης αποφάσεων.

Η εκτίμηση της διακινδύνευσης μπορεί να πραγματοποιηθεί με διάφορους βαθμούς λεπτομέρειας και πολυπλοκότητας, ανάλογα με τον σκοπό της ανάλυσης, τη διαθεσιμότητα και την αξιοπιστία των πληροφοριών και τους διαθέσιμους πόρους. Οι τεχνικές ανάλυσης μπορεί να είναι ποιοτικές, ποσοτικές ή συνδυασμός αυτών, ανάλογα με τις περιστάσεις και την προβλεπόμενη χρήση. Τα εξαιρετικά αβέβαια γεγονότα μπορεί να είναι δύσκολο να ποσοτικοποιηθούν. Αυτό μπορεί να είναι ένα ζήτημα κατά την ανάλυση γεγονότων με σοβαρές συνέπειες. Σε τέτοιες περιπτώσεις, η χρήση συνδυασμού τεχνικών παρέχει γενικά μεγαλύτερη προβολή.

Το πρότυπο ISO/IEC 31010:2019 [28], ένα διπλό πρότυπο για το ISO και το IEC, που δημοσιεύτηκε αρχικά το 2009 και αναθεωρήθηκε το 2019, παρέχει οδηγίες για την

επιλογή και την εφαρμογή τεχνικών για τη συστηματική εκτίμηση της διακινδύνευσης καλύπτοντας ένα ευρύ φάσμα περιπτώσεων. Οι τεχνικές αυτές χρησιμοποιούνται για την υποβοήθηση της λήψης αποφάσεων όπου υπάρχει αβεβαιότητα, για την παροχή πληροφοριών σχετικά με συγκεκριμένους κινδύνους αλλά και ως μέρος της διαδικασίας διαχείρισης της διακινδύνευσης. Το έγγραφο παρέχει περιλήψεις μιας σειράς τεχνικών, με αναφορές σε άλλα έγγραφα όπου οι τεχνικές περιγράφονται με περισσότερες λεπτομέρειες. Συγκριτικά με την αρχική έκδοση του 2009, η δεύτερη έκδοση του 2019 παρουσιάζει με περισσότερη λεπτομέρεια τη διαδικασία σχεδιασμού, υλοποίησης, επαλήθευσης και επικύρωσης των τεχνικών αυτών και επίσης περιέχει περισσότερες τεχνικές αλλά και πιο ευρύ πεδίο εφαρμογής τους.

Το πρότυπο IEC 31010:2019 λειτουργεί υποστηρικτικά στο πρότυπο ISO 31000:2018. Στόχος του είναι να παρουσιάσει καλές πρακτικές στην επιλογή και τη χρήση τεχνικών για την εκτίμηση διακινδύνευσης. Είναι γενικού σκοπού έτσι ώστε να μπορεί να παρέχει καθοδήγηση σε πολλούς κλάδους και τύπους συστημάτων και οργανισμών, ενώ ενδέχεται να υπάρχουν πιο συγκεκριμένα πρότυπα προσανατολισμένα και εστιασμένα σε συγκεκριμένα συστήματα από το χώρο της βιομηχανίας που να προτείνουν τεχνικές εκτίμησης της διακινδύνευσης για συγκεκριμένες εφαρμογές.

Οι τεχνικές που περιγράφονται στο πρότυπο ISO/IEC 31010:2019 χρησιμοποιούνται:

- όπου απαιτείται περαιτέρω κατανόηση σχετικά με την ύπαρξη κάποιου κινδύνου ή για την ύπαρξη συγκεκριμένου κινδύνου,
- στο πλαίσιο της λήψης μιας απόφασης, όταν είναι διαθέσιμη μια σειρά επιλογών που η καθεμία εμπεριέχει κίνδυνο, και
- στο πλαίσιο μιας διαδικασίας διαχείρισης κινδύνου που οδηγεί σε ενέργειες για την αντιμετώπιση του κινδύνου.

Οι τεχνικές χρησιμοποιούνται στα στάδια εκτίμησης, εντοπισμού, ανάλυσης και αξιολόγησης της διακινδύνευσης, όπως περιγράφονται στο πρότυπο ISO 31000:2018 και γενικότερα όποτε υπάρχει ανάγκη για κατανόηση της αβεβαιότητα και των επιπτώσεων της. Αν και οι τεχνικές που περιγράφονται μπορούν να χρησιμοποιηθούν σε ένα ευρύ πλαίσιο, η πλειοψηφία τους προέρχεται από τον τεχνικό τομέα για αυτό

και μπορεί να εφαρμοστούν για την εκτίμηση της διακινδύνευσης συνδυαστικά με το πρότυπο ISO/IEC 27001:2013. Ορισμένες τεχνικές είναι παρόμοιες αλλά αναφέρονται με διαφορετικά ονόματα και έχουν διαφορετικές μεθοδολογίες που αντικατοπτρίζουν την ιστορία της ανάπτυξης τους σε διαφορετικούς τομείς. Οι τεχνικές έχουν εξελιχθεί με την πάροδο του χρόνου και συνεχίζουν να εξελίσσονται, και πολλές μπορούν να χρησιμοποιηθούν ευρύτερα πέρα από την αρχική περιοχή εφαρμογής τους. Οι τεχνικές μπορούν να προσαρμοστούν κατάλληλα, να συνδυαστούν και να εφαρμοστούν με νέους τρόπους και να επεκταθούν για να ικανοποιήσουν τρέχουσες και μελλοντικές ανάγκες. Το πρότυπο ISO/IEC 31010:2019 απευθύνεται σε:

- οποιονδήποτε εμπλέκεται στην εκτίμηση ή στη διαχείριση της διακινδύνευσης,
- άτομα που εμπλέκονται στην καθοδήγηση που καθορίζει τον τρόπο εκτίμησης της διακινδύνευσης σε συγκεκριμένα πλαίσια,
- άτομα που καλούνται να λάβουν αποφάσεις όπου υπάρχει αβεβαιότητα, συμπεριλαμβανομένων αυτών που αναθέτουν ή αξιολογούν την εκτίμηση της διακινδύνευσης, αυτών που πρέπει να κατανοήσουν τα αποτελέσματα της εκτίμησης της διακινδύνευσης και των αξιολογήσεων και αυτών που πρέπει να επιλέξουν τεχνικές εκτίμησης διακινδύνευσης για να καλύψουν συγκεκριμένες ανάγκες.

Επίσης, το πρότυπο αυτό είναι χρήσιμο για οργανισμούς που υποχρεούνται να διενεργούν εκτίμηση διακινδύνευσης για λόγους συμμόρφωσης με συγκεκριμένα πρότυπα, όπως το ISO/IEC 27001:2013.

4.2. Υλοποιώντας τη διαδικασία της εκτίμησης της διακινδύνευσης

Η εκτίμηση της διακινδύνευσης αποτελείται από τα ακόλουθα στάδια/βήματα:

- Αναγνώριση διακινδύνευσης
- Ανάλυση διακινδύνευσης (Συνέπεια, Πιθανότητα, Επίπεδο)
- Αποτίμηση διακινδύνευσης

Δίνεται στη συνέχεια μια σύντομη περιγραφή των σταδίων της εκτίμησης διακινδύνευσης. Οι τεχνικές που εφαρμόζονται σε κάθε στάδιο παρουσιάζονται στο Κεφάλαιο 5 ενώ μια τεχνική μπορεί να βρίσκει εφαρμογή σε περισσότερα από ένα στάδια.

4.2.1. Αναγνώριση διακινδύνευσης

Το στάδιο αυτό στοχεύει στον προσδιορισμό του πιθανού, όπου θα πρέπει να λαμβάνεται υπόψη η αβεβαιότητα, από όποια πηγή και να προέρχεται, ανάλογα με το πλαίσιο και το σκοπό της εκτίμησης της διακινδύνευσης.

Οι τεχνικές για τον προσδιορισμό του κινδύνου συνήθως χρησιμοποιούν τη πρότερη γνώση και την εμπειρία των ενδιαφερομένων μερών και των ειδικών. Για την αναγνώριση της διακινδύνευσης θα πρέπει να εξεταστούν ζητήματα όπως:

- Υπάρχει αβεβαιότητα και αν ναι, ποιες μπορεί να είναι οι επιπτώσεις της;
- Ποιες συνθήκες και ποια ζητήματα (απτά ή άυλα) εν δυνάμει θα έχουν μελλοντικές συνέπειες;
- Ποιες πηγές κινδύνου υπάρχουν ή μπορεί να εμφανιστούν;
- Υπάρχουν σημεία ελέγχου και πόσο είναι αποτελεσματικά;
- Ποια γεγονότα, πως, πότε, που και γιατί μπορεί να εμφανιστούν και με ποιες συνέπειες;
- Τι έχει συμβεί στο παρελθόν και πώς αυτό μπορεί εύλογα να σχετίζεται με το μέλλον;
- Ποιες ανθρώπινες απόψεις και ποιοι οργανωτικοί παράγοντες μπορεί να ισχύουν;

Για τον εντοπισμό των πηγών κινδύνου ή πρώιμων προειδοποιήσεων που σηματοδοτούν πιθανές συνέπειες, μπορεί να είναι χρήσιμη η πραγματοποίηση έρευνας και επιθεώρησης. Τα αποτελέσματα του σταδίου της αναγνώρισης της διακινδύνευσης θα πρέπει να καταγράφονται σε μορφή λίστας κινδύνων με γεγονότα, αιτίες και συνέπειες ή χρησιμοποιώντας άλλες κατάλληλες μορφές.

Η περιγραφή των τεχνικών μέσω των οποίων μπορούμε να προσδιορίσουμε τον κίνδυνο, παρουσιάζεται στην Ενότητα 5.1. Όποιες και αν είναι οι τεχνικές που

χρησιμοποιούνται, η διαδικασία του εντοπισμού των κινδύνων θα πρέπει να γίνεται με μεθοδικότητα και επαναληψιμότητα, ώστε να είναι εμπεριστατωμένη και αποτελεσματική. Οι κίνδυνοι θα πρέπει να εντοπίζονται αρκετά έγκαιρα ώστε να επιτρέπεται η πραγματοποίηση ενεργειών. Υπάρχουν ωστόσο και περιπτώσεις που κάποιοι κίνδυνοι δεν μπορούν να εντοπιστούν κατά την αναγνώριση της διακινδύνευσης. Θα πρέπει επομένως να δημιουργηθεί ένας μηχανισμός για αποτύπωση των αναδυόμενων κινδύνων και την αναγνώριση πρώιμων προειδοποιητικών σημείων πιθανής επιτυχίας ή αποτυχίας.

4.2.2. Ανάλυση διακινδύνευσης

Η ανάλυση διακινδύνευσης συνίσταται στον προσδιορισμό των συνεπειών και των πιθανοτήτων τους για εντοπισμένα συμβάντα κινδύνου, λαμβάνοντας υπόψη την παρουσία (ή όχι) και την αποτελεσματικότητα τυχόν υπαρχόντων ελέγχων. Οι συνέπειες και οι πιθανότητές τους στη συνέχεια συνδυάζονται για να καθοριστεί ένα επίπεδο κινδύνου.

Πρέπει να προσδιορίζονται οι παράγοντες που επηρεάζουν τις συνέπειες και την πιθανότητα. Ένα γεγονός μπορεί να έχει πολλαπλές συνέπειες και μπορεί να επηρεάσει πολλούς στόχους. Θα πρέπει να λαμβάνονται υπόψη οι υφιστάμενοι έλεγχοι κινδύνου και η αποτελεσματικότητά τους.

Διάφορες μέθοδοι για αυτές τις αναλύσεις περιγράφονται στο Παράρτημα Β του [25] και μπορεί να απαιτούνται περισσότερες από μία τεχνικές για πολύπλοκες εφαρμογές.

Η ανάλυση διακινδύνευσης συνήθως περιλαμβάνει μια εκτίμηση του εύρους των πιθανών συνεπειών που μπορεί να προκύψουν από ένα γεγονός, μια κατάσταση ή περίσταση, και τις σχετικές πιθανότητες, προκειμένου να μετρηθεί το επίπεδο διακινδύνευσης. Ωστόσο, σε ορισμένες περιπτώσεις, όπου οι συνέπειες είναι πιθανό να είναι ασήμαντες ή η πιθανότητα αναμένεται να είναι εξαιρετικά χαμηλή, μια εκτίμηση παραμέτρου μπορεί να είναι αρκετή για να ληφθεί μια απόφαση. Σε ορισμένες περιπτώσεις, μια συνέπεια μπορεί να προκύψει ως αποτέλεσμα μιας σειράς διαφορετικών γεγονότων ή συνθήκες ή όταν το συγκεκριμένο συμβάν δεν προσδιορίζεται. Στην περίπτωση αυτή, το επίκεντρο της αξιολόγησης κινδύνου είναι

η ανάλυση της σημασίας και της ευπάθειας των στοιχείων του συστήματος με σκοπό τον καθορισμό δράσεων που σχετίζονται με επίπεδα προστασίας ή στρατηγικές ανάκτησης.

Η ποιοτική αξιολόγηση καθορίζει τη συνέπεια, την πιθανότητα και το επίπεδο κινδύνου με επίπεδα σημαντικότητας όπως «υψηλό», «μεσαίο» και «χαμηλό», μπορεί να συνδυάζει συνέπεια και πιθανότητα και αξιολογεί το επίπεδο κινδύνου σε σχέση με ποιοτικά κριτήρια.

Οι ημιποσοτικές μέθοδοι χρησιμοποιούν αριθμητικές κλίμακες αξιολόγησης για τις συνέπειες και τις πιθανότητες και τις συνδυάζουν για να παράγουν ένα επίπεδο κινδύνου χρησιμοποιώντας έναν μαθηματικό τύπο. Οι κλίμακες μπορεί να είναι γραμμικές ή λογαριθμικές ή να έχουν κάποια άλλη σχέση. Οι τύποι που χρησιμοποιούνται μπορεί επίσης να διαφέρουν.

Η ποσοτική ανάλυση εκτιμά τις πρακτικές τιμές για τις συνέπειες και τις πιθανότητες τους και παράγει τιμές του επιπέδου κινδύνου σε συγκεκριμένες μονάδες που ορίζονται κατά την ανάπτυξη του πλαισίου. Η πλήρης ποσοτική ανάλυση μπορεί να μην είναι πάντα δυνατή ή επιθυμητή λόγω ανεπαρκών πληροφοριών για το υπό ανάλυση σύστημα ή δραστηριότητα, έλλειψη δεδομένων, επιρροή ανθρώπινων παραγόντων κ.λ.π. ή επειδή η προσπάθεια ποσοτικής ανάλυσης δεν δικαιολογείται ή απαιτείται. Σε τέτοιες περιπτώσεις, μια συγκριτική ημιποσοτική ή ποιοτική κατάταξη των κινδύνων από ειδικούς, γνώστες στον αντίστοιχο τομέα τους, μπορεί να είναι ακόμα αποτελεσματική.

Σε περιπτώσεις που η ανάλυση είναι ποιοτική, θα πρέπει να υπάρχει σαφής επεξήγηση όλων των χρησιμοποιούμενων όρων και να καταγράφεται η βάση για όλα τα κριτήρια. Ακόμη και όταν έχει πραγματοποιηθεί πλήρης ποσοτικοποίηση, πρέπει να αναγνωριστεί ότι τα επίπεδα κινδύνου που υπολογίζονται είναι εκτιμήσεις. Θα πρέπει να λαμβάνεται μέριμνα ώστε να διασφαλίζεται ότι δεν τους αποδίδεται επίπεδο ακρίβειας που δεν συνάδει με την ακρίβεια των δεδομένων και των μεθόδων που χρησιμοποιούνται.

4.2.3. Αποτίμηση διακινδύνευσης

Η αποτίμηση της διακινδύνευσης αφορά στην επαλήθευση (verification) και στην επικύρωση (validation) των αποτελεσμάτων της ανάλυσης. Η επαλήθευση περιλαμβάνει τον έλεγχο ότι η ανάλυση έγινε σωστά. Η επικύρωση περιλαμβάνει τον έλεγχο ότι έγινε η σωστή ανάλυση για την επίτευξη των απαιτούμενων στόχων. Για ορισμένες περιπτώσεις η επαλήθευση και η επικύρωση μπορεί να περιλαμβάνουν ανεξάρτητες διαδικασίες αναθεώρησης.

Η επικύρωση μπορεί να περιλαμβάνει:

- Έλεγχος της καταλληλότητας της ανάλυσης, αναφορικά με τους δηλωθέντες στόχους.
- Επανεξέταση όλων των κρίσιμων υποθέσεων προκειμένου να διασφαλιστεί ότι είναι αξιόπιστες.
- Έλεγχος ότι χρησιμοποιήθηκαν κατάλληλες μέθοδοι, μοντέλα και δεδομένα.
- Χρήση πολλαπλών μεθόδων, προσεγγίσεων και ανάλυσης ευαισθησίας για δοκιμή και επικύρωση των συμπερασμάτων.

Η επαλήθευση μπορεί να περιλαμβάνει:

- Έλεγχο της εγκυρότητας των μαθηματικών χειρισμών και υπολογισμών.
- Έλεγχο ότι τα αποτελέσματα δεν είναι ευαίσθητα στον τρόπο με τον οποίο εμφανίζονται ή παρουσιάζονται.
- Σύγκριση αποτελεσμάτων με προηγούμενη εμπειρία, όπου υπάρχουν δεδομένα, ή με σύγκριση με αποτελέσματα μετά την εμφάνισή τους.
- Διαπίστωση ότι .τα αποτελέσματα είναι ευαίσθητα στον τρόπο με τον οποίο εμφανίζονται ή παρουσιάζονται τα δεδομένα ή τα αποτελέσματα και για τον προσδιορισμό των παραμέτρων εισόδου που έχουν σημαντική επίδραση στα αποτελέσματα της αξιολόγησης.
- Σύγκριση αποτελεσμάτων με προηγούμενη ή μεταγενέστερη εμπειρία, συμπεριλαμβανομένης της ρητής λήψης ανατροφοδότησης καθώς προχωρά ο χρόνος.

4.3. Επιλογή κατάλληλων τεχνικών για την εκτίμηση της διακινδύνευσης

Η επιλογή της τεχνικής για την εκτίμηση της διακινδύνευσης καθώς και ο τρόπος εφαρμογής της θα πρέπει να προσαρμόζεται ανάλογα με το πλαίσιο και τη χρήση αυτής και να παρέχει τις πληροφορίες εκείνες που χρειάζονται τα ενδιαφερόμενα μέρη. Σε γενικές γραμμές, το πλήθος και ο τύπος της τεχνικής που θα επιλεγεί εξαρτάται από τη σημασία της απόφασης, από περιορισμούς στο χρόνο και άλλους πόρους καθώς επίσης από το κόστος ευκαιρίας.

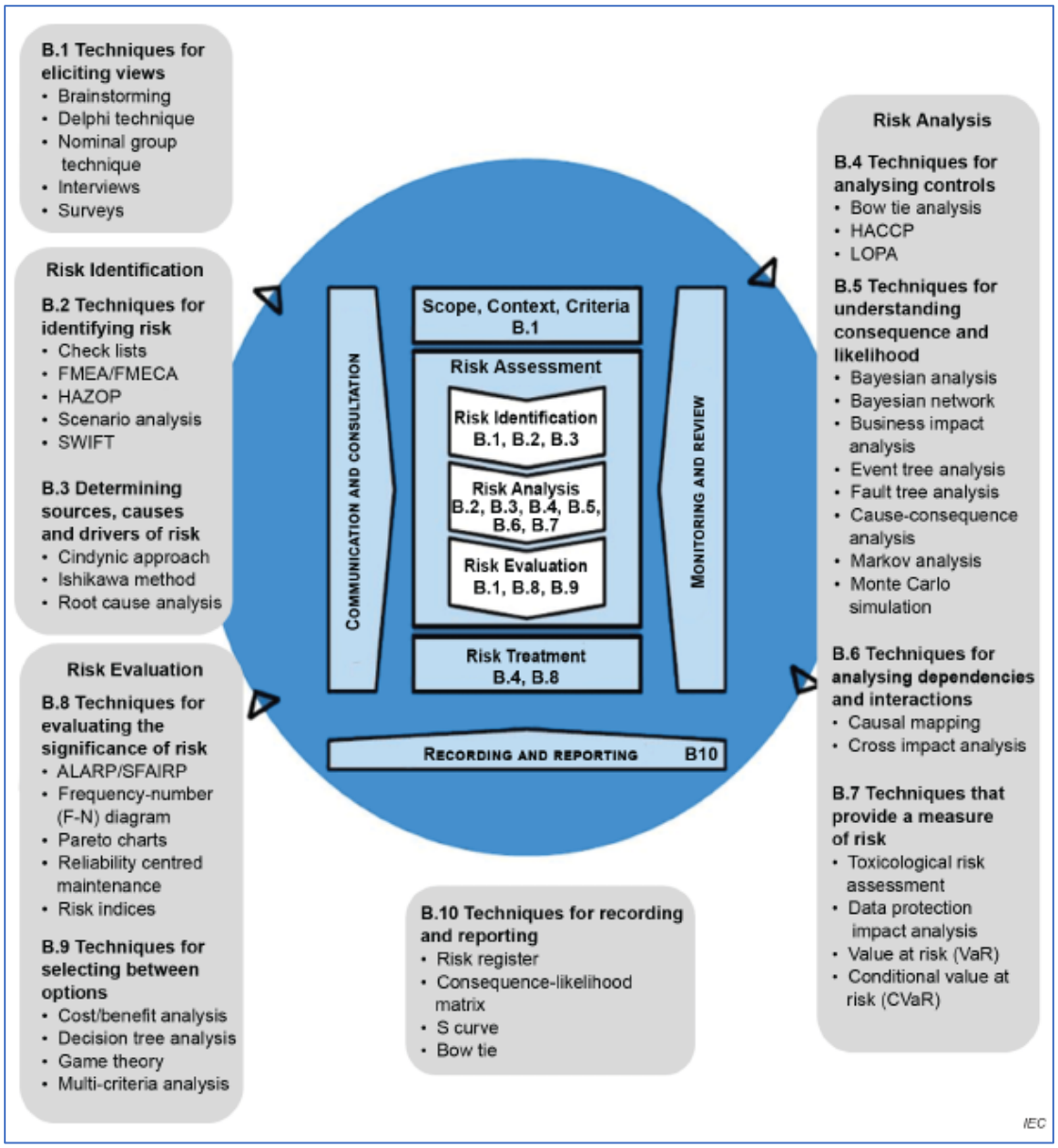
Για να αποφασίσουμε εάν μια ποιοτική ή ποσοτική τεχνική είναι καταλληλότερη, τα κύρια κριτήρια που πρέπει να ληφθούν υπόψη είναι η μορφή του προϊόντος που χρησιμοποιείται περισσότερο για τους ενδιαφερόμενους καθώς επίσης η διαθεσιμότητα και η αξιοπιστία των δεδομένων. Οι ποσοτικές τεχνικές γενικά απαιτούν δεδομένα υψηλής ποιότητας για να δώσουν ουσιαστικά αποτελέσματα. Ωστόσο, σε ορισμένες περιπτώσεις όπου τα δεδομένα δεν είναι επαρκή, η αυστηρότητα που απαιτείται για την εφαρμογή μιας ποσοτικής τεχνικής μπορεί να προσφέρει βελτιωμένη κατανόηση της επικινδυνότητας, παρόλο που το αποτέλεσμα του υπολογισμού μπορεί να είναι αβέβαιο.

Συχνά μπορεί κανείς να επιλέξει από μια ομάδα τεχνικών που σχετίζονται με μια δεδομένη περίσταση. Μπορεί να χρειαστεί να εξεταστούν διάφορες τεχνικές και η εφαρμογή περισσότερων από μία τεχνικών μπορεί μερικές φορές να προσφέρει χρήσιμη πρόσθετη κατανόηση [2]. Διαφορετικές τεχνικές μπορεί επίσης να είναι κατάλληλες καθώς γίνονται διαθέσιμες περισσότερες πληροφορίες.

Κατά την επιλογή μιας τεχνικής (ή τεχνικών) θα πρέπει επομένως να ληφθούν υπόψη τα ακόλουθα:

- ο σκοπός της εκτίμησης,
- οι ανάγκες των ενδιαφερομένων μερών,
- τυχόν νομικές, κανονιστικές και συμβατικές απαιτήσεις, και
- το λειτουργικό περιβάλλον και το σενάριο,

- η σπουδαιότητα της απόφασης (π.χ. τις συνέπειες εάν ληφθεί μια λανθασμένη απόφαση),
- τυχόν καθορισμένα κριτήρια απόφασης και τη μορφή τους,
- ο διαθέσιμος χρόνος πριν από τη λήψη απόφασης,
- οι πληροφορίες που είναι διαθέσιμες ή μπορούν να ληφθούν,
- η πολυπλοκότητα της κατάστασης,
- η εμπειρία που είναι διαθέσιμη ή που μπορεί να αποκτηθεί.



Εικόνα 12 Τεχνικές εκτίμησης διακινδύνευσης και εφαρμογή τους στη διαχείριση της διακινδύνευσης

Το πρότυπο ISO/IEC 31010:2019 [28] κατηγοριοποιεί τις τεχνικές εκτίμησης διακινδύνευσης σε κλάσεις ανάλογα με το στάδιο εφαρμογή τους στη διαδικασία εκτίμησης της διακινδύνευσης (αναγνώριση, ανάλυση και αποτίμηση διακινδύνευσης) και δίνει μια σύντομη περιγραφή αυτών. Οι τεχνικές ομαδοποιούνται σε πίνακες που προσδιορίζουν ποια τεχνική και σε ποιο βαθμό είναι εφαρμόσιμη σε κάθε στάδιο της εκτίμησης της διακινδύνευσης [Πίνακας Α.3 του προτύπου] και προβάλουν τα χαρακτηριστικά τους [Πίνακας Α.1 και Πίνακας Α.2 του προτύπου]. Κάποιες από τις τεχνικές αυτές είναι εφαρμόσιμες και σε άλλα στάδια της διαδικασίας διαχείρισης διακινδύνευσης (μια επισκόπηση αυτών δίνεται στην Εικόνα 12, Πηγή: [28]).

4.3.1. Κατηγοριοποίηση τεχνικών εκτίμησης διακινδύνευσης

Ο Πίνακας 1 παρουσιάζει τα χαρακτηριστικά σύμφωνα με τα οποία μπορεί να γίνει η επιλογή της ή των τεχνικών που πρόκειται να χρησιμοποιηθούν ([28], Πίνακας Α.1) στα διάφορα στάδια της εκτίμηση της διακινδύνευσης.

Χαρακτηριστικό	**Περιγραφή**	**Λεπτομέρειες (π.χ. δείκτες)**
Πεδίο εφαρμογής	Πως χρησιμοποιείται η τεχνική κατά την εκτίμηση διακινδύνευσης	Συγκέντρωση απόψεων, εντοπισμός, ανάλυση αιτιών, ανάλυση ελέγχων κοκ
Σκοπός	Εφαρμόζετε σε επίπεδο Οργανισμού, Τμήματος ή έργου, ή σε ατομικό επίπεδο διεργασίας ή σε επίπεδο εξοπλισμού	Οργανισμός (org) Έργο/Τμήμα (dep) Εξοπλισμός (equip) Διαδικασία (proc)
Χρονικός ορίζοντας	Εξετάζει τη διακινδύνευση σε βραχυπρόθεσμο, μεσοπρόθεσμο, μακροπρόθεσμο ή οποιοδήποτε χρονικό ορίζοντα	Βραχυπρόθεσμα (short) Μεσοπρόθεσμα (medium) Μακροπρόθεσμα (long) Οποτεδήποτε (any)
Επίπεδο απόφασης	Εφαρμόζεται σε στρατηγικό τακτικό ή επιχειρησιακό επίπεδο	Στρατηγικό (1) Τακτικό (2) Επιχειρησιακό (3)

Αρχικές πληροφορίες / απαιτούμενα δεδομένα	Το επίπεδο των αρχικών πληροφοριών ή των δεδομένων που απαιτούνται	Υψηλό (high) Μεσαίο (medium) Χαμηλό (low)
Εμπειρία (Τεχνογνωσία)	Το επίπεδο της εμπειρίας για την εφαρμογή της μεθόδου	Χαμηλή: διαίσθηση ή εκπαίδευση μιας – δυο ημερών (low) Μέτρια: μάθημα κατάρτισης άνω των δύο ημερών (moderate) Υψηλή: σημαντική εκπαίδευση ή εξειδικευμένη εμπειρία (high)
Ποιοτική – Ποσοτική	Ποιοτική, ημι-ποσοτική ή ποσοτική μέθοδος	Ποιοτική (qual) Ημι-ποσοτική (semi-quant) Ποσοτική (quant) Είτε ποσοτική είτε ποιοτική (either
Κόστος εφαρμογής	Απαιτούμενος χρόνος και κόστος για την εφαρμογή της τεχνικής	Υψηλό (high) Μεσαίο (medium) Χαμηλό (low)

Πίνακας 1 Χαρακτηριστικά τεχνικών εκτίμησης διακινδύνευσης

Στον Πίνακα Α.2 του προτύπου ISO/IEC 31010:2019 [28] παρουσιάζεται μια μεγάλη γκάμα από συνολικά 42 τεχνικές οι οποίες κατηγοριοποιούνται σύμφωνα με τα παραπάνω χαρακτηριστικά. Επιπρόσθετα, στον πίνακα Α.3 του προτύπου οι τεχνικές αυτές χαρακτηρίζονται ως «Εφαρμόσιμες», «Ισχυρά Εφαρμόσιμες» και «Μη Εφαρμόσιμες» στα διάφορα στάδια της εκτίμησης διακινδύνευσης. Στη συνέχεια, κάνουμε μια σύντομη αναφορά στις τεχνικές που χαρακτηρίζονται ως «Ισχυρά Εφαρμόσιμες». Αναλυτική περιγραφή αυτών δίνεται στο Παράρτημα Β του προτύπου.

5. Τεχνικές εκτίμησης της διακινδύνευσης

Στις ενότητες που ακολουθούν θα κάνουμε αναφορά στις τεχνικές του προτύπου για τα διάφορα στάδια της εκτίμησης της διακινδύνευσης, δίνοντας μια σύντομη περιγραφή αυτών οι οποίες χαρακτηρίζονται ως «ισχυρά εφαρμόσιμες» για κάθε στάδιο στον πίνακα Α.3 του προτύπου ISO/IEC 31010:2019 [28].

5.1. Τεχνικές αναγνώρισης διακινδύνευσης

Η αναγνώριση διακινδύνευσης είναι η διαδικασία του εντοπισμού, της αναγνώρισης και της καταγραφής των κινδύνων. Σκοπός της είναι να εντοπίσει τα αίτια και τις πηγές του κινδύνου, τα γεγονότα, τις καταστάσεις ή περιστάσεις που θα μπορούσαν να έχουν επιπτώσεις στον οργανισμό. Οι τεχνικές/μέθοδοι αναγνώρισης της διακινδύνευσης μπορεί να είναι:

- μέθοδοι που βασίζονται σε τεκμήρια, όπως για παράδειγμα οι λίστες ελέγχου και οι ανασκοπήσεις ιστορικών δεδομένων,
- συστηματικές προσεγγίσεις ομάδας, όπου μια ομάδα ειδικών ακολουθεί μια συστηματική διαδικασία για να αναγνωρίσει τους κινδύνους,
- τεχνικές επαγωγικής λογικής, όπου τα συμπεράσματα προκύπτουν με μετάβαση από το ειδικό στο γενικό, όπως η τεχνική HAZOP.

Μπορούν να χρησιμοποιηθούν διάφορες υποστηρικτικές τεχνικές για τη βελτίωση της ακρίβειας και της πληρότητας στην αναγνώριση κινδύνου, όπως ο καταιγισμός ιδεών και η τεχνική Delphi .

Το παραγόμενο αποτέλεσμα από την αναγνώριση διακινδύνευσης μπορεί να καταγραφεί ως λίστα κινδύνων με γεγονότα, αιτίες και καθορισμένες συνέπειες ή χρησιμοποιώντας άλλες κατάλληλες μορφές.

Ανεξάρτητα από τις τεχνικές που χρησιμοποιούνται, είναι σημαντικό να δοθεί η δέουσα προσοχή σε ανθρώπινους και οργανωτικούς παράγοντες. Ως εκ τούτου, στη διαδικασία αναγνώρισης διακινδύνευσης θα πρέπει να περιλαμβάνονται αποκλίσεις ανθρώπινων και οργανωτικών παραγόντων από τα αναμενόμενα, όπως επίσης και συμβάντα που αφορούν το υλικό καθώς και το λογισμικό.

Ο Πίνακας 2 παρουσιάζει τις τεχνικές που μπορούν να εφαρμοστούν κατά το στάδιο της αναγνώρισης της διακινδύνευσης. Με πλάγια γραφή εμφανίζονται αυτές που είναι ισχυρά εφαρμόσιμες, τις οποίες και θα περιγράψουμε στη συνέχεια.

Bow tie analysis	*Hazard analysis and critical control points (HACCP)*
Brainstorming	*Human reliability analysis*
Business impact analysis	*Ishikawa (fishbone)*
Causal mapping	Layer protection analysis (LOPA)
Cause-consequence analysis	Markov analysis
Checklists, classifications, and Taxonomies	Multi-criteria analysis (MCA)
Cindynic approach	*Nominal group technique*
Delphi technique	Privacy impact analysis/ data protection impact assessment (PIA/DPIA)
Failure modes and effects Analysis	Reliability centred maintenance
Failure modes and effects and criticality analysis	*Scenario analysis*
Fault tree analysis	*Structured or semi-structured interviews*
F-N diagrams	*Structured "What if?" (SWIFT)*
Game theory	*Surveys*
Hazard and operability studies (HAZOP)	*Toxicological risk assessment*

Πίνακας 2 Τεχνικές αναγνώρισης διακινδύνευσης σύμφωνα με τον πρότυπο ISO/IEC 31010:2019

5.1.1. Καταιγισμός ιδεών

Ο καταιγισμός ιδεών (brainstorming) [23] είναι μια διαδικασία που χρησιμοποιείται για την τόνωση και την ενθάρρυνση μιας ομάδας ανθρώπων να αναπτύξουν ιδέες που σχετίζονται με ένα από περισσότερα θέματα οποιασδήποτε φύσης. Σημαίνει οποιοδήποτε είδος ομαδικής συζήτησης, αλλά ο αποτελεσματικός καταιγισμός ιδεών απαιτεί συνειδητή προσπάθεια για να διασφαλιστεί ότι οι σκέψεις των άλλων στην ομάδα χρησιμοποιούνται ως εργαλεία για την τόνωση της δημιουργικότητας κάθε συμμετέχοντα. Η τεχνική είναι πολύ χρήσιμη όταν εργαζόμαστε σε καινοτόμα σχέδια, προϊόντα και διαδικασίες και χρησιμοποιείται για τον στατιστικό έλεγχο ποιότητας και τη βελτίωση της ποιότητας [29], [30].

5.1.2. Λίστες ελέγχου, κατηγοριοποιήσεις και ταξινομήσεις

Οι λίστες ελέγχου, οι κατηγοριοποιήσεις και οι ταξινομήσεις (checklists, classifications, Taxonomies) [23] χρησιμοποιούνται κατά την εκτίμηση διακινδύνευσης με διάφορους τρόπους, όπως για να βοηθήσουν στην κατανόηση του πλαισίου, στον εντοπισμό και στην ομαδοποίηση των κινδύνων με κοινά χαρακτηριστικά. Χρησιμοποιούνται επίσης κατά τη διαχείριση διακινδύνευσης, για παράδειγμα για την ταξινόμηση ελέγχων και θεραπειών, για τον καθορισμό ευθυνών ή για αναφορά και κοινοποίηση της διακινδύνευσης.

5.1.3. Η κινδυνική προσέγγιση

Η Κινδυνική είναι η επιστήμη του κινδύνου. Η κινδυνική προσέγγιση (Cindynic approach) εντοπίζει άυλες πηγές κινδύνου και παράγοντες που ενδέχεται να προκαλέσουν πολλές διαφορετικές συνέπειες [23]. Ειδικότερα, λαμβάνει υπόψη στόχους, αξίες, κανόνες, δεδομένα και μοντέλα ενδιαφερομένων (όπως προκύπτουν από ημι-δομιμένες συνεντεύξεις) και προσδιορίζει και αναλύει:

- ασυνέπειες, ασάφειες, παραλείψεις, άγνοια (ονομάζονται ελλείμματα),
- αποκλίσεις μεταξύ των ενδιαφερομένων (ονομάζονται ασυμφωνίες).

Τα παραπάνω αποτελούν συστημικές πηγές και οδηγούς κινδύνου.

5.1.4. Η τεχνική Delphi

Η τεχνική Delphi (Delphi technique) [28], [31] είναι μια διαδικασία για την απόκτηση απόψεων από μια ομάδα ειδικών. Αξιοποιεί τη γνώση και την εμπειρία ειδικών σε ένα πεδίο προκειμένου να ληφθούν αποφάσεις για ένα ζήτημα που σχετίζεται με το πεδίο. Είναι μια μέθοδος συλλογής και κατάταξης κρίσεων για ένα συγκεκριμένο θέμα μέσω ενός συνόλου διαδοχικών ερωτηματολογίων. Ένα ουσιαστικό χαρακτηριστικό της τεχνικής Delphi είναι ότι οι ειδικοί εκφράζουν τις απόψεις τους μεμονωμένα, ανεξάρτητα και ανώνυμα ενώ έχουν πρόσβαση στις απόψεις των άλλων ειδικών καθώς προχωρά η διαδικασία, η οποία επαναλαμβάνετε μέχρι να επιτευχθεί σύγκλιση απόψεων.

Η τεχνική Delphi χρησιμοποιείται για πολύπλοκα προβλήματα για τα οποία υπάρχει αβεβαιότητα και για τα οποία απαιτείται η κρίση των ειδικών για την αντιμετώπιση

αυτής της αβεβαιότητας. Η ασύγχρονη αλληλεπίδραση και ανωνυμία των συμμετεχόντων την καθιστούν ως μια «από τα κάτω προς τα πάνω» δημοκρατική προσέγγιση στη λήψη αποφάσεων (decision making) και στη χάραξη πολιτικής (policy making). Εφαρμόζεται σε διάφορες περιοχές όπως στην Τεχνολογία, στην Υγεία αλλά και στην Εκπαίδευση όπως για παράδειγμα για τον προσδιορισμό των ικανοτήτων καθηγητών Γ' βάθμιας εκπαίδευσης [32].

5.1.5. Ανάλυση Τρόπων Αστοχίας και Αποτελεσμάτων (FMEA)

Η ανάλυση τρόπων αστοχίας και αποτελεσμάτων (Failure Mode and Effect Analysis – FMEA), η οποία είναι γνωστή και ως Μελέτη Αστοχίας, είναι μια τεχνική που αξιολογεί την πιθανότητα εμφάνισης αστοχίας (αποτυχίας) ενός προϊόντος (πιθανότητα ύπαρξης ελαττώματος), καθώς και τις επιπτώσεις αυτής της αστοχίας [29], [33]. Εφαρμόζεται σε επίπεδο συστήματος (System Failure Mode and Effect Analysis, SFMEA), παραγωγής (Process Failure Mode and Effect Analysis, PFMEA) και σχεδιασμού (Design Failure Mode and Effect Analysis, DFMEA). Την Μελέτη Αστοχίας μπορεί να ακολουθήσει ανάλυση κρισιμότητας που καθορίζει τη σημασία κάθε αστοχίας τρόπου αποτυχίας (Failure modes and effects and criticality analysis – FMECA) [28].

Στην Μελέτη Αστοχίας, μια ομάδα υποδιαιρεί το υλικό, ένα σύστημα, μια διαδικασία ή μια διεργασία σε επιμέρους συνιστώσες. Για κάθε συνιστώσα εξετάζονται οι τρόποι με τους οποίους μπορεί να αποτύχει καθώς και οι αιτίες και τα αποτελέσματα της αποτυχίας. Επίσης, για κάθε συνιστώσα καταγράφονται: η λειτουργία της, η αστοχία που μπορεί να συμβεί (λειτουργία αποτυχίας), η πιθανότητα εμφάνισης (occurrence), οι μηχανισμοί που θα μπορούσαν να προκαλέσουν αυτούς τους τρόπους αστοχίας, η πιθανότητα εντοπισμού (detection), η φύση των συνεπειών σε περίπτωση αστοχίας, εάν η αστοχία είναι ακίνδυνη ή επιβλαβής (βαθμός σοβαρότητας, severity), πώς και πότε μπορεί να εντοπιστεί η αστοχία καθώς επίσης και τις εγγενείς προβλέψεις που υπάρχουν προκειμένου να αντισταθμίσουν την αστοχία. Στη συνέχεια, στην ανάλυση κρισιμότητας (FMECA), η ομάδα μελέτης ταξινομεί κάθε έναν από τους τρόπους αστοχίας σύμφωνα με την κρισιμότητα του. Μπορούν να χρησιμοποιηθούν διάφορες μέθοδοι κρισιμότητας, με πιο συχνά

χρησιμοποιούμενο τον πίνακα συνεπειών/πιθανότητας (consequence/likelihood matrix) και τον Αριθμό Προτεραιότητας Διακινδύνευσης (Risk Priority Number – RPN) ο οποίος υπολογίζεται πολλαπλασιάζοντας το βαθμό της κρισιμότητας (S), της πιθανότητας εμφάνισης (O) και της πιθανότητας εντοπισμού(D), δηλαδή, RPN = S x O x D. Η συνιστώσα με το μεγαλύτερο Αριθμό Προτεραιότητας Διακινδύνευσης θα πρέπει να αξιολογηθεί πρώτα, με σκοπό τη μείωση του βαθμού της κρισιμότητας, της πιθανότητας εμφάνισης και της πιθανότητας εντοπισμού και την εφαρμογή αποτελεσματικών διορθωτικών ενεργειών εντός ενός προκαθορισμένου χρονικού διαστήματος. Στη συνέχει υπολογίζεται εκ νέου ο Αριθμός Προτεραιότητας Διακινδύνευσης και εφαρμόζονται πρόσθετες διορθωτικές ενέργειες εφόσον απαιτούνται. Οδηγίες για τον τρόπο βαθμολόγησης της κρισιμότητας, της πιθανότητας εμφάνισης και της πιθανότητας εντοπισμού αστοχιών δίνονται αντίστοιχα στους Πίνακες 4.2, 4.3 και 4.4 στο [33].

5.1.6. Ανάλυση κινδύνων και κρίσιμων σημείων ελέγχου (HACCP)

Η ανάλυση κινδύνων και κρίσιμων σημείων ελέγχου (Hazard analysis and critical control points – HACCP) [28] αναπτύχθηκε για να διασφαλίσει την ασφάλεια των τροφίμων για το διαστημικό πρόγραμμα της NASA, αλλά μπορεί να χρησιμοποιηθεί και για διεργασίες ή δραστηριότητες που δεν αφορούν τα τρόφιμα. Η τεχνική παρέχει μια δομή για τον εντοπισμό των πηγών διακινδύνευσης (κινδύνους ή απειλές) και την εφαρμογή ελέγχων σε όλα τα σχετικά μέρη μιας διαδικασίας για την προστασία από αυτές. Η τεχνική HACCP χρησιμοποιείται σε επιχειρησιακό επίπεδο, ωστόσο τα αποτελέσματά της μπορούν να υποστηρίξουν τη συνολική στρατηγική ενός οργανισμού. Η HACCP στοχεύει να διασφαλίσει ότι η διακινδύνευση ελαχιστοποιείται μέσω της παρακολούθησης και των ελέγχων σε όλη τη διαδικασία και όχι μέσω της επιθεώρησης στο τέλος της διαδικασίας.

5.1.7. Μελέτη Επικινδυνότητας και Λειτουργικότητας (HAZOP)

Η μελέτη επικινδυνότητας και λειτουργικότητας (Hazard and operability study – HAZOP) είναι μια δομημένη και συστηματική εξέταση μιας προγραμματισμένης ή υπάρχουσας διαδικασίας, διεργασίας ή συστήματος που περιλαμβάνει τον εντοπισμό πιθανών αποκλίσεων από τον αρχικό σχεδιασμό και την εξέταση των

πιθανών αιτιών και των συνεπειών τους [28]. Αποτελεί ένα de facto βιομηχανικό πρότυπο για τον προσδιορισμό πιθανών αποκλίσεων προβλημάτων που μπορεί να αποκαλυφθούν με την επανεξέταση της ασφάλειας των σχεδίων και την επανεξέταση των υφιστάμενων διεργασιών και λειτουργιών σε χημικές, φαρμακευτικές, πετρελαιοειδείς και πυρηνικές βιομηχανίες [34].

Για τη μελέτη επικινδυνότητας και λειτουργικότητας, συγκροτείται μια διεπιστημονική ομάδα που αποτελείται από έναν επικεφαλής και από μέλη που μπορούν να συνεργαστούν και να παρέχουν διαφορετικές οπτικές με βάση τα πεδία εξειδίκευσής τους στην αναγνώριση πηγών κινδύνων και πιθανών αποκλίσεων από το σχεδιασμό (περιλαμβάνει σχεδιαστές, χειριστές του συστήματος καθώς και άτομα που δεν εμπλέκονται άμεσα στο σχεδιασμό του υπό μελέτη συστήματος). Η ομάδα υποδιαιρεί το σύστημα, τη διαδικασία ή τη διεργασία σε επιμέρους συνιστώσες και παράγει σχέδια ή διαγράμματα για οπτική αναπαράσταση του τρόπου διασύνδεσης των συνιστωσών. Στη συνέχεια, συμφωνεί το σκοπό για τον οποίο έχει σχεδιαστεί κάθε συνιστώσα, καθορίζει της παραμέτρους και τα όρια ασφαλούς λειτουργίας κάθε συνιστώσας και προσδιορίζει πιθανές αποκλίσεις. Η ομάδα επιλέγει κατευθυντήριες λέξεις (guidewords)[2] που φανερώνουν την ενέργεια που θα πρέπει να πραγματοποιηθεί και εφαρμόζει τις κατευθυντήριες λέξεις διαδοχικά σε κάθε παράμετρο για κάθε συνιστώσα για να υποθέσει πιθανές αποκλίσεις από τον αρχικό σχεδιασμό που θα μπορούσαν να έχουν ανεπιθύμητα αποτελέσματα. Στη συνέχεια συμφωνεί την αιτία και τις συνέπειες σε κάθε περίπτωση, προτείνοντας πώς θα μπορούσαν να αντιμετωπιστούν και τέλος τεκμηριώνει τη συζήτηση και συμφωνεί για πιθανές ενέργειες για την αντιμετώπιση των κινδύνων που εντοπίστηκαν.

5.1.8. Ανάλυση ανθρώπινης αξιοπιστίας (HRA)

Η ανάλυση ανθρώπινης αξιοπιστίας (Human reliability analysis - HRA) αφορά το σύνολο των τεχνικών για τον εντοπισμό του ενδεχόμενου να συμβεί ανθρώπινο σφάλμα και την εκτίμηση της πιθανότητας αυτής της αστοχίας. Εφαρμόζεται σε τακτικό επίπεδο σε συγκεκριμένες εργασίες όπου η σωστή απόδοση είναι κρίσιμη. Πρώτα, πραγματοποιείται μια αρχική ιεραρχική ανάλυση των εργασιών για τον

[2] Παραδείγματα βασικών κατευθυντήριων λέξεων και της σημασίας τους είναι διαθέσιμα στο [28].

εντοπισμό βημάτων και υποβημάτων. Σε κάθε υποβήμα προσδιορίζονται τα πιθανά σφάλματα, εντοπίζονται οι αιτίες αυτών, καθώς και πληροφορίες για τη μείωση της πιθανότητας εμφάνισης τους. Η πιθανότητα μιας λανθασμένης ενέργειας μπορεί να εκτιμηθεί με διάφορες μεθόδους, συμπεριλαμβανομένης της χρήσης μιας βάσης δεδομένων παρόμοιων εργασιών ή της κρίσης των ειδικών [28].

5.1.9. Ανάλυση Ishikawa (fishbone)

Η ανάλυση Ishikawa (αναπτύχθηκε από τον Kaoru Ishikawa) χρησιμοποιεί μια ομαδική προσέγγιση για να εντοπίσει πιθανές αιτίες οποιουδήποτε επιθυμητού ή ανεπιθύμητου γεγονότος, επίδρασης, θέματος ή κατάστασης. Οι πιθανοί παράγοντες που συμβάλλουν οργανώνονται σε μεγάλες κατηγορίες για να καλύψουν ανθρώπινα, τεχνικά και οργανωτικά αίτια. Οι πληροφορίες απεικονίζονται σε ένα διάγραμμα, το διάγραμμα Ishikawa ή διάγραμμα αιτίου – αποτελέσματος (cause and effect diagram) σε σχήμα ψαροκόκαλου (fishbone) [28],[29].

Τα κύρια βήματα για την εκτέλεση της ανάλυσης είναι τα ακόλουθα:

- Καθορισμός του αποτελέσματος που πρόκειται να αναλυθεί (αποτελεί την κεφαλή του διαγράμματος ψαροκόκαλου).
- Καθορισμός των κύριων κατηγοριών των αιτιών, σύμφωνα με τις συνθήκες που αναλύονται (π.χ. μέθοδοι, μηχανήματα, διαχείριση, υλικά, ανθρώπινο δυναμικό, χρήματα ή υλικά, μέθοδοι και διαδικασίες, περιβάλλον, εξοπλισμός, άνθρωποι, μετρήσεις).
- Ερώτηση "γιατί;" και "πώς μπορεί να συμβεί αυτό;" επαναληπτικά προκειμένου να διερευνηθούν τα αίτια και οι παράγοντες που επηρεάζουν την κάθε κατηγορία, προσθέτοντας έτσι το καθένα από τα οστά του διαγράμματος ψαροκόκαλου.
- Έλεγχος όλων των κλάδων του διαγράμματος για να επαληθευτεί η συνέπεια και η πληρότητα και να βεβαιωθεί ότι οι αιτίες ισχύουν για το κύριο αποτέλεσμα.
- Προσδιορισμός των πιο σημαντικών παραγόντων με βάση τη γνώμη της ομάδας και τα διαθέσιμα στοιχεία.

5.1.10. Ψήφος ομάδας

Η τεχνική της ψήφου ομάδας (nominal group technique) μπορεί να θεωρηθεί ως εξελικτικό βήμα του καταιγισμού ιδεών [28], [29]. Στοχεύει στη συλλογή ιδεών, με τις απόψεις των εμπλεκομένων μελών της ομάδας να αναζητούνται πρώτα μεμονωμένα χωρίς αλληλεπίδραση μεταξύ τους, και στη συνέχεια να συζητούνται από την ομάδα.

Η διαδικασία είναι η εξής: ένας διαμεσολαβητής παρέχει σε κάθε μέλος της ομάδας τις υπό εξέταση ερωτήσεις. Στη συνέχεα, κάθε μέλος της ομάδας καταγράφει τις ιδέες του σιωπηλά και ανεξάρτητα και τις παρουσιάζει χωρίς, σε αυτό το στάδιο, να πραγματοποιηθεί καμία συζήτηση. Εάν η δυναμική της ομάδας σημαίνει ότι ορισμένες φωνές έχουν μεγαλύτερη βαρύτητα από άλλες, οι ιδέες μπορούν να μεταβιβαστούν στον συντονιστή ανώνυμα. Στη συνέχεια, οι συμμετέχοντες μπορούν να ζητήσουν περαιτέρω διευκρινίσεις. Οι ιδέες συζητούνται από την ομάδα για την παροχή μιας συμφωνημένης λίστας. Τέλος, τα μέλη της ομάδας ψηφίζουν ιδιωτικά για τις ιδέες και λαμβάνεται μια ομαδική απόφαση με βάση την ψηφοφορία.

Η τεχνική της ψήφου ομάδας μπορεί να χρησιμοποιηθεί εναλλακτικά αντί του καταιγισμού ιδεών. Είναι επίσης χρήσιμη για την ιεράρχηση ιδεών μέσα σε μια ομάδα. Δεν απαιτεί δεδομένα εισόδου παρά τις ιδέες και τις εμπειρίες των συμμετεχόντων. Αποτέλεσμα της τεχνικής είναι ιδέες, λύσεις ή αποφάσεις όπως απαιτείται. Η τεχνική χρησιμοποιείται για τον στατιστικό έλεγχο ποιότητας [29].

5.1.11. Ανάλυση σεναρίων

Η ανάλυση σεναρίων (Scenario analysis) [23] συνίσταται στον καθορισμό ενός εύλογου σεναρίου και στην επεξεργασία του τι μπορεί να συμβεί με δεδομένες διάφορες πιθανές μελλοντικές εξελίξεις. Για σχετικά σύντομες χρονικές κλίμακες μπορεί να περιλαμβάνει παρέκταση από αυτό που έχει συμβεί στο παρελθόν. Για μεγαλύτερες χρονικές κλίμακες, η ανάλυση σεναρίων μπορεί να περιλαμβάνει τη δημιουργία ενός φανταστικού αλλά αξιόπιστου σεναρίου και στη συνέχεια να διερευνήσει τη φύση των κινδύνων σε αυτό το σενάριο. Τις περισσότερες φορές εφαρμόζεται από μια ομάδα ενδιαφερομένων με διαφορετικά ενδιαφέροντα και τεχνογνωσία. Η ανάλυση σεναρίου περιλαμβάνει τον καθορισμό με κάποια

λεπτομέρεια του σεναρίου ή των σεναρίων που πρέπει να ληφθούν υπόψη και τη διερεύνηση των επιπτώσεων του σεναρίου και του σχετικού κινδύνου.

5.1.12. Δομημένη ή ημι-δομημένη συνέντευξη

Σε μια δομημένη συνέντευξη (structured interview), ζητείται από τους μεμονωμένους συνεντευξιαζόμενους ένα σύνολο προκαθορισμένων ερωτήσεων. Μια ημι-δομημένη συνέντευξη (semi-structured interview) είναι παρόμοια, αλλά επιτρέπει μεγαλύτερη ελευθερία για συνομιλία για τη διερεύνηση ζητημάτων που πιθανών να προκύψουν. Σε μια ημι-δομημένη συνέντευξη παρέχεται η ευκαιρία να διερευνηθούν τομείς που ο ερωτώμενος θα ήθελε να καλύψει [28].

Οι ερωτήσεις πρέπει να είναι ανοιχτού τύπου, να είναι απλές και στην κατάλληλη γλώσσα για τον ερωτώμενο και κάθε ερώτηση να καλύπτει ένα μόνο θέμα. Επίσης θα πρέπει να έχουν προετοιμαστεί πιθανές επακόλουθες διευκρινιστικές ερωτήσεις.

Οι ερωτήσεις θα πρέπει να έχουν δοκιμαστεί από άτομα παρόμοιου υπόβαθρου με αυτά που θα ερωτηθούν προκειμένου να ελεγχθεί ότι δεν είναι διφορούμενες, ότι είναι σαφείς και σωστά κατανοητές και ότι οι απαντήσεις θα καλύπτουν τα ζητήματα που επιδιώκονται. επίσης, πρέπει να ληφθεί μέριμνα ώστε οι ερωτήσεις να μην μεροληπτούν προς κάποια απάντηση.

Οι δομημένες και ημι-δομημένες συνεντεύξεις είναι ένα μέσο για τη λήψη εις βάθος πληροφοριών και απόψεων από άτομα μιας ομάδας. Οι απαντήσεις τους μπορεί να είναι εμπιστευτικές εάν χρειαστεί. Παρέχουν εις βάθος πληροφορίες όταν τα άτομα δεν επηρεάζονται από τις απόψεις άλλων μελών μιας ομάδας. Είναι χρήσιμες όταν είναι δύσκολο να συγκεντρωθούν οι ενδιαφερόμενοι στο ίδιο μέρος την ίδια στιγμή ή εάν η ελεύθερη συζήτηση σε μια ομάδα δεν είναι κατάλληλη για την κατάσταση ή τα άτομα που εμπλέκονται. Παρέχουν πιο λεπτομερείς πληροφορίες από ότι μια έρευνα (survey) ή ένα εργαστήριο (workshop) και μπορούν να χρησιμοποιηθούν σε οποιοδήποτε επίπεδο σε έναν οργανισμό.

5.1.13. Δομημένη «τι θα γινόταν αν» (SWIFT)

Η τεχνική «τι θα γινόταν αν» (Structured "What if?" - SWIFT) είναι μια υψηλού επιπέδου τεχνική αναγνώρισης κινδύνου που μπορεί να χρησιμοποιηθεί ανεξάρτητα

ή ως μέρος μιας σταδιακής προσέγγισης προκειμένου να καταστήσει πιο αποτελεσματικές μεθόδους «από κάτω προς τα πάνω», όπως η Μελέτη Επικινδυνότητας και Λειτουργικότητας ή Ανάλυση Τρόπων Αστοχίας και Αποτελεσμάτων. Η τεχνική χρησιμοποιεί δομημένο καταιγισμό ιδεών σε ένα εργαστήριο όπου ένα προκαθορισμένο σύνολο κατευθυντήριων λέξεων (χρόνος, ποσό, κ.λπ.) συνδυάζεται με προτροπές που προέρχονται από τους συμμετέχοντες που συχνά ξεκινούν με φράσεις όπως "τι θα γινόταν αν;" ή «πώς θα μπορούσε;».

Πριν από την έναρξη της μελέτης, ο συντονιστής ετοιμάζει μια λίστα με κατευθυντήριες λέξεις προκειμένου να επιτρέψει μια ολοκληρωμένη ανασκόπηση των κινδύνων ή των πηγών κινδύνου. Στην αρχή του εργαστηρίου συζητείται το πλαίσιο, το πεδίο εφαρμογής και ο σκοπός της μελέτης και διατυπώνονται τα κριτήρια επιτυχίας. Χρησιμοποιώντας τις κατευθυντήριες λέξεις και φράσεις όπως «τι θα γινόταν αν;» ή «πως θα μπορούσε;», ο συντονιστής ζητά από τους συμμετέχοντες να εγείρουν και να συζητήσουν θέματα όπως γνωστούς κινδύνους, πηγές κινδύνου και οδηγοί, προηγούμενη εμπειρία, επιτυχίες και περιστατικά, γνωστοί και υφιστάμενοι έλεγχοι, κανονιστικές απαιτήσεις και περιορισμοί κ.α..

Ο συντονιστής χρησιμοποιεί τη λίστα με τις κατευθυντήριες λέξεις για να παρακολουθεί τη συζήτηση και να προτείνει επιπλέον θέματα και σενάρια προς συζήτηση στην ομάδα. Κάθε μέλος της ομάδας εκτιμά πιθανούς κινδύνους βασιζόμενος στην πρότερη εμπειρία του και στη γνώση παρόμοιων περιπτώσεων από το παρελθόν. Η ομάδα εξετάζει εάν οι έλεγχοι είναι επαρκείς και, εάν όχι, εξετάζει πιθανές θεραπείες. Κατά τη διάρκεια αυτής της συζήτησης, περαιτέρω τίθενται κι άλλα ερωτήματα όπως «τι θα γινόταν αν;». Σε ορισμένες περιπτώσεις εντοπίζονται συγκεκριμένοι κίνδυνοι και μπορεί να καταγραφεί μια περιγραφή του κινδύνου, των αιτιών, των συνεπειών και των ελέγχων του. Επιπλέον, μπορεί να εντοπιστούν πιο γενικές πηγές ή παράγοντες κινδύνου, προβλήματα ελέγχου ή συστημικά ζητήματα.

5.1.14. Έρευνα

Οι έρευνες (surveys) γενικά εμπλέκουν περισσότερους ανθρώπους από ότι οι συνεντεύξεις και συνήθως οι ερωτήσεις που θέτουν είναι πιο περιορισμένες [28].

Συνήθως μια έρευνα περιλαμβάνει ένα ερωτηματολόγιο σε έντυπη ή ηλεκτρονική μορφή. Οι ερωτήσεις συχνά επιδέχονται απαντήσεις «κλειστού τύπου» της μορφής ναι/όχι, επιλογές από μια κλίμακα αξιολόγησης ή επιλογές από μια σειρά επιλογών. Αυτό επιτρέπει τη στατιστική ανάλυση των αποτελεσμάτων, κάτι που είναι χαρακτηριστικό τέτοιων μεθόδων. Μπορούν να συμπεριληφθούν ορισμένες ερωτήσεις «ανοικτού τύπου» όπου ο ερωτώμενος να απαντά με ελεύθερο κείμενο, ωστόσο ο αριθμός τους θα πρέπει να είναι περιορισμένος καθώς η ανάλυση τους είναι δύσκολη.

Οι έρευνες μπορούν να χρησιμοποιηθούν σε οποιαδήποτε περίπτωση είναι χρήσιμη η ευρεία διαβούλευση με τα ενδιαφερόμενα μέρη, ιδιαίτερα, όταν απαιτούνται σχετικά λίγες πληροφορίες από μεγάλο αριθμό ατόμων.

Ένα ερωτηματολόγιο, με ελεγμένες σαφείς ερωτήσεις, αποστέλλεται σε ένα ευρέως αντιπροσωπευτικό δείγμα ατόμων που θα συμμετέχει στην έρευνα. Καθώς τα ποσοστά συμμετοχής είναι συνήθως χαμηλά, θα πρέπει να αποσταλούν πολλά ερωτηματολόγια προκειμένου ο αριθμός των απαντήσεων να είναι επαρκής ώστε να παρέχει στατιστική εγκυρότητα. Για την ανάπτυξη ενός ερωτηματολογίου που θα επιτύχει χρήσιμα αποτελέσματα απαιτείται εμπειρία και τεχνογνωσία, ομοίως και για τη στατιστική ανάλυση των αποτελεσμάτων. Το αποτέλεσμα μια έρευνας συνήθως είναι ένα γράφημα που αντικατοπτρίζει τις απαντήσεις των ερωτηθέντων.

5.1.15. Τοξικολογική εκτίμηση διακινδύνευσης

Η τοξικολογική εκτίμηση διακινδύνευσης (Toxicological risk assessment) αφορά την εκτίμηση τη επικινδυνότητας διεργασιών που αφορούν φυτά, ζώα, οικολογικούς τομείς καθώς και τον άνθρωπο ως αποτέλεσμα της έκθεσης σε μια σειρά περιβαλλοντικών κινδύνων. Οι κίνδυνοι για τα φυτά, τα ζώα, τους οικολογικούς τομείς και τον άνθρωπο μπορεί να οφείλονται σε φυσικούς, χημικούς και/ή βιολογικούς παράγοντες που έχουν ως αποτέλεσμα βλάβη στο DNA, γενετικές ανωμαλίες, εξάπλωση ασθενειών, μόλυνση των τροφικών αλυσίδων και μόλυνση του νερού. Η αξιολόγηση τέτοιων κινδύνων μπορεί να απαιτεί την εφαρμογή μιας σειράς τεχνικών που εφαρμόζονται στα ακόλουθα βήματα: διατύπωση προβλήματος,

προσδιορισμός και ανάλυση κινδύνου, εκτίμηση απόκρισης δόσης, εκτίμηση έκθεσης και χαρακτηρισμός κινδύνου [28].

5.2. Τεχνικές ανάλυσης διακινδύνευσης

Η ανάλυση της διακινδύνευσης στοχεύει στην κατανόηση του κινδύνου. Παρέχει στοιχεία για την αξιολόγηση κινδύνου, για τη λήψη αποφάσεων, για το εάν οι κίνδυνοι πρέπει να αντιμετωπιστούν και για το ποιες είναι οι καταλληλότερες στρατηγικές και μέθοδοι θεραπείας. Περιλαμβάνει την εξέταση των αιτιών και των πηγών του κινδύνου, των συνεπειών τους και τις πιθανότητες να συμβούν αυτές οι συνέπειες.

Οι μέθοδοι/τεχνικές που χρησιμοποιούνται για την ανάλυση της διακινδύνευσης μπορεί να είναι ποιοτικές, ημιποσοτικές ή ποσοτικές. Ο βαθμός λεπτομέρειας που θα απαιτηθεί εξαρτάται από τη συγκεκριμένη εφαρμογή, τη διαθεσιμότητα αξιόπιστων δεδομένων και τις ανάγκες λήψης αποφάσεων του οργανισμού. Σε ορισμένες μεθόδους ο βαθμός λεπτομέρειας της ανάλυσης ενδεχομένως να ορίζεται από τη νομοθεσία.

Ο Πίνακας 3 παρουσιάζει τις τεχνικές που μπορούν να εφαρμοστούν κατά το στάδιο της ανάλυσης της διακινδύνευσης. Με πλάγια γραφή εμφανίζονται αυτές που είναι ισχυρά εφαρμόσιμες, τις οποίες και θα περιγράψουμε στη συνέχεια. Οι τεχνικές κατηγοριοποιούνται ανάλογα με το αν αφορούν τις συνέπειες, την πιθανότητα και το επίπεδο της επικινδυνότητας.

Bayesian analysis	Hazard and operability studies (HAZOP)
Bayesian networks	*Hazard analysis and critical control points (HACCP)*
Bow tie analysis	*Human reliability analysis*
Brainstorming	Ishikawa (fishbone)
Business impact analysis	*Layer protection analysis (LOPA)*
Causal mapping	*Markov analysis*
Cause-consequence analysis	Monte Carlo simulation
Consequence/likelihood matrix	Nominal group technique
Cost/benefit analysis	Pareto charts

Cross impact analysis	Privacy impact analysis/ data privacy impact assessment (PIA/DPIA)
Decision tree analysis	Reliability centred maintenance
Event tree analysis	*Risk indices*
Failure modes and effects analysis	*S-curves*
Failure modes and effects and criticality analysis	*Scenario analysis*
Fault tree analysis	*Structured "What if?" (SWIFT)*
F-N diagrams	*Toxicological risk assessment*
Game theory	*Value at risk (VaR)*

Πίνακας 3 Τεχνικές ανάλυσης διακινδύνευσης σύμφωνα με τον πρότυπο ISO/IEC 31010:2019

5.2.1. Μπεϋζιανά δίκτυα (BN)

Ένα Μπεϋζιανό δίκτυο (Bayesian Network – BN) είναι ένα πιθανοτικό γραφικό μοντέλο που αναπαριστά ένα σύνολο μεταβλητών και τις εξαρτήσεις αυτών μέσω ενός κατευθυντικού ακυκλικού γραφήματος (directed acyclic graph, DAG). Οι κόμβοι του γραφήματος αντιπροσωπεύουν τυχαίες μεταβλητές (διακριτές ή συνεχείς) και συνδέονται μεταξύ τους με κατευθυνόμενα τόξα που αντιπροσωπεύουν άμεσες εξαρτήσεις (οι οποίες είναι συχνά αιτιακές συνδέσεις) μεταξύ μεταβλητών, ορίζοντας μια σχέση γονέα – απογόνου. Η σχέση μεταξύ των μεταβλητών (κόμβων) ποσοτικοποιείται με δεσμευμένες κατανομές πιθανότητας (Conditional Probability Distributions, CPDs), όπου η κατάσταση των απογόνων εξαρτάται από τον συνδυασμό των τιμών των γονέων αυτών.

Η μέθοδος αφορά την ανάλυση της πιθανότητας της επικινδυνότητας [28]. Ένα βασικό Μπεϋζιανό δίκτυο περιέχει μεταβλητές που αντιπροσωπεύουν αβέβαια γεγονότα και μπορούν να χρησιμοποιηθούν για την εκτίμηση της πιθανότητας της επικινδυνότητας ή για την εξαγωγή βασικών οδηγών που οδηγούν σε συγκεκριμένες συνέπειες. Ένα BN μπορεί να επεκταθεί για να περιλαμβάνει δράσεις απόφασης, αποτιμήσεις καθώς και αβεβαιότητες, οπότε είναι γνωστό ως διάγραμμα επιρροής, το οποίο μπορεί να χρησιμοποιηθεί για την αξιολόγηση του αντίκτυπου των ελέγχων/μετριασμού της επικινδυνότητας ή για την εκτίμηση των επιλογών παρέμβασης.

5.2.2. Ανάλυση επιχειρηματικού αντίκτυπου (BIA)

Η ανάλυση επιχειρηματικού αντίκτυπου (Business Impact Analysis – BIA) αφορά την ανάλυση των συνεπειών της επικινδυνότητας [28]. Η μέθοδος αναλύει τον τρόπο με τον οποίο τα περιστατικά και τα γεγονότα θα μπορούσαν να επηρεάσουν τις λειτουργίες ενός οργανισμού και προσδιορίζει και ποσοτικοποιεί τις δυνατότητες που θα χρειάζονταν για τη διαχείρισή του.

Συγκεκριμένα, η BIA βοηθά στην κατανόηση:

- της κρισιμότητας των βασικών επιχειρηματικών διαδικασιών, λειτουργιών και συναφών πόρων και των βασικών αλληλεξαρτήσεων που υπάρχουν για έναν οργανισμό,
- πώς απρόσμενα γεγονότα θα επηρεάσουν την επίτευξη κρίσιμων επιχειρηματικών στόχων,
- της απαιτούμενης ικανότητας για τη διαχείριση των επιπτώσεων μιας διακοπής και την ανάκαμψη στα συμφωνημένα επίπεδα λειτουργίας.

Η μέθοδος BIA μπορεί να πραγματοποιηθεί χρησιμοποιώντας ερωτηματολόγια, συνεντεύξεις, δομημένα εργαστήρια ή και συνδυασμό αυτών.

5.2.3. Ανάλυση αιτίας – συνέπειας (CCA)

Η ανάλυση αιτίας – συνέπειας (Cause-Consequence Analysis – CCA) είναι μια αναλυτική τεχνική που χρησιμοποιείται για την καλύτερη κατανόηση των αστοχιών ενός συστήματος. Αξιολογεί την πιθανότητα εμφάνισης μιας αστοχίας εστιάζοντας στα αίτια αυτής και, εν συνεχεία, απεικονίζει μέσω λογικών διαγραμμάτων τα πιθανά αποτελέσματα που προκύπτουν από τους συνδυασμούς των γεγονότων.

Η μέθοδος αφορά την ανάλυση των συνεπειών και της πιθανότητας της επικινδυνότητας [28] και αντιμετωπίζει καλύτερα από ένα δένδρο σφαλμάτων (βλέπε επόμενη ενότητα) τις περιπτώσεις όπου είναι ευκολότερο να αναπτυχθούν ακολουθίες γεγονότων παρά αιτιακές σχέσεις, διότι η ανάλυση δένδρου σφαλμάτων είναι αρκετά εκτενής ή υπάρχουν ξεχωριστές ομάδες που ασχολούνται με διαφορετικά μέρη της ανάλυσης.

5.2.4. Πίνακας Συνέπειας – Πιθανότητας

Ο πίνακας συνέπειας – πιθανότητας (Consequence/likelihood matrix), ο οποίος αναφέρεται και ως πίνακας επικινδυνότητας (risk matrix) ή και ως θερμικός χάρτης (heat map), αφορά την ανάλυση του επιπέδου της επικινδυνότητας [28]. Είναι ένας τρόπος παρουσίασης της επικινδυνότητας σύμφωνα με τις συνέπειες και τις πιθανότητες. Τα χαρακτηριστικά αυτά συνδυάζονται και εμφανίζεται ο βαθμός της επικινδυνότητας. Οι κλίμακες για την πιθανότητα και την συνέπεια παρουσιάζονται στις γραμμές και στις στήλες του πίνακα. Οι κλίμακες μπορεί να έχουν οποιονδήποτε αριθμό βαθμών – οι κλίμακες τριών, τεσσάρων ή πέντε βαθμών είναι οι πιο συνηθισμένες – και μπορεί να είναι ποιοτικές, ημιποσοτικές ή ποσοτικές. Εάν χρησιμοποιούνται αριθμητικές περιγραφές για τον καθορισμό των βημάτων των κλιμάκων, θα πρέπει να είναι συνεπείς με τα διαθέσιμα δεδομένα και να δίνονται μονάδες. Γενικά, για να είναι συνεπής η κλίμακα με τα δεδομένα, κάθε σημείο της κλίμακας θα πρέπει να είναι μιας τάξης μεγέθους μεγαλύτερη από την προηγούμενη.

Η κλίμακα συνεπειών μπορεί να απεικονίζει θετικές ή αρνητικές συνέπειες. Πρέπει να συνδέονται άμεσα με τους στόχους του οργανισμού και να εκτείνονται από τη μέγιστη αξιόπιστη συνέπεια έως τη χαμηλότερη συνέπεια του ενδιαφέροντος. Η κλίμακα πιθανότητας θα πρέπει να καλύπτει το εύρος που σχετίζεται με τα δεδομένα για τους κινδύνους που πρέπει να αξιολογηθούν. Μπορεί να έχει περισσότερους ή λιγότερους από πέντε βαθμούς και οι βαθμολογίες μπορούν να δοθούν ως λέξεις, αριθμοί ή γράμματα. Ο πίνακας μπορεί να έχει πρόσθετα βάρη στις συνέπειες ή στις πιθανότητες ή να είναι συμμετρικός, ανάλογα από το πεδίο εφαρμογής. Στην Εικόνα 13 δίνεται ένα παράδειγμα πίνακα επικινδυνότητας (Πηγή [35]).

Ο πίνακας επικινδυνότητας θα πρέπει να χρησιμοποιείται με ιδιαίτερη προσοχή καθώς, σύμφωνα με το [35], υπόκειται σε αβεβαιότητα (ο πίνακας στην Εικόνα 13 δεν θεωρείται παράδειγμα καλού σχεδιασμού).

		Consequences →				
		A	B	C	D	E
Likelihood →	V	Medium 5	High 10	High 15	Extreme 20	Extreme 25
	IV	Medium 4	Medium 8	High 12	High 16	Extreme 20
	III	Low 3	Medium 6	Medium 9	High 12	Extreme 15
	II	Low 2	Low 4	Medium 6	High 8	Extreme 10
	I	Negligible 1	Low 2	Medium 3	High 4	Extreme 5
Consequence scale 1		Description 1	Description 2	Description 3	Description 4	Description 5

Εικόνα 13 Παράδειγμα πίνακα επικινδυνότητας

5.2.5. Ανάλυση κόστους – οφέλους (CBA)

Η Ανάλυση κόστους – οφέλους (Cost/Benefit Analysis – CBA) σταθμίζει το συνολικό αναμενόμενο κόστος των δυνατών επιλογών έναντι των συνολικών αναμενόμενων οφελών τους, προκειμένου να επιλέξει την πιο αποτελεσματική ή την πιο κερδοφόρα επιλογή. Μπορεί να είναι ποιοτική ή ποσοτική ή να περιλαμβάνει συνδυασμό ποσοτικών και ποιοτικών στοιχείων και μπορεί να εφαρμοστεί σε οποιοδήποτε επίπεδο ενός οργανισμού.

Η μέθοδος αφορά την ανάλυση των συνεπειών της επικινδυνότητας. Χρησιμοποιείται σε επιχειρησιακό και στρατηγικό επίπεδο για να βοηθήσει στη λήψη απόφασης μεταξύ επιλογών. Στις περισσότερες περιπτώσεις αυτές οι επιλογές συνεπάγονται αβεβαιότητα. Στους υπολογισμούς πρέπει να ληφθούν υπόψη τόσο η μεταβλητότητα στην αναμενόμενη παρούσα αξία του κόστους και των οφελών, όσο και η πιθανότητα απροσδόκητων γεγονότων. Για αυτό μπορεί να χρησιμοποιηθεί ανάλυση ευαισθησίας ή ανάλυση Monte Carlo. Μπορεί επίσης να χρησιμοποιηθεί για τη λήψη αποφάσεων σχετικά με την αντιμετώπιση της επικινδυνότητας, για παράδειγμα, αν θα πρέπει να αντιμετωπιστεί, ποιος ο καλύτερος τρόπος αντιμετώπισης και ποιες επιλογές υπάρχουν για βραχυπρόθεσμη ή μακροπρόθεσμη αντιμετώπιση [28].

5.2.6. Ανάλυση διασταυρούμενων επιπτώσεων

Η ανάλυση διασταυρούμενων επιπτώσεων (cross impact analysis) είναι μια μεθοδολογία που σκοπεύει να προσδιορίσει πως οι συσχετίσεις μεταξύ γεγονότων θα έχουν επίπτωση στην πιθανότητα εμφάνισης κάποιου άλλου γεγονότος. Η ανάλυση διασταυρούμενων επιπτώσεων περιλαμβάνει την κατασκευή ενός πίνακα για να δείξει τις αλληλεξαρτήσεις διαφορετικών γεγονότων: στις γραμμές εμφανίζεται το σύνολο γεγονότων που ενδέχεται να προκύψουν και στις στήλες εμφανίζεται το σύνολο γεγονότων που ενδέχεται να επηρεαστούν από τα προηγούμενα γεγονότα. Στη συνέχεια, οι ειδικοί καλούνται να εκτιμήσουν την πιθανότητα κάθε γεγονότος, καθώς επίσης, και τη δεσμευμένη πιθανότητα εμφάνισης ενός γεγονότος δοθέντος ότι θα συμβεί ή δεν θα συμβεί ένα άλλο γεγονός.

Η τεχνική αφορά την ανάλυση του επιπέδου της επικινδυνότητας [28]. Χρησιμοποιείται σε μελέτες πρόβλεψης και ως αναλυτική τεχνική για την πρόβλεψη του τρόπου με τον οποίο διαφορετικοί παράγοντες επηρεάζουν τις μελλοντικές αποφάσεις. Μπορεί να συνδυαστεί με ανάλυση σεναρίων (βλέπε προηγούμενη ενότητα) για να αποφασιστεί ποια από τα σενάρια που παράγονται είναι τα πιο πιθανά. Μπορεί να χρησιμοποιηθεί όταν υπάρχουν πολλαπλοί αλληλοεπιδρώντες κίνδυνοι, για παράδειγμα, σε σύνθετα έργα ή στη διαχείριση επικινδυνότητας που αφορά την ασφάλεια.

5.2.7. Ανάλυση Δένδρου Αποφάσεων

Ένα δέντρο αποφάσεων (decision tree) μοντελοποιεί όλα τα πιθανά μονοπάτια που ακολουθούν από μια αρχική απόφαση που πρέπει να ληφθεί, για παράδειγμα, εάν θα προχωρήσουμε με το Έργο Α ή το Έργο Β. Καθώς προχωρούν τα δύο υποθετικά έργα, ενδέχεται να προκύψει μια σειρά γεγονότων και να χρειαστεί να ληφθούν διαφορετικές προβλέψιμες αποφάσεις. Αυτά παριστάνονται σε μορφή δέντρου, παρόμοια με ένα δέντρο συμβάντων. Η πιθανότητα των γεγονότων μπορεί να εκτιμηθεί μαζί με την αναμενόμενη τιμή ή την χρησιμότητα του τελικού αποτελέσματος κάθε διαδρομής. Οι πληροφορίες σχετικά με την καλύτερη διαδρομή απόφασης είναι λογικά αυτές που παράγουν την καλύτερη αναμενόμενη τιμή που υπολογίζεται ως το γινόμενο όλων των πιθανοτήτων υπό όρους κατά μήκος της

διαδρομής και της τιμής του αποτελέσματος. Η μέθοδος αφορά την ανάλυση των συνεπειών και της πιθανότητας της επικινδυνότητας [28].

5.2.8. Ανάλυση Δένδρου Συμβάντων (ETA)

Η Ανάλυση Δένδρου Συμβάντων (Event Tree Analysis – ETA) είναι μια τεχνική που στοχεύει στη δενδρική αναπαράσταση των αμοιβαία αποκλειόμενων αλληλουχιών γεγονότων που θα μπορούσαν να προκύψουν μετά από ένα αρχικό συμβάν. Το δέντρο απεικονίζει όλα τα δυνατά αποτελέσματα ανάλογα με το αν λειτουργούν ή όχι τα διάφορα συστήματα ελέγχου. Το δέντρο μπορεί να ποσοτικοποιηθεί για να παρέχει τις πιθανότητες των διαφορετικών πιθανών αποτελεσμάτων. Η μέθοδος αφορά την ανάλυση των συνεπειών της επικινδυνότητας [28]. Μελετώντας όλα τα σχετικά γεγονότα (που έχουν εντοπιστεί με προκαταρκτική ανάλυση κινδύνου, HAZOP ή κάποια άλλη τεχνική), η μέθοδος ETA μπορεί να χρησιμοποιηθεί για τον εντοπισμό όλων των πιθανών σεναρίων και ακολουθιών ατυχημάτων σε ένα σύνθετο σύστημα.

5.2.9. Ανάλυση Τρόπων Αστοχίας και Αποτελεσμάτων (FMEA)

Η μέθοδος αφορά την ανάλυση των συνεπειών της επικινδυνότητας. Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.2.10. Ανάλυση Κρισιμότητας Τρόπων Αστοχίας και Αποτελεσμάτων (FMECA)

Η μέθοδος αφορά την ανάλυση των συνεπειών, της πιθανότητας και του επιπέδου της επικινδυνότητας. Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.2.11. Ανάλυση Δένδρου Βλαβών (FTA)

Η Ανάλυση Δένδρου Βλαβών (Fault Tree Analysis – FTA) είναι μια τεχνική για τον εντοπισμό και την ανάλυση παραγόντων που συμβάλλουν σε ένα καθορισμένο ανεπιθύμητο γεγονός (το γεγονός κορυφής). Αυτοί οι παράγοντες μπορεί να είναι αστοχίες υλικού ή λογισμικού, ανθρώπινα σφάλματα ή άλλα σχετικά γεγονότα. Η λογική σχέση μεταξύ αυτών των αιτιών αντιπροσωπεύεται από έναν αριθμό Λογικών πυλών όπως πύλες AND και OR. Στη συνέχεια, κάθε αιτία αναλύεται σταδιακά με τον ίδιο τρόπο έως ότου η περαιτέρω ανάλυση καταστεί μη παραγωγική. Το αποτέλεσμα αναπαρίσταται σε ένα δενδρικό διάγραμμα το οποίο αποτελεί την γραφική αναπαράσταση μιας εξίσωσης Boole. Η μέθοδος αφορά την ανάλυση της

πιθανότητας της επικινδυνότητας [28] και χρησιμοποιείται επίσης για την εκτίμηση αξιοπιστίας σύνθετων συστημάτων [36].

5.2.12. Διάγραμμα Συχνοτήτων – Αριθμών

Ένα διάγραμμα συχνοτήτων – αριθμών (Frequency-Number diagram, F-N diagram) είναι μια ειδική περίπτωση ενός πίνακα ποσοτικής συνέπειας/πιθανότητας (δείτε προηγούμενη ενότητα) όπου ο άξονας Χ αντιπροσωπεύει τον αθροιστικό αριθμό των κινδύνων και ο άξονας Υ τη συχνότητα με την οποία συμβαίνουν. Και στους δύο άξονες οι κλίμακες είναι λογαριθμικές για να ταιριάζουν με τυπικά δεδομένα. Τα κριτήρια επικινδυνότητας παρουσιάζονται στο γράφημα ως ευθείες γραμμές, όπου όσο μεγαλύτερη είναι η κλίση της γραμμής, τόσο μεγαλύτερη είναι η αποστροφή για μεγαλύτερο κινδύνων. Η μέθοδος αφορά την ανάλυση των συνεπειών και της πιθανότητας της επικινδυνότητας [28].

5.2.13. Θεωρία Παιγνίων

Η Θεωρία Παιγνίων (Game Theory) είναι ένα μέσο για τη μοντελοποίηση των συνεπειών διαφορετικών πιθανών αποφάσεων, δεδομένου ενός αριθμού πιθανών μελλοντικών καταστάσεων. Οι μελλοντικές καταστάσεις μπορούν να καθοριστούν από διαφορετικό υπεύθυνο λήψης αποφάσεων (π.χ. έναν ανταγωνιστή) ή από ένα εξωτερικό γεγονός, όπως η επιτυχία ή η αποτυχία μιας τεχνολογίας ή μιας δοκιμής. Για παράδειγμα, έστω ότι στόχος είναι να καθοριστεί η τιμή ενός προϊόντος λαμβάνοντας υπόψη τις διαφορετικές αποφάσεις που θα μπορούσαν να ληφθούν από διαφορετικούς φορείς λήψης αποφάσεων (που ονομάζονται παίκτες) σε διαφορετικές χρονικές στιγμές. Ανάλογα με τη συγκεκριμένη χρονική περίοδο μπορεί να υπολογιστεί το κέρδος κάθε παίκτη που συμμετέχει στο παιχνίδι, καθώς επίσης και η στρατηγική με τη βέλτιστη απόδοση για κάθε παίκτη. Η θεωρία παιγνίων μπορεί επίσης να χρησιμοποιηθεί για να προσδιορίσει την αξία των πληροφοριών για τον άλλο παίκτη ή τα διαφορετικά πιθανά αποτελέσματα (π.χ. επιτυχία μιας τεχνολογίας).

Η μέθοδος αφορά την ανάλυση των συνεπειών της επικινδυνότητας. Επιτρέπει την αξιολόγηση της επικινδυνότητας σε περιπτώσεις όπου το αποτέλεσμα ορισμένων αποφάσεων εξαρτάται από τη δράση ενός άλλου παίκτη (π.χ. ενός ανταγωνιστή) ή

από έναν αριθμό πιθανών αποτελεσμάτων (π.χ. εάν μια νέα τεχνολογία θα λειτουργήσει) [28].

Η Θεωρία Παιγνίων αναπτύχθηκε από τον Ούγγρο μαθηματικό John von Neumann, ο οποίος προσέφερε σημαντικά αποτελέσματα σε πολλούς κλάδους των επιστημών, όπως τα μαθηματικά, τα οικονομικά και την πληροφορική (θεωρείται ο πατέρας των σύγχρονων υπολογιστών). Κύριο αντικείμενό της είναι η ανάλυση των αποφάσεων σε καταστάσεις στρατηγικής αλληλεξάρτησης. Βρίσκει εφαρμογή στα οικονομικά, στην πολιτική οικονομία, στην εξελικτική βιολογία, στην ψυχολογία, στην κοινωνιολογία και διάφορες άλλες επιστημονικές περιοχές διάφορες. Σημαντικός παιγνιοθεωρητικός επιστήμονας είναι ο Αμερικανός μαθηματικός και οικονομολόγος John Forbes Nash, γνωστός για την έννοια της ισορροπίας κατά Nash (Nash equilibrium) ο οποίος έχει τιμηθεί με βραβείο Νόμπελ οικονομικών Επιστημών. Στη βιβλιογραφία υπάρχει πληθώρα συγγραμμάτων για θεωρία παιγνίων (ενδεικτικά αναφέρονται τα [37], [38]).

5.2.14. Ανάλυση κινδύνων και κρίσιμων σημείων ελέγχου (HACCP)

Η μέθοδος αφορά την ανάλυση των συνεπειών της επικινδυνότητας. Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.2.15. Ανάλυση ανθρώπινης αξιοπιστίας (HRA)

Η μέθοδος αφορά την ανάλυση των συνεπειών, της πιθανότητας και του επιπέδου της επικινδυνότητας. Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.2.16. Ανάλυση επιπέδων προστασίας (LOPA)

Η Ανάλυση επιπέδων προστασίας (Layers Of Protection Analysis – LOPA) αναλύει τη μείωση της επικινδυνότητας που επιτυγχάνεται με ένα σύνολο ελέγχων. Μπορεί να θεωρηθεί ως μια ειδική περίπτωση της Ανάλυσης Δένδρου Συμβάντων (βλέπε προηγούμενη ενότητα) και μερικές φορές πραγματοποιείται ως συνέχεια της μελέτης HAZOP (βλέπε προηγούμενη ενότητα). Η τεχνική αφορά την ανάλυση των συνεπειών της επικινδυνότητας [28]. Ξεκινώντας από ένα αναγνωρισμένο σενάριο κινδύνου, η μέθοδος LOPA χρησιμοποιεί απλοποιημένους κανόνες για να αξιολογήσει τη συχνότητα των συμβάντων, τα ανεξάρτητα επίπεδα προστασίας και τις συνέπειες για να παρέχει μια εκτίμηση της τάξης μεγέθους της επικινδυνότητας. Στο [39] μπορεί

κανείς να βρει πληροφορίες για την εφαρμογή της μεθόδου σε οποιοδήποτε στάδιο του κύκλου ζωής μιας διεργασίας.

5.2.17. Ανάλυση Markov

Η ανάλυση Markov (Markov analysis) είναι μια ποσοτική τεχνική που μπορεί να εφαρμοστεί σε οποιοδήποτε σύστημα που μπορεί να περιγραφεί με όρους ενός συνόλου διακριτών καταστάσεων και μεταβάσεων μεταξύ τους, υπό την προϋπόθεση ότι η εξέλιξη από την τρέχουσα κατάστασή του δεν εξαρτάται από την κατάστασή του σε οποιαδήποτε στιγμή στο παρελθόν. Συνήθως θεωρείται ότι οι μεταβάσεις μεταξύ των καταστάσεων συμβαίνουν σε καθορισμένα χρονικά διαστήματα με αντίστοιχες πιθανότητες μετάβασης (διακριτή χρονική αλυσίδα Markov). Στην πράξη, αυτό προκύπτει συνήθως εάν το σύστημα εξετάζεται σε τακτά χρονικά διαστήματα για να προσδιοριστεί η κατάστασή του. Σε ορισμένες εφαρμογές οι μεταβάσεις διέπονται από εκθετικά κατανεμημένους τυχαίους χρόνους με αντίστοιχους ρυθμούς μετάβασης (συνεχής χρονική αλυσίδα Markov). Αυτό χρησιμοποιείται συνήθως για αναλύσεις αξιοπιστίας. Οι καταστάσεις και οι μεταβάσεις τους μπορούν να αναπαρασταθούν σε ένα διάγραμμα Markov ή από έναν πίνακα μετάβασης. Η μέθοδος αφορά την ανάλυση του επιπέδου της επικινδυνότητας [28].

5.2.18. Δείκτες επικινδυνότητας

Οι δείκτες επικινδυνότητας (risk indices) παρέχουν ένα μέτρο επικινδυνότητας το οποίο προκύπτει χρησιμοποιώντας μια προσέγγιση βαθμολόγησης και κατηγορηματικές (ordinal) κλίμακες. Προσδιορίζονται οι παράγοντες που πιστεύεται ότι επηρεάζουν το μέγεθος της επικινδυνότητας, βαθμολογούνται και συνδυάζονται χρησιμοποιώντας μια εξίσωση που επιχειρεί να αναπαραστήσει τη σχέση μεταξύ τους. Στις απλούστερες συνθέσεις, οι παράγοντες που αυξάνουν το επίπεδο της επικινδυνότητας πολλαπλασιάζονται μεταξύ τους και διαιρούνται με αυτούς που μειώνουν το επίπεδο της επικινδυνότητας. Όπου είναι δυνατόν, οι κλίμακες και ο τρόπος που συνδυάζονται βασίζονται σε στοιχεία και δεδομένα. Οι μαθηματικοί τύποι δεν μπορούν να εφαρμοστούν σε κατηγορηματικές κλίμακες. Επομένως, μόλις αναπτυχθεί το σύστημα βαθμολόγησης, το μοντέλο θα πρέπει να επικυρωθεί εφαρμόζοντάς το σε ένα σύστημα που είναι καλά κατανοητό. Για την επικύρωση της

μεθόδου θα πρέπει να δοκιμαστούν πολλά διαφορετικά συστήματα για τον υπολογισμό των βαθμολογιών [28]. Αφορά την ανάλυση των συνεπειών και της πιθανότητας της επικινδυνότητας.

5.2.19. Καμπύλη S

Η καμπύλη S (S-curve) είναι η γραφική αναπαράσταση της αθροιστικής συνάρτησης κατανομής πιθανότητας των συνεπειών μιας επικινδυνότητας (η μορφή της έχει το σχήμα S). Η πιθανότητα ότι μια συνέπεια θα υπερβεί μια συγκεκριμένη τιμή προκύπτει άμεσα από την καμπύλη S. Σε ορισμένες περιπτώσεις η κατανομή είναι γνωστή ενώ σε άλλες μπορεί να ληφθεί από δεδομένα ή είναι η έξοδος ενός μοντέλου. Διάφορα πιθανοτικά μέτρα μπορούν να χρησιμοποιηθούν ώστε να εκτιμηθεί το χαμηλό σημείο του εύρους συνεπειών, το πιθανό μέσο και το ανώτερο σημείο του εύρους. Η μέθοδος αφορά την ανάλυση του επιπέδου της επικινδυνότητας [28]. Επιπρόσθετα, οι καμπύλες S χρησιμοποιούνται για την γραφική αναπαράσταση της προόδου των εργασιών ενός έργου με την πάροδο του χρόνου και αποτελούν σημαντικό εργαλείο για την αποτελεσματική διαχείριση έργων [40] καθώς επίσης στην ολική διασφάλιση ποιότητας [41].

5.2.20. Ανάλυση σεναρίων

Η μέθοδος αφορά την ανάλυση των συνεπειών της επικινδυνότητας. Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.2.21. Δομημένη «τι θα γινόταν αν»

Η μέθοδος αφορά την ανάλυση των συνεπειών της επικινδυνότητας. Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.2.22. Τοξικολογική εκτίμηση διακινδύνευσης

Αφορά την ανάλυση των συνεπειών, της πιθανότητας και του επιπέδου της επικινδυνότητας. Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.2.23. Αξία σε Ρίσκο (VaR)

Η Αξία σε Ρίσκο (Value at Risk – VaR) χρησιμοποιείται ευρέως στον χρηματοπιστωτικό τομέα για να παρέχει έναν δείκτη του ποσού της πιθανής ζημίας σε ένα χαρτοφυλάκιο χρηματοοικονομικών περιουσιακών στοιχείων για μια συγκεκριμένη

χρονική περίοδο εντός ενός δεδομένου επιπέδου εμπιστοσύνης. Απώλειες μεγαλύτερες από το VaR υφίστανται μόνο με καθορισμένη μικρή πιθανότητα [28].

Η κατανομή κέρδους και ζημίας προκύπτει συνήθως με προσομοίωση Monte Carlo (βλέπε επόμενη ενότητα), από ιστορικά μοντέλα προσομοίωσης και από αναλυτικές μεθόδους και βασίζονται σε σειρά υποθέσεων ή από συνδυασμό αυτών. Οι συνήθεις μετρήσεις της VaR σχετίζονται με απώλειες μιας ημέρας μέχρι και δύο εβδομάδων, με πιθανότητες απώλειας 1 % και 5 %. Η μέθοδος αφορά την ανάλυση του επιπέδου της επικινδυνότητας.

5.3. Τεχνικές αποτίμησης διακινδύνευσης

Η διαδικασία της αποτίμησης διακινδύνευσης περιλαμβάνει τη σύγκριση των εκτιμώμενων επιπέδων κινδύνου με τα προκαθορισμένα κριτήρια κινδύνου, προκειμένου να προσδιοριστεί η σημασία του επιπέδου και του είδους κάθε κινδύνου.

Η αξιολόγηση κινδύνου χρησιμοποιεί την κατανόηση του κινδύνου που αποκτάται κατά την ανάλυση κινδύνου για τη λήψη αποφάσεων για μελλοντικές ενέργειες. Δεοντολογικά, νομικά, οικονομικά και άλλα ζητήματα, συμπεριλαμβανομένων των αντιλήψεων κινδύνου, αποτελούν επίσης στοιχεία για την απόφαση.

Ο Πίνακας 4 παρουσιάζει τις τεχνικές που μπορούν να εφαρμοστούν κατά το στάδιο της αποτίμησης της διακινδύνευσης. Με πλάγια γραφή εμφανίζονται αυτές που είναι ισχυρά εφαρμόσιμες, τις οποίες και θα περιγράψουμε στη συνέχεια.

ALARP, ALARA and SFAIRP	Human reliability analysis
Bayesian networks	*Monte Carlo simulation*
Bow tie analysis	*Multi-criteria analysis (MCA)*
Cause-consequence analysis	*Pareto charts*
Consequence/likelihood matrix	*Privacy impact analysis/ data protection impact assessment (PIA/DPIA)*
Cross impact analysis	*Reliability centred maintenance*
Decision tree analysis	*Risk indices*
Event tree analysis	*S-curves*

Failure modes and effects and criticality analysis	Scenario analysis
Fault tree analysis	Structured "What if?" (SWIFT)
F-N diagrams	*Toxicological risk assessment*
Game theory	*Value at risk (VaR)*
Hazard analysis and critical control points (HACCP)	

Πίνακας 4 Τεχνικές αποτίμησης διακινδύνευσης σύμφωνα με τον πρότυπο ISO/IEC 31010:2019

5.3.1. ALARP/ALARA και SFAIRP

Τα ακρωνύμια ALARP, ALARA και SFAIRP ενσωματώνουν την αρχή του «ευλόγως εφικτού» (reasonably practicable). Οι αντίστοιχες τεχνικές αναπαριστούν κριτήρια όπου ο έλεγχος για την αποδοχή ή την ανεκτικότητα της επικινδυνότητας βασίζεται στο αν είναι ευλόγως εφικτό να πραγματοποιηθούν περισσότερες ενέργειες ώστε η επικινδυνότητα να μειωθεί κι άλλο. Η τεχνική ALARP απαιτεί το επίπεδο επικινδυνότητας να μειωθεί τόσο χαμηλά όσο είναι ευλόγως εφικτό (as low as reasonable practicable). Αντίστοιχα η ALARA απαιτεί το επίπεδο επικινδυνότητας να μειωθεί τόσο χαμηλά όσο είναι ευλόγως επιτεύξιμο (as low as reasonable achievable). Η τεχνική SFAIRP απαιτεί η ασφάλεια να διασφαλίζεται τόσο όσο είναι ευλόγως εφικτό (so far as is reasonable practicable) [28].

Τα κριτήρια SFAIRP και ALARP στοχεύουν στο ίδιο αποτέλεσμα, ωστόσο διαφέρουν σημασιολογικά. Το ALARP επιτυγχάνει την ασφάλεια καθιστώντας την επικινδυνότητα όσο το δυνατόν χαμηλότερη, ενώ το SFAIRP δεν κάνει καμία αναφορά στο επίπεδο επικινδυνότητας. Το SFAIRP συνήθως ερμηνεύεται ως ένα κριτήριο με το οποίο αξιολογούνται οι έλεγχοι για να διαπιστωθεί εάν είναι δυνατές περαιτέρω θεραπείες και αν ναι, εάν είναι εφικτές. Η έννοια του ALARP εισήχθη για πρώτη φορά από το Στέλεχος Υγείας και Ασφάλειας του Ηνωμένου Βασιλείου. Μια σύντομη περιγραφή της τεχνικής είναι διαθέσιμη στον σύνδεσμο [42].

5.3.2. Μπεϋζιανά δίκτυα

Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.3.3. Ανάλυση διασταυρούμενων επιπτώσεων

Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.3.4. Διάγραμμα Συχνοτήτων – Αριθμών

Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.3.5. Θεωρία Παιγνίων

Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.3.6. Ανάλυση κινδύνων και κρίσιμων σημείων ελέγχου (HACCP)

Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.3.7. Ανάλυση Κρισιμότητας Τρόπων Αστοχίας και Αποτελεσμάτων (FMECA)

Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.3.8. Προσομοίωση Monte Carlo

Κατά την ανάλυση της επικινδυνότητας υπάρχουν υπολογισμοί που περιλαμβάνουν κατανομές. Ωστόσο, η εκτέλεση υπολογισμών με κατανομές δεν είναι εύκολη, καθώς συχνά δεν είναι δυνατή η εξαγωγή αναλυτικών λύσεων, εκτός εάν οι κατανομές έχουν καλά καθορισμένα σχήματα, και κάτω από περιορισμούς και υποθέσεις που μπορεί να μην είναι ρεαλιστικές. Κάτω από αυτές συνθήκες, μπορούν να χρησιμοποιηθούν τεχνικές όπως η προσομοίωση Monte Carlo (Monte Carlo simulation) [28]. Η προσομοίωση συνήθως περιλαμβάνει τη λήψη τυχαίου δείγματος από καθεμία από τις κατανομές εισόδου, την εκτέλεση υπολογισμών για την εξαγωγή μιας τιμής αποτελέσματος και, στη συνέχεια, την επανάληψη της διαδικασίας μέσω μιας σειράς επαναλήψεων για τη δημιουργία μιας κατανομής των αποτελεσμάτων. Το αποτέλεσμα μπορεί να δοθεί ως κατανομή πιθανότητας της τιμής ή κάποιο στατιστικό στοιχείο όπως η μέση τιμή.

Γενικά, η προσομοίωση Monte Carlo μπορεί να εφαρμοστεί σε οποιοδήποτε σύστημα για το οποίο:

- Ένα σύνολο εισόδων αλληλεπιδρούν για να ορίσουν μια έξοδο.
- Η σχέση μεταξύ των εισόδων και των εξόδων μπορεί να εκφραστεί ως ένα σύνολο εξαρτήσεων.
- Οι αναλυτικές τεχνικές δεν είναι σε θέση να παρέχουν σχετικά αποτελέσματα ή όταν υπάρχει αβεβαιότητα στα δεδομένα εισόδου.

Η προσομοίωση Monte Carlo μπορεί να χρησιμοποιηθεί ως μέρος της αξιολόγησης της επικινδυνότητας για δύο διαφορετικούς σκοπούς:

- Τη διάδοση της αβεβαιότητας σε συμβατικά αναλυτικά μοντέλα.
- Τους πιθανοτικούς υπολογισμούς όταν οι αναλυτικές τεχνικές δεν λειτουργούν ή δεν είναι εφικτές.

Για περισσότερες πληροφορίες αναφορικά με τις αρχές της μεθόδου Monte Carlo, μπορεί κανείς να ανατρέξει στο [43].

5.3.9. Ανάλυση Πολλαπλών Κριτηρίων (MCA)

Η τεχνική της Ανάλυσης Πολλαπλών Κριτηρίων (Multi-criteria analysis – MCA) χρησιμοποιεί μια σειρά κριτηρίων για να αποτιμήσει και να αξιολογήσει με διαφάνεια και να συγκρίνει τη συνολική απόδοση ενός συνόλου επιλογών. Γενικά, ο στόχος είναι να παραχθεί μια σειρά προτίμησης για ένα σύνολο επιλογών. Η ανάλυση περιλαμβάνει την ανάπτυξη μιας μήτρας επιλογών και κριτηρίων που ταξινομούνται και συγκεντρώνονται για να παρέχουν μια συνολική βαθμολογία για κάθε επιλογή [28]. Σε γενικές γραμμές η διαδικασία που ακολουθείται είναι η εξής:

- Καθορισμός των στόχων και των χαρακτηριστικών (κριτήρια ή μέτρα λειτουργικής απόδοσης) που σχετίζονται με κάθε στόχο.
- Ιεράρχηση των χαρακτηριστικών σύμφωνα με τις αναγκαίες και επιθυμητές απαιτήσεις.
- Προσδιορισμός της σπουδαιότητας κάθε κριτηρίου και ορισμός σταθμίσεων (βαρών) σε κάθε κριτήριο.
- Συναίνεση των ενδιαφερομένων μερών για την σταθμισμένη ιεραρχία.
- Αξιολόγηση εναλλακτικών λύσεων σε σχέση με τα κριτήρια (μέσω ενός πίνακα βαθμολογιών).
- Συνδυασμός πολλαπλών βαθμολογιών κάθε χαρακτηριστικού σε μια συνολική σταθμισμένη βαθμολογία πολλαπλών χαρακτηριστικών.
- Αξιολόγηση των αποτελεσμάτων για κάθε επιλογή.

- Αξιολόγηση της ευρωστίας της κατάταξης των επιλογών μέσω ανάλυσης ευαισθησίας (sensitivity analysis) προκειμένου να διερευνηθεί το αντίκτυπο της αλλαγής της στάθμισης της ιεραρχίας των χαρακτηριστικών.

Ένας πρακτικός οδηγός ανάλυσης πολλαπλών κριτηρίων είναι διαθέσιμος στο [44].

5.3.10. Διαγράμματα Pareto

Ένα διάγραμμα Pareto (Pareto chart) είναι ένα εργαλείο για την επιλογή ενός αριθμού εργασιών που θα παράγουν σημαντικό συνολικό αποτέλεσμα. Χρησιμοποιεί την αρχή Pareto (γνωστή και ως κανόνας 80/20) σύμφωνα με την οποία το 80% των προβλημάτων παράγονται από το 20% των αιτιών ή, διαφορετικά, κάνοντας το 20% της εργασίας μπορεί κανείς να αποφέρει το 80% του οφέλους [28].

Σκοπός της ανάλυσης Pareto είναι να διαχωρίσει τις σημαντικές πλευρές ενός προβλήματος από τις λιγότερο σημαντικές. Απεικονίζοντας γραφικά τις πιο σημαντικές πλευρές ενός προβλήματος, μπορούμε να επικεντρώνουμε τις προσπάθειές μας στην επίλυση αυτών. Όταν οι προσπάθειες έχουν ως στόχο τον περιορισμό των πιο σημαντικών πλευρών ενός προβλήματος, τότε συνολικά έχουμε σημαντική βελτίωση του προβλήματος. Σε περίπτωση που οι προσπάθειες είχαν επικεντρωθεί σε πλευρές του προβλήματος που δεν ήταν τόσο σημαντικές, τότε το αποτέλεσμα θα ήταν να έχουμε πάλι βελτίωση του προβλήματος, αλλά όχι τόσο μεγάλη όπως στην πρώτη περίπτωση [29].

5.3.11. Εκτίμηση Αντικτύπου Ιδιωτικότητας (PIA) / Εκτίμηση Αντικτύπου Προστασίας Δεδομένων (DPIA)

Η μέθοδος εκτίμησης αντικτύπου ιδιωτικότητας (ιδιωτικού απορρήτου) (Privacy Impact Assessment – PIA) καθώς επίσης και η μέθοδος εκτίμησης αντικτύπου προστασίας δεδομένων (Data Protection Impact Assessment – DPIA) αναλύουν τον τρόπο με τον οποίο τα περιστατικά και τα γεγονότα θα μπορούσαν να επηρεάσουν το απόρρητο των προσωπικών δεδομένων και προσδιορίζουν και ποσοτικοποιούν τις δυνατότητες που θα απαιτούνται για τη διαχείρισή του. Πρόκειται για διαδικασίες για την αξιολόγηση μιας πρότασης για τον εντοπισμό των πιθανών επιπτώσεων στο απόρρητο και τα προσωπικά δεδομένα των υποκειμένων [28].

Οι μέθοδοι PIA και DPIA βοηθούν τους οργανισμούς να εντοπίζουν, να αξιολογούν και να αντιμετωπίζουν την επικινδυνότητα που σχετίζεται με δραστηριότητες επεξεργασίας δεδομένων. Είναι ιδιαίτερα σημαντικό να εφαρμόζονται όταν εισάγεται μια νέα διαδικασία, σύστημα ή τεχνολογία επεξεργασίας δεδομένων στον οργανισμό. Αποτελούν αναπόσπαστο μέρος της προσέγγισης «ιδιωτικότητα βάσει σχεδιασμού» (Privacy by Design). Η DPIA βοηθά επίσης τους οργανισμούς να συμμορφωθούν με τις απαιτήσεις των ρυθμιστικών αρχών προστασίας δεδομένων (όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης, GDPR) και αποδεικνύουν ότι έχουν ληφθεί τα κατάλληλα μέτρα για τη διασφάλιση της συμμόρφωση με αυτές[3].

Συγκεκριμένα, οι μέθοδοι:

- Αναλύουν τις πιθανές συνέπειες μιας παραβίασης της ιδιωτικότητας των προσωπικών δεδομένων ενός υποκειμένου.
- Λαμβάνουν υπόψη εάν η επεξεργασία προσωπικών πληροφοριών ενέχει υψηλό κίνδυνο σε περίπτωση παραβίασης της ιδιωτικότητας προσωπικών δεδομένων.
- Εκτελούν μια εις βάθος ανάλυση επικινδυνότητας για την επεξεργασία προσωπικών δεδομένων.

Οι μέθοδοι PIA και DPIA μπορούν να πραγματοποιηθούν χρησιμοποιώντας ερωτηματολόγια, συνεντεύξεις, δομημένα εργαστήρια ή συνδυασμό αυτών, χρησιμοποιώντας τις οδηγίες της Ομάδας Εργασίας του Άρθρου 29 της ΕΕ [18] και διάφορα πρότυπα που αναπτύχθηκαν, για παράδειγμα, από την Αρχή Προστασίας Δεδομένων του Ηνωμένου Βασιλείου (Information Commissioner ’s Office – ICO) και την Αρχή Προστασίας Δεδομένων της Γαλλίας (Commission Nationale de l’Informatique et des Libertés – CNIL).

[3] Στην παρούσα ενότητα κάνουμε μια σύντομη αναφορά στην μέθοδο DPIA. Εκτενή αναφορά σε αυτήν, στον ΓΚΠΔ και στις κατευθυντήριες γραμμές για την εφαρμογή της DPIA θα κάνουμε στο επόμενο κεφάλαιο.

5.3.12. Συντήρηση με επίκεντρο την αξιοπιστία

Η συντήρηση με επίκεντρο την αξιοπιστία (Reliability Centred Maintenance – RCM) χρησιμοποιείται για τον προσδιορισμό των κατάλληλων πολιτικών και εργασιών συντήρησης για ένα σύστημα και τις συνιστώσες, ώστε να επιτυγχάνεται αποτελεσματικά και αποδοτικά η απαιτούμενη ασφάλεια, διαθεσιμότητα και οικονομία λειτουργίας για όλους τους τύπους εξοπλισμού. Περιλαμβάνει όλα τα στάδια της διαδικασίας για την πραγματοποίηση εκτίμησης διακινδύνευσης, συμπεριλαμβανομένου της αναγνώρισης, της ανάλυσης και της αξιολόγησης επικινδυνότητας [28].

Τα βασικά βήματα ενός προγράμματος RCM είναι:

- Έναρξη και σχεδιασμός.
- Ανάλυση λειτουργιών αστοχιών.
- Επιλογή εργασιών συντήρησης.
- Υλοποίηση.
- Συνεχής βελτίωση.

Η ανάλυση λειτουργικών αστοχιών πραγματοποιείται συνήθως με την εκτέλεση της Ανάλυση Κρισιμότητας Τρόπων Αστοχίας και Αποτελεσμάτων FMECA (βλέπε προηγούμενη ενότητα) εστιάζοντας σε καταστάσεις όπου οι πιθανές αστοχίες μπορούν να εξαλειφθούν ή να μειωθούν σε συχνότητα και/ή συνέπεια με την εκτέλεση εργασιών συντήρησης. Οι συνέπειες καθορίζονται με τον καθορισμό των επιπτώσεων αστοχίας και στη συνέχεια η επικινδυνότητα αναλύεται με εκτίμηση της συχνότητας κάθε τρόπου αστοχίας χωρίς να πραγματοποιηθεί συντήρηση. Ο καθορισμός των κατηγοριών για τα επίπεδα της επικινδυνότητας πραγματοποιείται μέσω ενός πίνακα επικινδυνότητας (βλέπε προηγούμενη ενότητα).

5.3.13. Δείκτες επικινδυνότητας

Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.3.14. Καμπύλη S

Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.3.15. Τοξικολογική εκτίμηση διακινδύνευσης

Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

5.3.16. Αξία σε Ρίσκο (VaR)

Η περιγραφή της μεθόδου δόθηκε σε προηγούμενη ενότητα.

6. Γενικός Κανονισμός Προστασίας Δεδομένων και Εκτίμηση Αντικτύπου Προστασίας Δεδομένων

6.1. Η ασφάλεια της επεξεργασίας των προσωπικών δεδομένων

Στο άρθρο 32 του Γενικού Κανονισμού Προστασίας Δεδομένων [14] ορίζονται οι απαιτήσεις για την ασφάλεια της επεξεργασίας. Σε αντίθεση με το νομικό τοπίο έως τον Μάιο του 2018, το σύστημα για τον καθορισμό των κατάλληλων τεχνικών και οργανωτικών μέτρων βασίζεται πλέον ρητά στην αξιολόγηση της επικινδυνότητας που έχει εντοπιστεί. Σύμφωνα με την παρ. 1 του άρθρου 32, ο υπεύθυνος της επεξεργασίας και ο εκτελών την επεξεργασία θα πρέπει να διασφαλίζουν ότι λαμβάνουν τα κατάλληλα μέτρα για την προστασία των προσωπικών δεδομένων:

«Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων.»

Ο υπεύθυνος επεξεργασίας (controller) είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους. Ο εκτελών την επεξεργασία (processor) είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας. Τέλος, ο Υπεύθυνος Προστασίας Δεδομένων (Data Processing Officer - DPO) είναι το φυσικό ή νομικό πρόσωπο που έχει ρόλο συμβουλευτικό προς τους παραπάνω, παρακολουθεί τη συμμόρφωση με τον κανονισμό, και συνεργάζεται με την εποπτική αρχή. Ως επεξεργασία δεδομένων (data processing) θεωρούμε κάθε

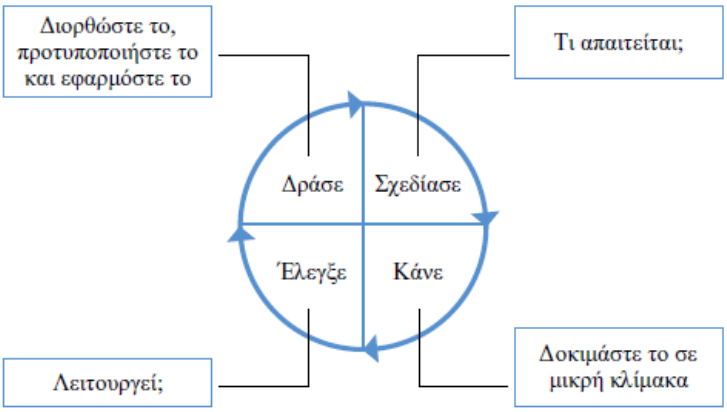
πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

Η εκτίμηση της επικινδυνότητας και η υιοθέτηση μέτρων δεν προέκυψε ως απαίτηση του ΓΚΠΔ. Οι εταιρίες και οι οργανισμοί είχαν υιοθετήσει και εφαρμόσει ΣΔΑΠ πριν τον Μάιο του 2018, προκειμένου να συμμορφώνονται με το πρότυπο ISO 27001. Ωστόσο, η προσέγγιση που ακολουθείται στον ΓΚΠΔ για την προστασία δεδομένων διαφέρει κάπως από αυτήν που αφορά την ασφάλεια πληροφοριών. Στην προστασία δεδομένων και την ασφάλεια των πληροφοριών, χρησιμοποιούμε τις ίδιες αρχές για να αξιολογήσουμε την ασφάλεια των προσωπικών δεδομένων και την ασφάλεια των πληροφοριών (πρόκειται για την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα που περιγράψαμε στο Κεφάλαιο 2). Ωστόσο η αξιολόγηση αυτών γίνεται από διαφορετικές οπτικές γωνίες, δηλαδή, στην ασφάλεια πληροφοριών μας ενδιαφέρει η πρόσβαση από τρίτα μέρη ενώ στην προστασία δεδομένων μας ενδιαφέρουν τα υποκείμενα των δεδομένων. Λόγω των διαφορετικών οπτικών, τα αποτελέσματα που προκύπτουν από την ασφάλεια των πληροφοριών δεν μπορούν απλώς να υιοθετηθούν για την προστασία δεδομένων, υπό την προϋπόθεση ότι οι κίνδυνοι για τις ελευθερίες και τα δικαιώματα των υποκειμένων των δεδομένων δεν έχουν ήδη ληφθεί επαρκώς υπόψη στην υπάρχουσα μεθοδολογία. Τα αποτελέσματα της αξιολόγησης κινδύνου προστασίας δεδομένων και ασφάλειας πληροφοριών μπορεί να συμπίπτουν, αλλά όχι απαραίτητα.

Παράδειγμα. Ένα εκπαιδευτικό ίδρυμα χρησιμοποιεί μια ηλεκτρονική εφαρμογή υποβολής αιτήσεων συνεργαζόμενου εκπαιδευτικού προσωπικού. Μέσω της εφαρμογής αυτής οι αιτούντες μπορούν να καταχωρούν την αίτηση τους αλλά και να ενημερώσουν τα δεδομένα αυτής. Ωστόσο, η μέθοδος αυθεντικοποίησης των χρηστών για τον έλεγχο της ταυτότητας τους είναι αδύναμη επειδή το όνομα χρήστη (username) αντιστοιχεί στη διεύθυνση ηλεκτρονικού ταχυδρομείου (email) του

αιτούντος και δεν υπάρχουν περιορισμοί σχετικά με το μήκος και την πολυπλοκότητα του κωδικού εισόδου (password). Σε περίπτωση παραβίασης του λογαριασμού του χρήστη, μια απλή θεώρηση της πιθανής απώλειας για το ίδρυμα θα καθόριζε χαμηλό κίνδυνο όσον αφορά την απώλεια του απορρήτου καθώς το ίδρυμα δεν θα υποστεί άμεση ζημία. Ωστόσο, βάσει του άρθρου 32 του ΓΚΠΔ, θα πρέπει να ληφθεί υπόψη και η πιθανή ζημία (π.χ. οικονομική) για το υποκείμενο των δεδομένων, καθώς όλες οι πληροφορίες και τα έγγραφα της αίτησης του θα είναι πλέον δημοσίως γνωστά. Επομένως, αυτό μπορεί να οδηγήσει σε αλλαγή του αποτελέσματος της αξιολόγησης επικινδυνότητας και, ως εκ τούτου, να απαιτήσει περαιτέρω μέτρα διαχείρισης αυτής.

Σύμφωνα με την παρ. 1(δ) του άρθρου 32 του ΓΚΠΔ [14], θα πρέπει οι οργανισμοί να τηρούν «διαδικασία για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας». Συνεπώς οι οργανισμοί είναι υποχρεωμένοι στην τήρηση κατάλληλων διαδικασιών και μάλιστα σε τακτική βάση. Οι διαδικασίες αυτές απαιτούν συνέργεια ενός μοντέλου για τη διαρκή βελτίωση της πολιτικής ασφάλειας και του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών του οργανισμού.

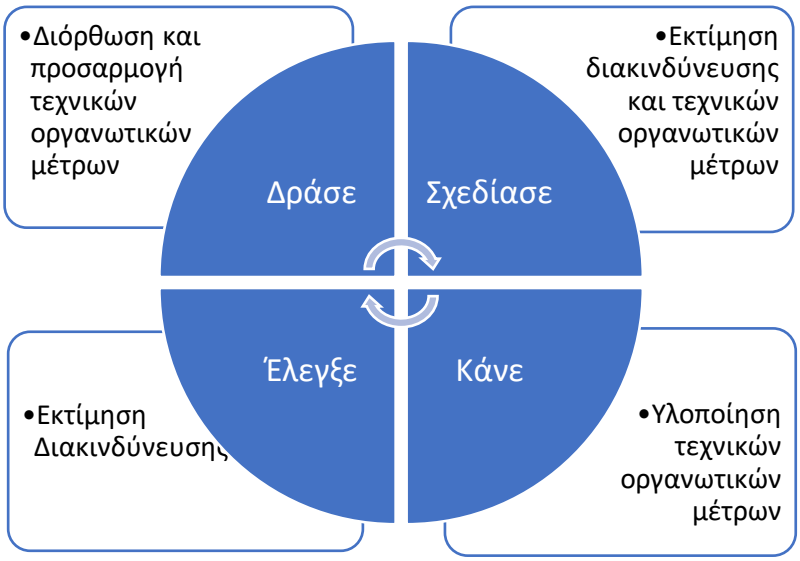


Εικόνα 14 Ο κύκλος του Deming

Το πιο συχνά χρησιμοποιούμενο μοντέλο είναι το μοντέλο Plan-Do-Check-Act (PDCA) η διαφορετικά ο κύκλος του Deming (Εικόνα 14, Πηγή [30]). Ο Δρ.Wiliam Edwards Deming (1900-1993) είναι πιθανότατα ο πλέον αξιοσέβαστος «γκουρού» στο χώρο της Ολικής Ποιότητας. Το μοντέλο PDCA προτάθηκε για τη βελτίωση διαδικασιών

παραγωγής, ωστόσο, χρησιμοποιείται για όλα τα είδη διαδικασιών συμπεριλαμβανομένης και της ασφάλειας πληροφοριών. Μάλιστα, ήταν υποχρεωτική μέθοδος στην έκδοση 2005 του ISO 27001.

Στην Εικόνα 15 (Πηγή [45]) βλέπουμε την εφαρμογή του μοντέλου PDCA στην ασφάλεια πληροφοριών. Η συγχώνευση του μοντέλου PDCA με τη διαδικασία διαχείρισης της ασφάλειας πληροφοριών και το ΣΔΑΠ ενός οργανισμού είναι ιδιαίτερα ευαίσθητη λόγο της εγγύτητας του προτύπου ISO/IEC 27001 και των απαιτήσεων ασφαλείας για την επεξεργασία προσωπικών δεδομένων. Το γεγονός αυτό δημιουργεί σημαντικές συνέργειες στην εκτίμηση και την αντιμετώπιση της επικινδυνότητας και την εφαρμογή των μέτρων, αλλά αυξάνει και την αποδοχή των απαιτήσεων επικινδυνότητας στον οργανισμό.



Εικόνα 15 Ο κύκλος του Deming στην προστασία δεδομένων

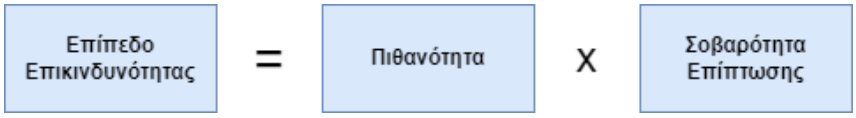
6.2. Η υλοποίηση της διαδικασίας ασφάλειας επεξεργασίας

Για τη συμμόρφωση του οργανισμού σύμφωνα με το πρότυπο ISO/IEC 27001 υιοθετείται ένα ΣΔΑΠ και ακολουθείται η διαδικασία διαχείρισης διακινδύνευσης που περιγράψαμε στο Κεφάλαιο 3. Κατά την προετοιμασία της διαδικασίας, πρέπει να εξεταστούν και να αποφασιστούν δύο σημαντικά σημεία: (α) ποιος είναι ο σκοπός της εκτίμησης της διακινδύνευσης και (β) ποια μεθοδολογία/τεχνική θα

χρησιμοποιηθεί. Η διαδικασία διακινδύνευσης για την προστασία των δεδομένων θα μπορούσε να είναι η ακόλουθη:

- Καθορισμός πλαισίου
- Αναγνώριση διακινδύνευσης
- Ανάλυση διακινδύνευσης
- Αξιολόγηση διακινδύνευσης
- Αντιμετώπιση διακινδύνευσης
- Παρακολούθηση διακινδύνευσης

Τα στάδια αυτά μπορούν να υλοποιηθούν με οποιαδήποτε από τις τεχνικές/μεθόδους που παρουσιάσαμε στο Κεφάλαιο 5. Για παράδειγμα, ο ΓΚΠΔ δεν προσδιορίζει κάποια μέθοδο για την ανάλυση της διακινδύνευσης. Στην ασφάλεια πληροφοριών η διακινδύνευση εξετάζεται σε σχέση με μια πιθανή ζημία για την εταιρεία. Στην προστασία των δεδομένων, σύμφωνα με τον ΓΚΠΔ, το επίπεδο διακινδύνευσης εξαρτάται από τον αντίκτυπό του στα υποκείμενα των δεδομένων. Η πιθανότητα (likelihood) στην ασφάλεια πληροφοριών, εστιάζει στις αδυναμίες που έχει ένα σύστημα και στην σοβαρότητα της επίπτωσης (severity) που έχει η εκμετάλλευση αυτών των αδυναμιών. Αυτό διαφέρει από την αξιολόγηση του επιπέδου επικινδυνότητας για την προστασία των δεδομένων. Έτσι το επίπεδο επικινδυνότητας (risk level) μπορεί να οριστεί ως το γινόμενο της πιθανότητας (likelihood) επί την σοβαρότητα της επίπτωσης (severity) σύμφωνα με την Εικόνα 16 (Πηγή [45]).



Εικόνα 16 Ορισμός του επιπέδου επικινδυνότητας στην προστασία δεδομένων

Πρωταρχικό αγαθό στην προστασία δεδομένων είναι τα προσωπικά δεδομένα των υποκειμένων, ωστόσο παράλληλα προστατεύονται και τα υποστηρικτικά αγαθά, όπως το υλικό, το λογισμικό, τα δίκτυα μεταφοράς δεδομένων, τα έγγραφα, οι χρήστες κ.α. Οι πηγές επικινδυνότητας (ανθρώπινες ή φυσικές) πραγματοποιούν ενέργειες (actions) ενάντια στα υποστηρικτικά αγαθά, οι οποίες με τη σειρά τους

μπορεί να οδηγήσουν σε παραβίαση των δεδομένων. Το σενάριο που μόλις περιγράψαμε είναι μια διακριτή απειλή (threat).

Παράδειγμα. Ένας υπάλληλος (πηγή κινδύνου) μιας εταιρίας χρησιμοποιεί υλικό (υποστηριζόμενο αγαθό) στο οποίο υποβάλλονται σε επεξεργασία προσωπικά δεδομένα σε αντίθεση με τη καθορισμένη χρήση (ενέργεια). Αυτό σημαίνει απώλεια των προσωπικών δεδομένων (επικινδυνότητα προστασίας δεδομένων). Η διακριτή απειλή είναι η εξής: Ένας υπάλληλος χρησιμοποιεί εταιρικό υλικό για προσωπικούς σκοπούς.

6.2.1. Εμπλοκή μελών ανώτατης διοίκησης

Η υλοποίηση της ασφάλειας πληροφοριών ξεκινά με την συμμετοχή των μελών της ανώτατης διοίκησης του οργανισμού. Η ανώτατη διοίκησης εγκρίνει αποφάσεις αναφορικά με την εκτίμηση και την αποδοχή της επικινδυνότητας. Θα πρέπει να λαμβάνει αναφορές με τα αποτελέσματα εσωτερικών ελέγχων και να τεκμηριώνει συστηματικά πρακτικά συναντήσεων, εσωτερικούς οδηγούς και πιστοποιητικά εκπαίδευσης.

6.2.2. Ορισμός ομάδας έργου

Στη συνέχεια θα πρέπει να καθοριστεί μια ομάδα έργου εφοδιασμένη με τις απαραίτητες ικανότητες και πόρους από τη διοίκηση του οργανισμού. Αυτό μπορεί να γίνει με την υιοθέτηση μιας πολιτικής διαχείρισης επικινδυνότητας που θα ορίζει ποιος είναι υπεύθυνος για τη διεξαγωγή της εκτίμησης διακινδύνευσης (την ασφάλεια της επεξεργασίας και την μελέτη εκτίμησης σχετικά με την προστασία των δεδομένων (DPIA)),

- ποιος παρέχει πληροφορίες και αξιολογεί τους κινδύνους προστασίας δεδομένων,
- ποιος είναι ο υπεύθυνος επεξεργασίας,
- πόσο συχνά πραγματοποιείται η επιχειρηματική διαδικασία,
- ποια είναι η μεθοδολογία/τεχνική εκτίμηση της επικινδυνότητας,
- ποιες είναι διαθέσιμες ισχύουσες επιλογές αντιμετώπισης της επικινδυνότητας,

- τι θα συμβεί μετά την ανάλυση των αποτελεσμάτων της εκτίμησης της διακινδύνευσης.

6.2.3. Προσδιορισμών εσωτερικού και εξωτερικού πλαισίου

Με τα δεδομένα των υποκειμένων σχετίζονται απαιτήσεις οι οποίες θα πρέπει να προσδιοριστούν. Τέτοιες απατήσεις για την προστασία των δεδομένων μπορεί να αποτελούν:

- Απαιτήσεις από το διεθνές ή το εθνικό δίκαιο, δικαστικές αποφάσεις και κανονισμοί
- Συμβατικές υποχρεώσεις (π.χ., επεξεργασία δεδομένων για λογαριασμό του υπεύθυνου επεξεργασίας)
- Επιχειρηματικοί παράγοντες (π.χ., κώδικες δεοντολογίας, βιομηχανικά πρότυπα)
- Συστήματα εσωτερικού ελέγχου και τεχνικές προδιαγραφές

6.2.4. Σκοπός της εκτίμησης της επικινδυνότητας

Ακολουθεί ο ορισμός τους σκοπού της εκτίμησης της διακινδύνευσης όπου θα πρέπει να ληφθούν υπόψη επιχειρηματικές διαδικασίες, εφάπαξ ενέργειες ή έργα από τον υπεύθυνο επεξεργασίας καθώς και οι πληροφοριακές υποδομές (λογισμικό, υλικό, δίκτυο). Χρήσιμη είναι η δημιουργία ενός αρχείου καταγραφής δραστηριοτήτων επεξεργασίας με σαφείς οδηγίες του υπευθύνου επεξεργασίας στον εκτελών την επεξεργασία για τον τρόπο επεξεργασίας των δεδομένων.

6.2.5. Αναγνώριση της επικινδυνότητας

Για την αναγνώριση της επικινδυνότητας στην ασφάλεια επεξεργασίας αρκεί να αναγνωριστούν οι κίνδυνοι που συνεπάγονται παραβίαση των στόχων που έχουν ήδη προσδιοριστεί. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία πρέπει να προσδιορίσει τους κινδύνους προστασίας δεδομένων που είναι εγγενείς στη δραστηριότητα επεξεργασίας δεδομένων. Για τον εντοπισμό κινδύνων, τα ακόλουθα βήματα θα πρέπει να ταξινομούν τις πηγές κινδύνου, τα περιουσιακά στοιχεία (συμπεριλαμβανομένων πληροφοριών, προσωπικών δεδομένων, συστημάτων κ.λπ.), τις απειλές και τις αδυναμίες, καθώς και τους πιθανούς κινδύνους επιπτώσεων και

προστασίας δεδομένων. Για το στάδιο αυτό μπορούν να χρησιμοποιηθούν τεχνικές που αναφέρθηκαν στην ενότητα 5.1.

6.2.6. Ανάλυση της επικινδυνότητας

Στην ανάλυση της επικινδυνότητας αρχικά θα πρέπει να εντοπιστούν και να τεκμηριωθούν τα υπάρχοντα μέτρα για την πρόληψη της παραβίασης της εμπιστευτικότητας, της διαθεσιμότητας ή της ακεραιότητας. Στη συνέχεια θα πρέπει να ληφθούν υπόψη

- οι απειλές και οι πηγές επικινδυνότητας,
- οι συνέπειες από την παραβίαση της ασφάλειας των δεδομένων των υποκειμένων,
- ο προσδιορισμός των σχετικών πηγών,
- η εκτίμηση της σοβαρότητας των επιπτώσεων, και
- η εκτίμηση της πιθανότητας.

Απειλές και πηγές επικινδυνότητας

Οι πηγές επικινδυνότητας μπορεί να είναι εσωτερικές, εξωτερικές ή άλλες (πυρκαγιά, πλημύρα, φυσικές καταστροφές). Για την εκτίμηση μιας πηγής επικινδυνότητας είναι χρήσιμο να γνωρίσουμε το εσωτερικό ή εξωτερικό κίνητρο. Έτσι, θα πρέπει να τεκμηριωθεί η πηγή επικινδυνότητας (ο τύπος αυτής) και το κίνητρο. Στη συνέχεια ακολουθεί η αναγνώριση των απειλών και η κατάταξη τους στις πηγές επικινδυνότητας. Ο Πίνακας 5 (Πηγή [45]) παρουσιάζει ένα παράδειγμα αναγνώρισης και τεκμηρίωσης πηγών επικινδυνότητας. Για την ανάλυση της επικινδυνότητας μπορούν να χρησιμοποιηθούν τεχνικές που αναφέρθηκαν στην ενότητα 5.3.

Επίπτωση στην παραβίαση της ασφάλειας δεδομένων

Τρεις μορφές επίπτωσης θα πρέπει να θεωρήσουμε στην παραβίαση της ασφάλειας των δεδομένων των υποκειμένων:

- Μη εξουσιοδοτημένη πρόσβαση σε προσωπικά δεδομένα
- Ανεπιθύμητη τροποποίηση προσωπικών δεδομένων
- Απώλεια προσωπικών δεδομένων

Πηγές Επικινδυνότητας (Τύπος)			**Σχετιζόμενες πηγές επικινδυνότητας**	**Περιγραφή της δραστικότητας της πηγής επικινδυνότητας**
Ανθρώπινη	Εσωτερική	Τυχαία	εργαζόμενοι, διευθυντές, διαχειριστές ΠΣ	Οι σχετιζόμενες πηγές επικινδυνότητας δεν χρησιμοποιούν πηγές για τυχαίες ενέργειες.
		Εσκεμμένα		Οι σχετιζόμενες πηγές επικινδυνότητας χρησιμοποιούν ελάχιστες πηγές για εσκεμμένες ενέργειες (π.χ. σε ένα γεγονός τερματισμού ή προειδοποίησης).
	Εξωτερική	Τυχαία	διαχειριστές ΠΣ, ανταγωνιστές, χάκερς	Οι σχετιζόμενες πηγές επικινδυνότητας δεν χρησιμοποιούν πηγές για τυχαίες ενέργειες.
		Εσκεμμένα		
	Εσωτερική		πλημμύρα λόγω διαρροής σωλήνα, φωτιά	Πλημμύρα λόγω διαρροής σωλήνα ή φωτιά δεν έχει συμβεί τα τελευταία 15 έτη λειτουργίας.
Μη Ανθρώπινη	Εξωτερική		Διακοπή ρεύματος, αποτυχία σύνδεσης στο διαδίκτυο	Διακοπή ρεύματος η αποτυχία σύνδεσης στο διαδίκτυο συμβαίνει τακτικά, ωστόσο οι λειτουργικές διακοπές δεν ήταν σχετικές μέχρι σήμερα.

Πίνακας 5 Παράδειγμα αναγνώρισης και τεκμηρίωσης πηγών επικινδυνότητας

Συμβάν (πιθανό γεγονός προστασίας δεδομένων)	**Πηγή Επικινδυνότητας**	**Αποτέλεσμα του συμβάντος**	**Ενδεχόμενη επίπτωση των ενδιαφερόμενων μερών**
μη εξουσιοδοτημένη πρόσβαση σε προσωπικά δεδομένα (εμπιστευτικότητα)	εργαζόμενοι, επιβλέποντες, διαχειριστές ΠΣ	• μη περαιτέρω μετάδοση • χρήση προσωπικών δεδομένων	αποκάλυψη στοιχείων πληρωμής από πιστωτές και συνεπαγόμενες χρηματικές ζημίες σε περίπτωση κακής χρήσης
μη επιθυμητή τροποποίηση των προσωπικών δεδομένων (ακεραιότητα)	εργαζόμενοι, επιβλέποντες, διαχειριστές ΠΣ	• δυσλειτουργία στην επεξεργασία	προβλήματα ρευστότητας του οργανισμού
απώλεια των προσωπικών δεδομένων (διαθεσιμότητα)	εργαζόμενοι, επιβλέποντες, διαχειριστές ΠΣ, μολυσμένος κώδικας, πλημμύρα, φωτιά	• δυσλειτουργία στην επεξεργασία • Διαταραχή στην επεξεργασία	προβλήματα ρευστότητας του οργανισμού

Πίνακας 6 Παράδειγμα τεκμηρίωσης και αποτίμησης συμβάντων παραβίασης προσωπικών δεδομένων

Στη συνέχεια οι πιθανές επιπτώσεις και οι αντίστοιχες πηγές επικινδυνότητας θα πρέπει να αποδοθούν στα γεγονότα. Ο Πίνακας 6 (Πηγή [45]) παρουσιάζει ένα παράδειγμα τεκμηρίωσης και αποτίμησης των συμβάντων. Οι ενέργειες που μπορούν να συμβούν μετά από μια παραβίαση της ασφάλειας των δεδομένων είναι: μη κατάλληλη χρήση, παρακολούθηση, υπερφόρτωση, χειρισμός, καταστροφή, αλλοίωση και απώλεια.

Ο υπεύθυνος επεξεργασίας θα πρέπει να κατανοήσει τις απειλές που σχετίζονται με το συνολικό περιβάλλον της επεξεργασίας των προσωπικών δεδομένων (εξωτερικό ή εσωτερικό) και να αξιολογήσει την πιθανότητά τους (πιθανότητα εμφάνισης απειλής). Για την απλούστευση αυτής της διαδικασίας, έχουν οριστεί ορισμένα ερωτήματα αξιολόγησης τα οποία σχετίζονται με τέσσερις κύριες διαστάσεις/περιοχές αξιολόγησης:

- Δίκτυο Δεδομένων και τεχνικοί πόροι (υλικό και λογισμικό)
- Διεργασίες/διαδικασίες που σχετίζονται με την επεξεργασία δεδομένων
- Διάφορα μέρη και άτομα που εμπλέκονται στη διαδικασία επεξεργασίας
- Επιχειρηματικός τομέας και κλίμακα επεξεργασίας

Μια εκτενής λίστα με ερωτήματα κάθε περιοχής αξιολόγησης δίνεται στο [46].

Εκτίμηση της σοβαρότητα της επίπτωσης

Οι επιπτώσεις κατηγοριοποιούνται ως προς τη σοβαρότητα τους σε τέσσερα επίπεδα επικινδυνότητας:

1. Αμελητέα (Negligible)
2. Περιορισμένη (Limited)
3. Σημαντική (Significant)
4. Μέγιστη (Maximum)

Η αιτιολογική σκέψη 75 του ΓΚΠΔ [15] αναφέρει ότι: «Οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων, ποικίλης πιθανότητας και σοβαρότητας, είναι δυνατόν να προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία θα μπορούσε να οδηγήσει σε σωματική, υλική ή μη υλική βλάβη,…»

Για κάθε επίπεδο επικινδυνότητας θα πρέπει να οριστούν κριτήρια και παραδείγματα για κάθε τύπο επικινδυνότητας και να οριστεί ένα σύστημα κατηγοριοποίησης ώστε να προκύπτει πάντα το ίδιο αποτέλεσμα κάθε φορά που θα πραγματοποιηθεί εκ νέου η εκτίμηση της επικινδυνότητας. Η επιλογή των τεσσάρων επιπέδων για την εκτίμηση των επιπτώσεων και της πιθανότητας μπορεί να είναι κοινή, αλλά μπορεί να επιλεγεί διαφορετικά ανάλογα με το επιχειρηματικό αντικείμενο μιας εταιρείας, την πολυπλοκότητα των διαδικασιών ή των συστημάτων της και πολλούς άλλους παράγοντες.

Εκτίμηση της πιθανότητας

Για την εκτίμηση της πιθανότητας θα πρέπει να ληφθούν υπόψη διάφορες πτυχές, οι δεδομένες συνθήκες, η προηγούμενη εμπειρία και στατιστικές μετρήσεις. Τα επίπεδα μπορεί να είναι κοινά με αυτά της σοβαρότητας της επίπτωσης.

1. Αμελητέα (Negligible): Δεν φαίνεται δυνατό για τις επιλεγμένες πηγές κινδύνου να προκαλέσουν απειλή εκμεταλλευόμενοι τα υποστηρικτικών αγαθά του οργανισμού (π.χ. κλοπή εγγράφου που είναι αποθηκευμένο σε γραφείο που προστατεύεται από συσκευή ανάγνωσης κάρτας εισόδου και κωδικό πρόσβασης).
2. Περιορισμένη (Limited): Φαίνεται δύσκολο για τις επιλεγμένες πηγές κινδύνου να προκαλέσουν απειλή εκμεταλλευόμενοι τα υποστηρικτικά αγαθά του οργανισμού (π.χ. κλοπή εγγράφου που είναι αποθηκευμένο σε γραφείο που προστατεύεται από συσκευή ανάγνωσης κάρτας εισόδου).
3. Σημαντική (Significant): Φαίνεται πιθανό για τις επιλεγμένες πηγές κινδύνου να προκαλέσουν απειλή εκμεταλλευόμενοι τα υποστηρικτικά αγαθά του οργανισμού (π.χ. κλοπή εγγράφου που είναι αποθηκευμένο σε γραφείο στο οποίο δεν είναι δυνατή η πρόσβαση χωρίς να γίνει πρώτα έλεγχος στη ρεσεψιόν).
4. Μέγιστη (Maximum): Φαίνεται εξαιρετικά εύκολο για τις επιλεγμένες πηγές κινδύνου να προκαλέσουν απειλή εκμεταλλευόμενοι τα υποστηρικτικά αγαθά του οργανισμού (π.χ. κλοπή εγγράφου που είναι αποθηκευμένο σε δημόσιο χώρο).

6.2.7. Εκτίμηση επικινδυνότητας

Για τη διαχείριση της επικινδυνότητας αρχικά αναπτύσσονται διάφορα σενάρια πιθανών απειλών που μπορεί να οδηγήσουν στην εμφάνιση κινδύνου που σχετίζεται με την ασφάλεια των πληροφοριών και των μέσων που χρησιμοποιούνται για την επεξεργασία αυτών. Για τα σενάρια αυτά λαμβάνονται υπόψη οι υφιστάμενοι υποστηρικτικοί πόροι, πιθανές ευπάθειες αυτών, τυχόν επαπειλούμενοι κίνδυνοι που μπορούν να επέλθουν ως αποτέλεσμα των ευπαθειών, τα υφιστάμενα μέτρα ελέγχου-αντιμετώπισης του κινδύνου, η σοβαρότητα της επίπτωσης και το μέγεθος του αντικτύπου καθώς και η πιθανότητα εμφάνισης του κινδύνου.

Για την αποτίμηση της σοβαρότητας της επίπτωσης του κινδύνου εξετάζονται οι επιπτώσεις αυτού στα προσωπικά δεδομένα και στην ιδιωτικότητα των προσωπικών δεδομένων. Στον πίνακα που ακολουθεί (Πίνακας 7) αποτυπώνονται τα επίπεδα επίπτωσης στα προσωπικά δεδομένα.

Επίπεδο	Τιμή	Περιγραφή
Μέγιστη	**4**	Το επίφοβο συμβάν επηρεάζει προσωπικά δεδομένα σε μεγάλη – πολύ μεγάλη κλίμακα.
Σημαντική	**3**	Το συμβάν επηρεάζει προσωπικά δεδομένα σε μεσαία – μεσαία προς μεγάλη κλίμακα.
Περιορισμένη	**2**	Το συμβάν επηρεάζει προσωπικά δεδομένα σε περιορισμένη – μικρή κλίμακα.
Αμελητέα	**1**	Το συμβάν δεν επηρεάζει/επηρεάζει προσωπικά δεδομένα σε πολύ μικρή κλίμακα.

Πίνακας 7 Επίπεδα επίπτωσης σε προσωπικά δεδομένα

Ο Πίνακας 8 παρουσιάζει τα επίπεδα επίπτωσης στην ιδιωτικότητα των προσωπικών δεδομένων των υποκειμένων.

Επίπεδο	Τιμή	Περιγραφή
Μέγιστη	**4**	Τα υποκείμενα αντιμετωπίζουν σημαντικές ή μη αναστρέψιμες επιπτώσεις τις οποίες δεν μπορούν να ξεπεράσουν (ανικανότητα για εργασία, μακροχρόνιες ψυχολογικές ή σωματικές ασθένειες, θάνατος κ.α.)
Σημαντική	**3**	Τα υποκείμενα αντιμετωπίζουν σημαντικές επιπτώσεις οι οποίες μπορούν να ξεπεραστούν μέσα από σοβαρές δυσκολίες (κατάχρηση κεφαλαίων, εγγραφή από χρηματοπιστωτικά ιδρύματα σε μαύρη λίστα, υλικές

		ζημιές, απώλεια εργασίας, κλήτευση, επιδείνωση της υγείας κ.α.)
Περιορισμένη	**2**	Τα υποκείμενα αντιμετωπίζουν σημαντικές επιπτώσεις οι οποίες θα ξεπεράσουν με κάποιες δυσκολίες (επιπλέον κόστος, άρνηση πρόσβασης σε επιχειρηματικές υπηρεσίες, φόβος, έλλειψη κατανόησης, άγχος, μικρές σωματικές παθήσεις κ.α.).
Αμελητέα	**1**	Τα φυσικά πρόσωπα δεν επηρεάζονται ή αντιμετωπίζουν επιπτώσεις οι οποίες μπορούν εύκολα να ξεπεραστούν (χρόνος για την εκ νέου εισαγωγή δεδομένων, ενοχλήσεις, εκνευρισμοί κ.α.).

Πίνακας 8 Επίπεδα επίπτωσης στην ιδιωτικότητα προσωπικών δεδομένων

Η αξιολόγηση του αντίκτυπου είναι μια ποιοτική διαδικασία και αρκετοί παράγοντες πρέπει να ληφθούν υπόψη από τον υπεύθυνο επεξεργασίας, όπως τα είδη των προσωπικών δεδομένων, η κρισιμότητα της διαδικασίας επεξεργασίας, ο όγκος των προσωπικών δεδομένων, τα ειδικά χαρακτηριστικά του υπευθύνου επεξεργασίας δεδομένων, καθώς και ως ειδικές κατηγορίες υποκειμένων δεδομένων. Προκειμένου να υποστηριχθεί ο υπεύθυνος επεξεργασίας σε αυτή τη διαδικασία, ο Πίνακας 9 μπορεί να χρησιμοποιηθεί για να αξιολογήσει χωριστά τον αντίκτυπο από την απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας. Μετά από αυτήν την αξιολόγηση, θα ληφθούν τρία διαφορετικά επίπεδα επιπτώσεων (για απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας). Το υψηλότερο από αυτά τα επίπεδα θεωρείται ως το τελικό αποτέλεσμα της αξιολόγησης του αντίκτυπου, που σχετίζεται με τη συνολική επεξεργασία προσωπικών δεδομένων.

Α/Α	**Ερώτηση**	**Εκτίμηση**
Ε.1	Εκτιμήστε τον αντίκτυπο που θα μπορούσε να έχει στο υποκείμενο μια μη εξουσιοδοτημένη αποκάλυψη προσωπικών δεδομένων (απώλεια εμπιστευτικότητας), στο πλαίσιο όπου λαμβάνει χώρα η επιχειρηματική σας δραστηριότητα	Μέγιστη ☐ Σημαντική ☐ Περιορισμένη ☐ Αμελητέα ☐
Ε.2	Εκτιμήστε τον αντίκτυπο που θα μπορούσε να έχει στο υποκείμενο μια μη εξουσιοδοτημένη τροποποίηση προσωπικών δεδομένων (απώλεια ακεραιότητας), στο πλαίσιο όπου λαμβάνει χώρα η επιχειρηματική σας δραστηριότητα	Μέγιστη ☐ Σημαντική ☐ Περιορισμένη ☐ Αμελητέα ☐

Ε.3	Εκτιμήστε τον αντίκτυπο που θα μπορούσε να έχει στο υποκείμενο μια μη εξουσιοδοτημένη καταστροφή η απώλεια προσωπικών δεδομένων (απώλεια διαθεσιμότητας), στο πλαίσιο όπου λαμβάνει χώρα η επιχειρηματική σας δραστηριότητα	Μέγιστη ☐ Σημαντική ☐ Περιορισμένη ☐ Αμελητέα ☐

Πίνακας 9 Ερωτηματολόγιο εκτίμησης αντικτύπου

Ακολουθεί η εκτίμηση της πιθανότητας εμφάνισης του κινδύνου, που αφορά είτε την δυσλειτουργία (ευπάθεια) των υποστηρικτικών αγαθών (πόρων) είτε την ικανότητα της πηγής του κινδύνου να εκμεταλλευτεί αποτελεσματικά την ευπάθεια των υποστηρικτικών αγαθών. Ο Πίνακας 10 παρουσιάζει τα επίπεδα ευπάθειας των υποστηρικτικών αγαθών.

Επίπεδο	**Τιμή**	**Περιγραφή**
Μέγιστη	**4**	Η πιθανότητα ευπάθειας υποστηρικτικών αγαθών υπό συνθήκες «απειλής» είναι μεγάλη έως πολύ μεγάλη.
Σημαντική	**3**	Η πιθανότητα ευπάθειας υποστηρικτικών αγαθών υπό συνθήκες «απειλής» είναι μεσαία προς μεγάλη.
Περιορισμένη	**2**	Η πιθανότητα ευπάθειας υποστηρικτικών αγαθών υπό συνθήκες «απειλής» είναι μικρή – περιορισμένη.
Αμελητέα	**1**	Η πιθανότητα ευπάθειας υποστηρικτικών αγαθών υπό συνθήκες «απειλής» είναι μηδενική – πολύ μικρή.

Πίνακας 10 Επίπεδα πιθανότητας ευπάθειας υποστηρικτικών αγαθών

Επίπεδο	**Τιμή**	**Περιγραφή**
Μέγιστη	**4**	Τα φυσικά πρόσωπα αντιμετωπίζουν σημαντικές ή μη αναστρέψιμες επιπτώσεις τις οποίες δεν μπορούν να ξεπεράσουν.
Σημαντική	**3**	Σημαντικές επιπτώσεις στα φυσικά πρόσωπα οι οποίες μπορούν να ξεπεραστούν μέσα από σοβαρές δυσκολίες.
Περιορισμένη	**2**	Τα φυσικά πρόσωπα αντιμετωπίζουν σημαντικά προβλήματα τα οποία θα ξεπεράσουν με κάποιες δυσκολίες.
Αμελητέα	**1**	Τα φυσικά πρόσωπα δεν επηρεάζονται ή ταλαιπωρούνται ελαφρώς.

Πίνακας 11 Επίπεδα ικανότητας πηγών κινδύνου να εκμεταλλευτούν την δυσλειτουργία των υποστηρικτικών αγαθών

Ο Πίνακας 11 παρουσιάζει τα επίπεδα πιθανότητας οι κίνδυνοι να εμφανιστούν ως αποτέλεσμα της ικανότητας των πηγών κινδύνου να εκμεταλλευτούν αποτελεσματικά τη δυσλειτουργία των υποστηρικτικών αγαθών.

Η εκτίμηση της επίπτωσης και της πιθανότητας της επικινδυνότητας μπορεί να δώσει τα επίπεδα επικινδυνότητας «Υψηλού Κινδύνου» (high risk), «Κινδύνου» (risk), «Μειωμένου Κινδύνου» (reduced risk) και «Χαμηλού Κινδύνου» (low risk), όπως προτείνονται στον παρακάτω πίνακα (Πηγή: [45]):

Επίπεδα Επικινδυνότητας	**Παράγοντας**
Υψηλού Κινδύνου	16
Κινδύνου	12-15
Μειωμένου Κινδύνου	6-11
Χαμηλού Κινδύνου	1-5

Πίνακας 12 Τέσσερα επίπεδα επικινδυνότητας

Παρόλο που ο ΓΚΠΔ προτείνει δύο επίπεδα («Υψηλού Κινδύνου» και «Χαμηλού Κινδύνου»), περισσότερα επίπεδα προσφέρουν περισσότερη γνώση και πληροφορία καθώς η κατάταξη των προσωπικών δεδομένων σε επίπεδα επικινδυνότητας επηρεάζει την μελλοντική χρήση των δεδομένων αυτών. Για παράδειγμα, αν τα προσωπικά δεδομένα ανήκουν στο επίπεδο υψηλού κινδύνου, είναι σημαντικό να ελεγχθεί αν έχει πραγματοποιηθεί μελέτη εκτίμησης αντικτύπου (DPIA). Επίσης, αν τα προσωπικά δεδομένα που παραβιάστηκαν ανήκουν στο επίπεδο χαμηλού κινδύνου, θα πρέπει να ενημερωθεί η αρμόδια εποπτική αρχή ενώ αν ανήκουν στο επίπεδο υψηλού κινδύνου, θα πρέπει να ενημερωθεί και το υποκείμενο των δεδομένων.

Επίπτωση στα δεδομένα του υποκειμένου					
	4 Μέγιστη	4	8	12 απώλεια εμπιστευτικότητας	16
	3 Σημαντική	3	6	9	12
	2 Περιορισμένη	2	4 απώλεια διαθεσιμότητας	6 απώλεια ακεραιότητας	8
	1 Αμελητέα	1	2	3	4

	1 Αμελητέα	2 Περιορισμένη	3 Σημαντική	4 Μέγιστη
	Πιθανότητα			

Πίνακας 13 Πίνακας επικινδυνότητας 4 επιπέδων

Η αναπαράσταση της επικινδυνότητας ως το γινόμενο της πιθανότητας (likelihood) επί την σοβαρότητα της επίπτωσης (severity) μπορεί να πραγματοποιηθεί μέσω του πίνακα επικινδυνότητας τεσσάρων επιπέδων (χάρτης επικινδυνότητας) που δίνεται παρακάτω (Πηγή [45]). Στον πίνακα φαίνονται και σημεία εκκίνησης της επικινδυνότητας σε ότι αφορά την απώλεια της διαθεσιμότητας, της εμπιστευτικότητας και της ακεραιότητας των προσωπικών δεδομένων.

Ο χρωματικός κώδικας απεικονίζει τον χαρακτηρισμό της επικινδυνότητας, ως εξής:

Χρώμα	Χαρακτηρισμός
Πράσινο	Αποδεκτός
Κίτρινο	Αποδεκτός, μόνον εφόσον διαπιστωθεί ότι δεν μπορεί να μειωθεί η πιθανότητα εμφάνισης και η σοβαρότητα της επίπτωσης έχει χαρακτηριστεί «περιορισμένη» (τιμή 2). Απαιτούνται ενέργειες για τη μείωση της πιθανότητας εμφάνισης της συγκεκριμένης κατηγορίας κινδύνων.
Πορτοκαλί	Αποδεκτός, μόνον εφόσον διαπιστωθεί ότι δεν μπορεί να μειωθεί η σοβαρότητα της επίπτωσης και η πιθανότητα εμφάνισης έχει χαρακτηριστεί «περιορισμένη» (τιμή 2). Απαιτούνται ενέργειες για τη μείωση τόσο της σοβαρότητας της επίπτωσης όσο και της πιθανότητας εμφάνισης της συγκεκριμένης κατηγορίας κινδύνων.
Κόκκινο	Μη αποδεκτοί κίνδυνοι. Απαιτείται αποφυγή της συγκεκριμένης κατηγορίας κινδύνων ή περιορισμός αυτών μέσω κατάλληλων μέτρων που θα οδηγήσουν στη μείωση τόσο της σοβαρότητας της επίπτωσης όσο και της πιθανότητας εμφάνισής τους.

Πίνακας 14 Χρωματικός κώδικας χάρτη επικινδυνότητας 4 επιπέδων

Το επίπεδο της πιθανότητας εμφάνισης κινδύνου, για κάθε μία από τις περιοχές αξιολόγησης μπορεί να οριστεί ως εξής [46]:

- Υψηλή: η απειλή είναι πιθανό να πραγματοποιηθεί
- Μέτρια: υπάρχει εύλογη πιθανότητα η απειλή να πραγματοποιηθεί
- Χαμηλή: η απειλή είναι απίθανο να πραγματοποιηθεί

Ο Πίνακας 15 χρησιμοποιείται για την εκτίμηση του επιπέδου εμφάνισης απειλών για κάθε περιοχή αξιολόγησης. Στη συνέχεια το άθροισμα αυτών δίνει το συνολικό επίπεδο επικινδυνότητας (Πίνακας 16).

Περιοχή αξιολόγησης	**Εκτίμηση Πιθανότητας**	
	Επίπεδο	**Τιμή**
Δίκτυο και τεχνικοί πόροι (υλικό και λογισμικό)	Υψηλή ☐	3
	Μέτρια ☐	2
	Χαμηλή ☐	1
Διεργασίες/διαδικασίες που σχετίζονται με την επεξεργασία δεδομένων	Υψηλή ☐	3
	Μέτρια ☐	2
	Χαμηλή ☐	1
Διάφορα μέρη και άτομα που εμπλέκονται στη διαδικασία επεξεργασίας	Υψηλή ☐	3
	Μέτρια ☐	2
	Χαμηλή ☐	1
Επιχειρηματικός τομέας και κλίμακα επεξεργασίας	Υψηλή ☐	3
	Μέτρια ☐	2
	Χαμηλή ☐	1

Πίνακας 15 Εκτίμηση πιθανότητας εμφάνισης απειλών ανά περιοχή αξιολόγησης

Επίπεδο Επικινδυνότητας	**Παράγοντας**
Υψηλό	9-12
Μέτριο	6-8
Χαμηλό	4-5

Πίνακας 16 Εκτίμηση του συνολικού βαθμού επικινδυνότητας

Τέλος, εκτιμάται η συνολική επικινδυνότητα, μέσω του χάρτη επικινδυνότητας τριών επιπέδων (Πίνακας 17).

Επίπτωση στα δεδομένα του υποκειμένου	3 Υψηλή			
	2 Μέτρια			

	1 Χαμηλή			
		1 Χαμηλή	2 Μέτρια	3 Υψηλή
		Πιθανότητα		

Πίνακας 17 Πίνακας επικινδυνότητας 3 επιπέδων

Τα χρώματα πράσινο, κίτρινο και κόκκινο αντιστοιχούν σε Χαμηλή, Μέτρια και Υψηλή επικινδυνότητα. Ο υπεύθυνος επεξεργασίας έχει τη δυνατότητα να τροποποιήσει τα αποδεκτά επίπεδα επικινδυνότητας λαμβάνοντας υπόψη τα ειδικά χαρακτηριστικά της διαδικασίας επεξεργασίας δεδομένων (που έχουν χαθεί κατά τη διαδικασία εκτίμησης) και παρέχοντας επαρκή αιτιολόγηση για αυτήν την προσαρμογή.

6.2.8. Αντιμετώπιση της επικινδυνότητας

Υπάρχουν τέσσερις διαφορετικοί τρόποι αντιμετώπισης της επικινδυνότητας:

- Μείωση επικινδυνότητας με λήψη μέτρων
- Αποφυγή επικινδυνότητας (π.χ. διακοπή της επεξεργασίας ορισμένων κατηγοριών δεδομένων)
- Μεταφορά επικινδυνότητας σε τρίτους
- Αποδοχή επικινδυνότητας

Δεν είναι πάντα δυνατό να χρησιμοποιηθούν όλα αυτά τα μέτρα μείωσης της επικινδυνότητας. Για παράδειγμα, η μεταφορά της επικινδυνότητας σε τρίτους είναι συχνά δύσκολο να εφαρμοστεί στην προστασία δεδομένων. Το ίδιο ισχύει και για την αποδοχή της επικινδυνότητας σε ότι αφορά τη ζημία στο υποκείμενο των δεδομένων

Ο ΓΚΠΔ [15] στο Άρθρο 32, παράγραφος 1, θεωρεί ως μοναδική επιλογή για την αντιμετώπιση της επικινδυνότητας τη λήψη μέτρων, δηλαδή «… εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, …», και προτείνει κατά περίπτωση τα ακόλουθα:

α. την ψευδωνυμοποίηση και την κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα,

β. τη δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,

γ. τη δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος,

δ. τη διαδικασία για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

Στην περίπτωση λήψης μέτρων για τη μείωση της επικινδυνότητας, πρέπει να διατηρείται ένας κατάλογος μέτρων και να τεκμηριώνεται ποιο μέτρο έχει προγραμματιστεί, ποιος είναι υπεύθυνος για την υλοποίηση του και πότε πρόκειται να ολοκληρωθεί η υλοποίηση του μέτρου.

Στα πρότυπα ποιότητας, όπως για παράδειγμα στο ISO/IEC 29151:2017 [47] καθώς και στο ISO/IEC 27001, Παράρτημα Α, [24] υπάρχουν πλήρεις κατάλογοι κοινά αποδεκτών μέτρων που μπορούν να ληφθούν για την μείωση της επικινδυνότητας στην ασφάλεια πληροφοριών. Ο ΓΚΠΔ δεν απαιτεί την εφαρμογή συγκεκριμένων μέτρων, δίνει δε τη δυνατότητα στον υπεύθυνο της επεξεργασίας να χρησιμοποιήσει οποιαδήποτε μέτρα, λαμβάνοντας υπόψιν το Άρθρο 32 του κανονισμού. Επίσης, θα πρέπει να τηρείται ο εγκεκριμένος κώδικας δεοντολογίας ή ο εγκεκριμένος μηχανισμός πιστοποίησης και να ακολουθούνται οι αρχές προστασίας δεδομένων «ήδη από το σχεδιασμό και εξ ορισμού» («by design & by default») όπως αναφέρεται στο Άρθρο 25 του ΓΚΠΔ [15]. Ένας εκτενής κατάλογος μέτρων για κάθε επίπεδο επικινδυνότητας είναι διαθέσιμος και από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) στο [48] , μαζί με μια αντιστοιχία αυτών με τους ελέγχους του προτύπου ISO/IEC 27001:2013 [24]. Τα μέτρα που προτείνονται είναι γενικά και δεν λαμβάνονται υπόψη πρόσθετες απαιτήσεις ασφάλειας ανάλογα με τον τομέα δραστηριοποίησης του οργανισμού ή κανονιστικές

υποχρεώσεις. Σε κάθε περίπτωση, ο υπεύθυνος επεξεργασίας μπορεί να εφαρμόσει επιπλέον μέτρα.

Οι εταιρείες/οργανισμοί ενθαρρύνονται να εφαρμόζουν τεχνικά και οργανωτικά μέτρα, στα πρώτα στάδια του σχεδιασμού των εργασιών επεξεργασίας, κατά τρόπο που να διασφαλίζει εξαρχής τις αρχές της ιδιωτικότητας και της προστασίας των δεδομένων («προστασία δεδομένων κατά το σχεδιασμό»). Παράδειγμα προστασίας δεδομένων κατά το σχεδιασμό είναι η ψευδωνυμοποίηση και κρυπτογράφηση των δεδομένων. Επίσης, οι εταιρείες/οργανισμοί θα πρέπει να διασφαλίζουν ότι τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία με την υψηλότερη προστασία απορρήτου (για παράδειγμα, υποβάλλονται σε επεξεργασία μόνο τα απαραίτητα δεδομένα, με σύντομη περίοδο αποθήκευσης και με περιορισμένη προσβασιμότητα) έτσι ώστε εξ ορισμού τα προσωπικά δεδομένα να μην είναι προσβάσιμα σε αόριστο πλήθος ατόμων («προστασία δεδομένων εξ ορισμού»). Παράδειγμα προστασίας δεδομένων εξ ορισμού είναι μια πλατφόρμα κοινωνικής δικτύωσης να περιορίζει εξ ορισμού την προσβασιμότητα του προφίλ των χρηστών της ώστε να μην είναι εξ αρχής προσπελάσιμο από αόριστο αριθμό χρηστών [48].

6.2.9. Παρακολούθηση και επανεξέταση

Ο ΓΚΠΔ υποχρεώνει τον υπεύθυνο επεξεργασίας να καθιερώσει και να πραγματοποιήσει μια διαδικασία για την επανεξέταση και την παρακολούθηση της ασφάλειας της επεξεργασίας. Ως εκ τούτου, πρέπει να αξιολογηθεί η αποτελεσματικότητα των τεχνικών και οργανωτικών μέτρων. Για την εκπλήρωση του καθήκοντος λογοδοσίας του ΓΚΠΣ, συνιστάται λεπτομερής τεκμηρίωση ενός προγράμματος επιθεώρησης. Εάν στην επιθεώρηση διαπιστωθούν αποκλίσεις, θα πρέπει να συστηματοποιηθούν και να τεκμηριωθούν τα κατάλληλα διορθωτικά μέτρα.

6.3. Η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων

Η Εκτίμηση Αντικτύπου σχετικά με την Προστασία των Δεδομένων (ΕΑΠΔ, DPIA) επεκτείνει την εκτίμηση διακινδύνευσης στην ασφάλεια της επεξεργασίας δεδομένων σε ότι αφορά τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων

αλλά και τη συμμόρφωση με την νομοθεσία. Στις νομοθετικές υποχρεώσεις περιλαμβάνονται τα πιθανά αιτήματα του υποκειμένου των δεδομένων προς τον ίδιο τον υπεύθυνο επεξεργασίας ή μέσω ενώσεων. Επιπλέον, το επίπεδο τεκμηρίωσης αυξάνεται και συνίσταται η συμμετοχή του υποκειμένου των δεδομένων.

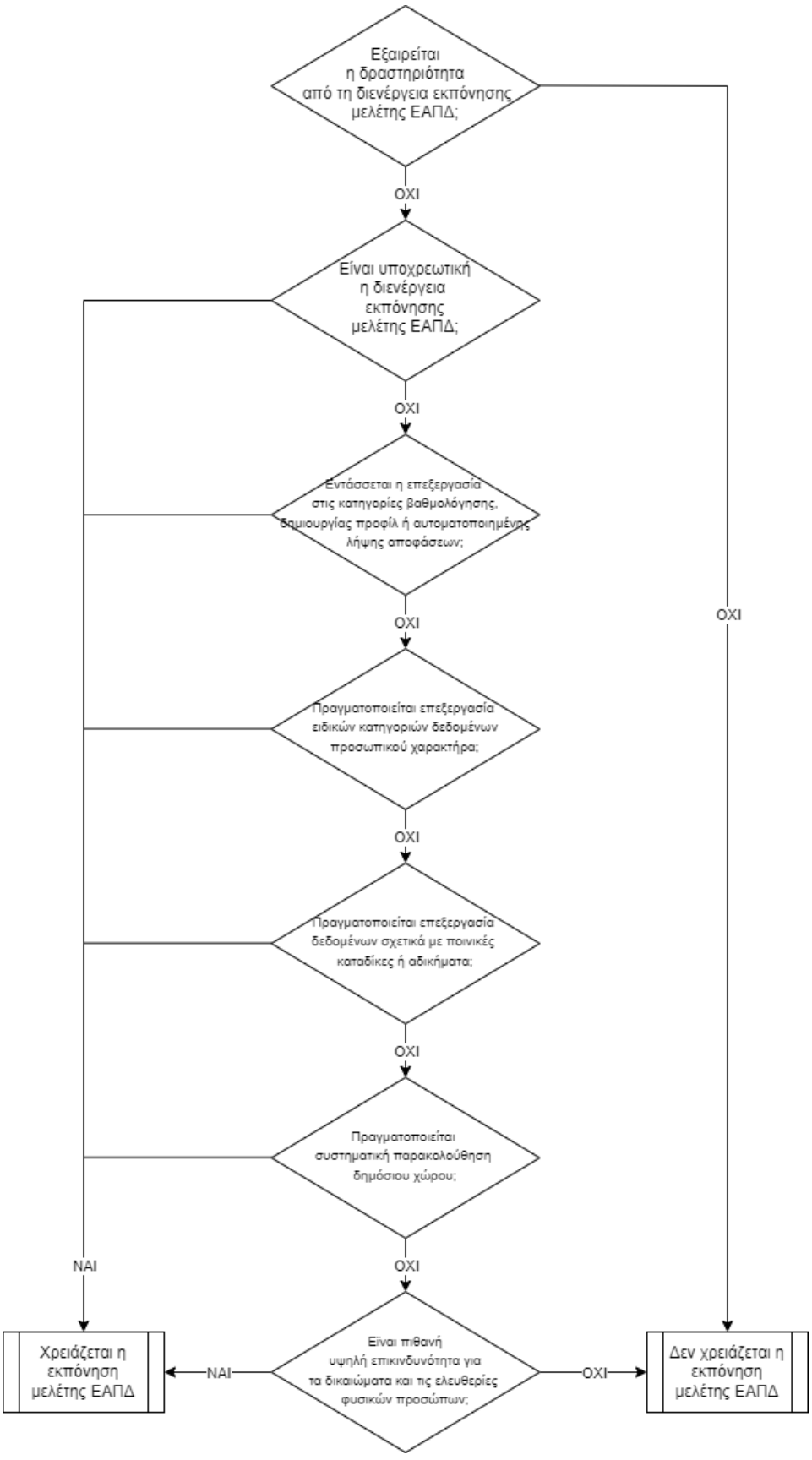
Στο Τμήμα 3 του Γενικού Κανονισμού Προστασίας Δεδομένων [15], δίνονται οι οδηγίες για την Εκτίμηση Αντικτύπου σχετικά με την Προστασία των Δεδομένων (Άρθρο 35) καθώς και διαβούλευση που θα πρέπει να προηγηθεί (Άρθρο 36). Η *ομάδα προστασίας των προσώπων έναντι στην επεξεργασία δεδομένων προσωπικού χαρακτήρα*, όπως συστάθηκε σύμφωνα με την οδηγία 95/46/ΕΚ [17], εξέδωσε το 2017 για τους σκοπούς το ΓΚΠΔ κατευθυντήριες γραμμές για την ΕΑΠΔ και για τον καθορισμό του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» [18]. Στο άρθρο της, η ομάδα επεξηγεί τον κανονισμό, αναφέρει πότε είναι και πότε δεν είναι υποχρεωτική η διενέργεια ΕΑΠΔ, πότε πρέπει να διενεργείται, από ποιόν και με ποια μεθοδολογία, πότε ο κίνδυνος χαρακτηρίζεται υψηλός κ.α. Στις παραγράφους που ακολουθούν θα αναφέρουμε συνοπτικά κάποιες πληροφορίες καθώς και ένα πρότυπο εγγράφου που μπορεί να χρησιμοποιηθεί για τη διενέργεια της ΕΑΠΔ.

6.3.1. Απαίτηση για εκπόνηση μελέτης Εκτίμησης Αντικτύπου Προστασίας Δεδομένων

Η Αρχή Προστασίας Δεδομένων μπορεί να καταρτίζει κατάλογο των ειδών δραστηριοτήτων επεξεργασίας για τις οποίες, σε γενικές γραμμές, δεν απαιτείται μελέτη ΕΑΠΔ καθώς και των ειδών δραστηριοτήτων επεξεργασίας που υπόκεινται πάντα στην απαίτηση για μελέτη ΕΑΠΔ. Ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να διενεργήσει μελέτη ΕΑΠΔ στις περιπτώσεις όπου η επεξεργασία των δεδομένων χαρακτηρίζεται ως υψηλής επικινδυνότητας για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων.

Ο ΓΚΠΔ απαιτεί από τον υπεύθυνο επεξεργασίας να εκτιμήσει την επικινδυνότητα με βάση αντικειμενικά κριτήρια. Επίσης η ευρωπαϊκή νομοθεσία θεωρεί ότι ιδίως οι νέες τεχνολογίες αποτελούν έναυσμα για την υποχρέωση εκπόνησης μελέτης ΕΑΠΔ. Όμως ανεξάρτητα από την υποχρέωση, η μελέτη ΕΑΠΔ μπορεί πάντα να γίνει εθελοντικά

και επιπρόσθετα στην εκτίμηση επικινδυνότητας, σύμφωνα με το άρθρο 32 του ΓΚΠΔ. Πολλές δραστηριότητες επεξεργασίας δεδομένων με παρόμοια υψηλή επικινδυνότητα, μπορούν να εξεταστούν σε μία κοινή μελέτη ΕΑΠΔ. Στην Εικόνα 17 δίνουμε ένα διάγραμμα αποφάσεων, όπως προτείνεται στο [45], μέσω του οποίου ο υπεύθυνος επεξεργασίας μπορεί να αποφασίσει αν είναι απαραίτητη ή όχι η εκπόνησης μελέτη ΕΑΠΔ. Ο Υπεύθυνος Προστασίας Δεδομένων του οργανισμού, επικουρεί τον υπεύθυνο επεξεργασίας συμβουλευτικά.



Εικόνα 17 Διάγραμμα αποφάσεων για την εκπόνηση μελέτης ΕΑΠΔ

6.3.2. Συστηματική περιγραφή των δραστηριοτήτων επεξεργασίας δεδομένων

Πριν την εκπόνηση της μελέτης, είναι σημαντικό να έχει καταγραφεί ο σκοπός της δραστηριότητας ή των δραστηριοτήτων επεξεργασίας δεδομένων για την οποία/τις οποίες πρόκειται να εκπονηθεί η μελέτη. Αναφορικά με τον σκοπό, ο υπεύθυνος επεξεργασίας θα πρέπει να αξιολογήσει την αναγκαιότητα και την επάρκεια αυτής της δραστηριότητας. Ανάλογα με το βαθμό λεπτομέρειας ακρίβειας της περιγραφής, θα πρέπει να αιτιολογηθεί το έννομο συμφέρον του υπευθύνου επεξεργασίας.

Για να διεξαχθεί μια ΕΑΠΔ θα πρέπει να έχει προηγηθεί λεπτομερής περιγραφή της δραστηριότητας (είτε με μορφή πίνακα είτε με διάγραμμα ροής). Σε κάθε φάση της επεξεργασίας, θα πρέπει να συγκεντρώνονται και να τεκμηριώνονται τα εξής:

- Αναλυτική περιγραφή των σταδίων επεξεργασίας.
- Πληροφοριακά συστήματα που χρησιμοποιούνται.
- Πρόσθετα υποστηρικτικά περιουσιακά στοιχεία που χρησιμοποιούνται.

Στις κατευθυντήριες γραμμές για την ΕΑΠΔ και για τον καθορισμό του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» [18], δίνονται τα κριτήρια προκειμένου ο υπεύθυνος επεξεργασίας να αποφανθεί αν η μελέτη ΕΑΠΔ είναι η όχι απαραίτητη.

1. Αξιολόγηση ή βαθμολόγηση, συμπεριλαμβανομένης της κατάρτισης προφίλ και προβλέψεων.
2. Λήψη αυτοματοποιημένων αποφάσεων που παράγουν έννομα αποτελέσματα ή σημαντικά αποτελέσματα κατά ανάλογο τρόπο.
3. Συστηματική παρακολούθηση.
4. Ευαίσθητα δεδομένα ή δεδομένα εξαιρετικά προσωπικού χαρακτήρα.
5. Δεδομένα μεγάλης κλίμακας επεξεργασίας.
6. Η αντιστοίχιση ή ο συνδυασμός συνόλων δεδομένων.
7. Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων.
8. Καινοτόμος χρήση ή εφαρμογή νέων τεχνολογικών ή οργανωτικών λύσεων.
9. Διασυνοριακή μεταφορά δεδομένων εκτός Ευρωπαϊκής Ένωσης.
10. Όταν η επεξεργασία αυτή καθαυτή «εμποδίζει τα υποκείμενα των δεδομένων να ασκήσουν κάποιο δικαίωμα ή να χρησιμοποιήσουν μια υπηρεσία ή μια σύμβαση».

Να αναφέρουμε ότι σύμφωνα με τα άρθρα 9 και 10 του ΓΚΠΔ, ευαίσθητα δεδομένα προσωπικού χαρακτήρα είναι αυτά που αποκαλύπτουν φυλετική ή εθνοτική

καταγωγή, πολιτικά φρονήματα, θρησκευτικές πεποιθήσεις, γενετικά ή βιομετρικά ή ιατρικά δεδομένα, δεδομένα που αφορούν ποινικές καταδίκες ή αδικήματα, δια τα οποία απαγορεύεται η επεξεργασία τους ή επιτρέπεται υπό συνθήκες [14].

Σύμφωνα με την ομάδα εργασίας του [17], όσα περισσότερα είναι τα κριτήρια που ικανοποιούνται, τόσο μεγαλύτερο είναι το ενδεχόμενο υψηλής επικινδυνότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

6.3.3. Εκτίμηση επικινδυνότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων

Στο Άρθρο 5 του ΓΚΠΔ [15] δίνεται μια σειρά από αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα:

- νομιμότητα (lawfulness)
- αντικειμενικότητα (fairness)
- διαφάνεια (transparency)
- περιορισμός του σκοπού (purpose limitation)
- ελαχιστοποίηση των δεδομένων (data minimization)
- ακρίβεια (accuracy)
- περιορισμός της περιόδου αποθήκευσης (storage limitation)
- ακεραιότητα και εμπιστευτικότητα (integrity and confidentiality)
- διαθεσιμότητα (availability)
- συμμετοχή και πρόσβαση υποκειμένου (personal participation and access)
- λογοδοσία (accountability)

Ο υπεύθυνος της επεξεργασίας πρέπει να περιγράψει την επικινδυνότητα που μπορεί να προκύψει σε περίπτωση παραβίασης των αρχών αυτών ναι να αξιοποιήσει τη διαδικασία ασφάλειας επεξεργασίας που περιγράψαμε στην προηγουμένη ενότητα για την εκπόνηση μελέτης ΕΑΠΔ. Στην εκπόνηση της μελέτης ΕΑΠΔ προβλέπεται ρητά και η συμμετοχή των ενδιαφερομένων μερών «όπου χρειάζεται». Η συμμετοχή των ενδιαφερόμενων μερών ενισχύει τη διαφάνεια άρα και την αποδοχή της ΕΑΠΔ προς όφελος του υπευθύνου επεξεργασίας

6.3.4. Μέτρα αντιμετώπισης επικινδυνότητας

Ο υπεύθυνος επεξεργασίας πρέπει να περιγράψει ποια μέτρα θα λάβει προκειμένου να αντιμετωπιστούν παραβιάσεις των αρχών προστασίας δεδομένων. Και πάλι πρέπει να γίνει διάκριση μεταξύ της συμμόρφωσης και της ασφάλειας των πληροφοριών. Στο Άρθρο 35, παράγραφος 7(δ), ο ΓΚΠΔ [15] απαιτεί τον καθορισμό μέτρων (συμπεριλαμβανομένων εγγυήσεων, μέτρων ασφαλείας και διαδικασιών) που διασφαλίζουν την προστασία των προσωπικών δεδομένων και αποδεικνύουν πως πληρούνται οι απαιτήσεις αυτού. Στον καθορισμό των μέτρων θα πρέπει να λαμβάνονται υπόψη τα δικαιώματα των υποκειμένων των δεδομένων και των άλλων θιγόμενων υποκειμένων. Για λόγους λογοδοσίας, τα μέτρα που θα λάβει ο οργανισμούς θα πρέπει να καταγράφονται σε έναν κατάλογο (σχέδιο διαχείρισης επικινδυνότητας) όπου για κάθε μέτρο θα καθορίζεται η προθεσμία και ο υπεύθυνος υλοποίησης. Στο Παράρτημα του [45] δίνεται ο κατάλογος μέτρων για την προστασία δεδομένων όπως προτείνονται από την CNIL. (Ο κατάλογος αυτός συντάχθηκε πριν την δημοσίευση του ΓΚΠΔ οπότε θα πρέπει στις απαιτήσεις του CNIL θα πρέπει να προστεθούν και νομικές απαιτήσεις).

6.3.5. Έκθεση της μελέτης για την ΕΑΠΔ

Σύμφωνα με το άρθρο 35, παράγραφος 7, του ΓΚΠΔ [15], η έκθεση της μελέτης για την ΕΑΠΔ θα πρέπει να περιλαμβάνει τουλάχιστον τα ακόλουθα στοιχεία:

α. συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας,

β. εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,

γ. εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στην παράγραφο 1 και

δ. τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα κανονισμό, λαμβάνοντας

υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων.

Όταν η εν δυνάμει ΕΑΠΔ υποδεικνύει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο ελλείψει μέτρων μετριασμού του κινδύνου από τον υπεύθυνο επεξεργασίας, τότε σύμφωνα με το άρθρο 36, παράγραφος 3 του ΓΠΚΔ [15], ο υπεύθυνος επεξεργασίας ζητά διαβούλευση με την Αρχή Προστασίας Δεδομένων (εποπτική αρχή), παρέχοντας της τα παρακάτω στοιχεία:

α. κατά περίπτωση, τις αντίστοιχες αρμοδιότητες του υπευθύνου επεξεργασίας, των από κοινού υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία που συμμετέχουν στις εργασίες, ιδίως όσον αφορά επεξεργασία εντός ομίλου επιχειρήσεων,
β. τους σκοπούς και τα μέσα της σχεδιαζόμενης επεξεργασίας,
γ. τα μέτρα και τις εγγυήσεις για την προστασία των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων σύμφωνα με τον παρόντα κανονισμό,
δ. κατά περίπτωση, τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων,
ε. την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων που προβλέπεται στο άρθρο 35, και
στ. κάθε άλλη πληροφορία που ζητεί η εποπτική αρχή.

Στην Εικόνα 18 δίνεται μια πιθανή δομή για μια έκθεση ΕΑΠΔ που πληροί τις απαιτήσεις του άρθρου 35 παράγραφος 7 του ΓΚΠΔ [15].

Εάν εξακολουθεί να υπάρχει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων μετά τη λήψη μέτρων για τη μείωση των κινδύνων («ελλείψει μέτρων που λαμβάνονται από τον υπεύθυνο επεξεργασίας») και «και ο υπεύθυνος επεξεργασίας είναι της γνώμης ότι ο κίνδυνος δεν μπορεί να μετριάζεται με εύλογα μέσα όσον αφορά τις διαθέσιμες τεχνολογίες και το κόστος εφαρμογής»), ο υπεύθυνος επεξεργασίας πρέπει να συμβουλευτεί την εποπτική αρχή πριν ξεκινήσει η επεξεργασία των δεδομένων. Ο υπεύθυνος επεξεργασίας παρέχει στην εποπτική αρχή τις απαραίτητες πληροφορίες. Κατά τη διαδικασία διαβούλευσης, η

εποπτική αρχή ελέγχει εάν η εν λόγω επεξεργασία συμμορφώνεται με τον ΓΚΠΔ. Εάν όχι, ο υπεύθυνος επεξεργασίας ενημερώνεται εντός 14 εβδομάδων (μέγιστο 8 εβδομάδες και πιθανή παράταση 6 εβδομάδων). Σε περίπτωση συμμόρφωσης, δεν απαιτείται ειδοποίηση από την εποπτική αρχή.

Εκτίμηση Αντικτύπου Προστασίας Δεδομένων

1. Εισαγωγή

2 Πεδίο εφαρμογής της ΕΑΠΔ

2.1 Συστηματική περιγραφή των σκοπών των δραστηριοτήτων επεξεργασίας δεδομένων

2.2 Εκτίμηση της αναγκαιότητας και της επάρκειας των δραστηριοτήτων επεξεργασίας σε σχέση με τον σκοπό

2.3 Σκοποί και μέσα της προγραμματισμένης επεξεργασίας

2.4 Εμπλεκόμενα μέρη:

2.4.1 Υπεύθυνος Επεξεργασίας

2.4.2 Κοινοί Υπεύθυνοι Επεξεργασίας

2.4.3 Εκτελών την Επεξεργασία

2.4.4 Υπεύθυνο Προστασίας Δεδομένων

3 Απαιτήσεις προστασίας δεδομένων

4 Προοπτική Επικινδυνότητας για την προστασίας δεδομένων

4.1 Αναγνώριση Επικινδυνότητας

4.2 Ανάλυση Επικινδυνότητας

4.3 Εκτίμηση Επικινδυνότητας

5 Προγραμματισμένα μέτρα για την διασφάλιση της προστασίας προσωπικών δεδομένων

6 Αποτέλεσμα ΕΑΠΔ και πιθανή υποχρέωση διαβούλευσης με την Αρχή Προστασίας Δεδομένων

Εικόνα 18 Παράδειγμα έκθεσης ΕΑΠΔ

7. Μελέτη περίπτωσης: διαχείριση δεδομένων ενός Πανεπιστημιακού Ιδρύματος

Στη κεφάλαιο αυτό θα περιγράψουμε, ως μελέτη περίπτωσης, τη διαδικασία διαχείρισης εκπαιδευτικών δεδομένων ενός πανεπιστημιακού ιδρύματος. Τα δεδομένα αυτά προέρχονται από ένα περιβάλλον εικονικής μάθησης (Virtual Learning Environment, VLE) ή από ένα σύστημα διαχείρισης μάθησης (Learning Management System, LMS) που χρησιμοποιείται από το εκπαιδευτικό ίδρυμα για την παροχή σύγχρονης και ασύγχρονης εξ αποστάσεως εκπαίδευσης. Ακολουθεί η μελέτη Εκτίμησης Αντικτύπου σχετικά με την Προστασία Δεδομένων (ΕΑΠΔ), όπως προβλέπεται από τον Γενικό Κανονισμό Προστασίας Δεδομένων, άρθρο 35, αναφορικά με την εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα.

7.1. Εισαγωγή

Το σύστημα διαχείρισης μάθησης του ιδρύματος χρησιμοποιείται για την παροχή ασύγχρονης διδασκαλίας και μάθησης και της συνεργασίας και αλληλεπίδρασης μεταξύ φοιτητών και διδασκόντων. Η επικοινωνία μεταξύ αυτών γίνεται ασύγχρονα μέσω χώρων συζητήσεων και ανακοινώσεων (forum) και σύγχρονα μέσω ανταλλαγής μηνυμάτων (chat). Οι διδάσκοντες αναρτούν το εκπαιδευτικό υλικό σε ψηφιακή μορφή (σημειώσεις, διαφάνειες, βίντεο, συνδέσμους σε ιστοτόπους στο διαδίκτυο, κ.α.) το οποίο μπορούν να ανακτούν οι φοιτητές και να το μεταφορτώνουν τοπικά τους υπολογιστές τους. Αναρτούν επίσης εκπαιδευτικές δραστηριότητες (κουίζ, δραστηριότητες, ενδιάμεσες και τελικές εργασίες αξιολόγησης ακαδημαϊκού εξαμήνου, κ.α.). Οι φοιτητές καλούνται να εκπονήσουν τις δραστηριότητες προαιρετικά για λόγους αυτο-αξιολόγησης, ή υποχρεωτικά προκειμένου να αξιολογηθούν και να λάβουν ανατροφοδότηση και βαθμό στο πλαίσιο των υποχρεώσεων τους για την επιτυχή παρακολούθηση και ολοκλήρωση του μαθήματος. Οι διδάσκοντες αξιολογούν τις υποβολές των φοιτητών και αναρτούν για τον καθένα ξεχωριστά ανατροφοδότηση καθώς και τον βαθμό τους. Η πλατφόρμα μπορεί να φιλοξενεί επίσης και θέματα τελικών εξετάσεων, σε περίπτωση που η

εξέταση του μαθήματος πραγματοποιείται με μορφή εκπόνησης εργασίας (project) στο τέλος του ακαδημαϊκού εξαμήνου. Οι βαθμοί των φοιτητών ανακτώνται μέσω κατάλληλης διασύνδεσης του συστήματος διαχείρισης μάθησης με το πληροφοριακό σύστημα του μητρώου φοιτητών (φοιτητολόγιο) για ενημέρωση του ηλεκτρονικού φακέλου του φοιτητή.

Η πλατφόρμα αρχικοποιείται από τους διαχειριστές του συστήματος πριν την έναρξη κάθε έτους ή εξαμήνου με την εγγραφή των χρηστών, την απόδοση κατάλληλων ρόλων με διαβαθμισμένη πρόσβαση σε φοιτητές και διδάσκοντες, τη δημιουργία μαθημάτων και την εγγραφή των χρηστών σε αυτά. Επίσης δίνονται τα κατάλληλα δικαιώματα και προνόμια στο προσωπικό του ιδρύματος που είναι απαραίτητο να έχει πρόσβαση στην πλατφόρμα. Όλες οι ενέργειες που πραγματοποιούνται και αφορούν δραστηριότητα των χρηστών στην πλατφόρμα, καταγράφονται σε αρχεία καταγραφής (log files).

Το σύστημα φιλοξενείται σε έναν εξυπηρετητή (server) στις πληροφοριακές υποδομές του ιδρύματος (in-house) ενώ η πρόσβαση σε αυτό γίνεται μέσω του προγράμματος περιήγησης του χρήστη. Για την πρόσβαση του χρήστη στο σύστημα χρησιμοποιούνται τα διαπιστευτήρια του στον λογαριασμό ηλεκτρονικού ταχυδρομείου (email account) μέσω της υπηρεσίας Κεντρικής Πιστοποίησης Χρηστών (Υπηρεσία «Single Sign On» - SSO) που παρέχεται από εξωτερικό πάροχο, ο οποίος έχει λάβει όλα τα απαραίτητα μέτρα για την αυθεντικοποίηση των χρηστών.

7.2. Πεδίο εφαρμογής

Σύμφωνα με τον ΓΚΠΔ, η ΕΑΠΔ είναι μια διαδικασία που σκοπεύει να περιγράψει την επεξεργασία, να αξιολογήσει την αναγκαιότητα και την αναλογικότητά της και να συνδράμει στη διαχείριση της επικινδυνότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που αυτή συνεπάγεται. Πρωταρχικός σκοπός της είναι να διασφαλιστεί και να αποδειχθεί ότι η επεξεργασία θα διενεργηθεί/διενεργείται σύμφωνα με τις θεμελιώδεις αρχές για την προστασία των προσωπικών δεδομένων, όπως αυτές επαναλαμβάνονται στο άρθρο 5 του ΓΚΠΔ. Παράλληλα, μέσω του προσδιορισμού και της περαιτέρω αξιολόγησης της επικινδυνότητας και

συνακόλουθα μέσω του καθορισμού μέτρων για την αντιμετώπισή της, η ΕΑΠΔ καθίσταται σημαντικό εργαλείο για την πλήρωση της υποχρέωσης λογοδοσίας, προκειμένου ο Υπεύθυνος Επεξεργασίας (το ακαδημαϊκό ίδρυμα), να μπορεί να αποδεικνύει ότι έχουν ληφθεί τα ενδεδειγμένα μέτρα για την επίτευξη της συμμόρφωσης σύμφωνα με τις προδιαγραφές του ΓΚΠΔ. Το ακαδημαϊκό ίδρυμα δεσμεύεται να προστατεύει τα Δεδομένα Προσωπικού Χαρακτήρα (ΔΠΧ) των υποκειμένων και να διατηρεί ένα διαφανή τρόπο στην επεξεργασία τους, τηρώντας τα όσα αναφέρονται στον ΓΚΠΔ. Επίσης, μέσω της μελέτης, ενημερώνει τα υποκείμενα των δεδομένων για τον τρόπο που το επιτυγχάνει αυτό.

Η κρίσιμη διεργασία (δραστηριότητα επεξεργασίας) για την οποία εκπονείται η ΕΑΠΔ είναι η ακόλουθη: *Επεξεργασία εκπαιδευτικών δεδομένων φοιτητών και διδασκόντων στο πλαίσιο της παροχής σύγχρονης και ασύγχρονης εξ αποστάσεως εκπαίδευσης*.

Σκοπός της δραστηριότητας επεξεργασίας είναι η παροχή σύγχρονης και ασύγχρονης εξ αποστάσεως διδασκαλίας και μάθησης, μέσω ηλεκτρονικής πλατφόρμας (συστήματος διαχείρισης μάθησης) όπου οι φοιτητές αλληλοεπιδρούν μεταξύ τους και με τους διδάσκοντες, μελετούν εκπαιδευτικό υλικό, εκπονούν δραστηριότητες, αξιολογούνται και βαθμολογούνται από τους διδάσκοντες στο πλαίσιο των υποχρεώσεων τους για την επιτυχή ολοκλήρωση των σπουδών τους σε προπτυχιακό ή μεταπτυχιακό επίπεδο σπουδών. Η δραστηριότητα επεξεργασίας είναι αναγκαία, λόγω της μορφής της προσφερόμενης εκπαίδευσης (εξ αποστάσεως ασύγχρονη και σύγχρονη εκπαίδευση) και επαρκής για το σκοπό αυτό, ωστόσο ενισχύεται με άλλα μέσα όπως οι εικονικές αίθουσες διδασκαλίας για την σύγχρονη διδασκαλία.

Τα υποκείμενα των δεδομένων είναι οι φοιτητές και οι διδάσκοντες του ιδρύματος. Η δραστηριότητα επεξεργασίας πραγματοποιείται μέσω του συστήματος διαχείρισης μάθησης σε ημερήσια βάση, κατά τη διάρκεια ενός ακαδημαϊκού έτους ή ακαδημαϊκού εξαμήνου. Αποδέκτες των δεδομένων είναι η διοίκηση του ιδρύματος και οι Προϊστάμενοι των Γραμματειών των Τμημάτων του ιδρύματος. Η επεξεργασία εκτελείται εσωτερικά στο ίδρυμα (δεν εμπλέκεται εξωτερικός εκτελών την επεξεργασία). Στη διαδικασία εμπλέκονται ο νόμιμος εκπρόσωπος, μέλος της

διοίκησης του ιδρύματος, ως «ο υπεύθυνος επεξεργασίας», οι διοικητικοί υπάλληλοι του ιδρύματος ως «ο εκτελών την επεξεργασία» καθώς και ο ορισμένος από την διοίκηση υπάλληλος ως «υπεύθυνος προστασίας δεδομένων».

Για την εκπόνηση της μελέτης ΕΑΠΔ χρησιμοποιήθηκαν:

- Ο Γενικός Κανονισμός Προστασίας Δεδομένων [15].
- Οι κατευθυντήριες γραμμές για την ΕΑΠΔ και για τον καθορισμό του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» [18].
- Το προτεινόμενο πρότυπο και οι σχετικές οδηγίες της Αρχής Προστασίας Δεδομένων της Γαλλίας (CNIL).
- Οι σχετικές οδηγίες της Αρχής Προστασίας Δεδομένων του Ηνωμένου Βασιλείου (ICO).
- Οι σχετικές οδηγίες του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) [46].
- Η διαδικτυακή πλατφόρμα για την ασφάλεια προσωπικών δεδομένων της ENISA (διαθέσιμη στον σύνδεσμο https://www.enisa.europa.eu/risk-level-tool/risk) και το εγχειρίδιο με τις βασικές λειτουργίες αυτής [49].

Στόχος της μελέτης ΕΑΠΔ είναι να αναγνωριστούν και να καταγραφούν οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, οι οποίοι απορρέουν από την επεξεργασία προσωπικών δεδομένων φοιτητών και διδασκόντων κατά την παροχή σύγχρονης και ασύγχρονης εκπαίδευσης μέσω ενός συστήματος διαχείρισης μάθησης. Τέτοιου είδους κίνδυνοι είναι η διαρροή προσωπικών δεδομένων, η μη εξουσιοδοτημένη τροποποίηση προσωπικών δεδομένων, και η απώλεια ή κλοπή προσωπικών δεδομένων. Γενικότερα, στόχος της ΕΑΠΔ είναι η εκτίμηση των επιπτώσεων στα υποκείμενα των δεδομένων σε περίπτωση απώλειας της διαθεσιμότητας, της εμπιστευτικότητας ή της ακεραιότητας των προσωπικών δεδομένων φοιτητών και διδασκόντων που υπόκεινται σε επεξεργασία μέσω του συστήματος διαχείρισης μάθησης.

7.3. Απαιτήσεις προστασίας δεδομένων

Τα προσωπικά δεδομένα ανά κατηγορία υποκειμένων είναι τα ακόλουθα:

- Φοιτητής: Όνομα Χρήστη, Επώνυμο, Όνομα, Αριθμός Μητρώου, email, Τηλέφωνο Επικοινωνίας, Ρόλος, Μάθημα, Τμήμα, Βαθμός Δραστηριοτήτων, Βαθμός Εξετάσεων
- Διδάσκοντας: Όνομα Χρήστη, Επώνυμο, Όνομα, Αριθμός Μητρώου, email, Τηλέφωνο Επικοινωνίας, Ρόλος, Μάθημα, Τμήμα
- Διοικητικό Προσωπικό: Όνομα Χρήστη, Επώνυμο, Όνομα, email, Τηλέφωνο Επικοινωνίας, Ρόλος, Μάθημα
- Τεχνικό Προσωπικό: Όνομα Χρήστη, Επώνυμο, Όνομα, Ρόλος

Το διοικητικό και τεχνικό προσωπικό του ιδρύματος έχει πρόσβαση στα δεδομένα όλων των χρηστών (το διοικητικό προσωπικό έχει περιορισμένη πρόσβαση επεξεργασίας), οι διδάσκοντες έχουν πρόσβαση σε επίπεδο μαθήματος ενώ οι φοιτητές έχουν περιορισμένη πρόσβαση σε επίπεδο τμήματος μόνο.

Οι φοιτητές έχουν πρόσβαση στα δεδομένα όσο διαρκεί η φοίτηση τους ενώ οι διδάσκοντες όσο έχουν σχέση εργασίας με το ίδρυμα. Τα υποκείμενα των δεδομένων ενημερώνονται για τα δικαιώματά τους και σχετικά με την επεξεργασία από τον υπεύθυνο επεξεργασίας ή την πολιτική απορρήτου που είναι αναρτημένη στο σύστημα διαχείρισης μάθησης. Η συγκατάθεση των υποκειμένων των δεδομένων επιτυγχάνεται με την αποδοχή της πολιτικής απορρήτου κατά την πρώτη τους είσοδο στο σύστημα διαχείρισης μάθησης. Τα υποκείμενα των δεδομένων μπορούν να ασκήσουν τα δικαιώματά του επικοινωνώντας με τον υπεύθυνο επεξεργασίας. Ο εκτελών την επεξεργασία λαμβάνει όλα τα τεχνικά και οργανωτικά μέτρα για την διασφάλιση της ασφάλειας των πληροφοριών στο σύστημα διαχείρισης μάθησης. Το ίδρυμα δεν διαχειρίζεται ούτε αποθηκεύει ευαίσθητα προσωπικά δεδομένα στο σύστημα διαχείρισης μάθησης.

7.4. Εκτίμηση επικινδυνότητας για την προστασία δεδομένων

Στο στάδιο αυτό πραγματοποιείται εκτίμηση της επικινδυνότητας, σε ότι αφορά τα δικαιώματα και τις ελευθερίες των υποκειμένων, σε περίπτωση απώλειας της ασφάλειας (εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα) των προσωπικών δεδομένων, σύμφωνα με επίπεδα επικινδυνότητας (Πίνακας 8) και το σχετικό

ερωτηματολόγιο (Πίνακας 9). Η εκτίμηση πραγματοποιείται για κάθε κατηγορία υποκειμένων.

7.4.1. Απώλεια Εμπιστευτικότητας

Η επίπτωση που θα μπορούσε να έχει μια μη εξουσιοδοτημένη αποκάλυψη προσωπικών δεδομένων (απώλεια εμπιστευτικότητας) εκτιμάται ως περιορισμένη καθώς μπορεί να οδηγήσει σε μη εξουσιοδοτημένη σύνδεση στο σύστημα διαχείρισης μάθησης, σε πιθανή αλλοίωση των υποβολών των φοιτητών σε δραστηριότητες και εργασίες, πιθανή αλλοίωση των δραστηριοτήτων και των εργασιών, πιθανή αλλοίωση της βαθμολογίας των φοιτητών, με αποτέλεσμα να επιφέρει επίπτωση στο υποκείμενο των δεδομένων και στη δημόσια εικόνα του.

Για τη μείωση της επικινδυνότητας, αποδίδονται συγκεκριμένοι ρόλοι στους χρήστες ώστε να περιορίζονται τα επίπεδα πρόσβασης στα δεδομένα. Επιπρόσθετα η αυθεντικοποίηση των χρηστών γίνεται από εξωτερικό πάροχο, ο οποίος έχει λάβει όλα τα απαραίτητα μέτρα για την ασφάλεια των πληροφοριών. Ταυτόχρονα το δίκτυο δεδομένων του ιδρύματος προστατεύεται από σύγχρονο λογισμικό (τοίχος προστασίας) και λαμβάνεται μέριμνα ώστε να είναι πάντα ενημερωμένη η έκδοση του συστήματος διαχείρισης μάθησης καθώς και το λειτουργικό σύστημα και το υποστηριζόμενο λογισμικό του εξυπηρετητή που το φιλοξενεί.

7.4.2. Απώλεια ακεραιότητας

Η επίπτωση που θα μπορούσε να έχει στο υποκείμενο μια μη εξουσιοδοτημένη τροποποίηση προσωπικών δεδομένων (απώλεια ακεραιότητας), εκτιμάται ως περιορισμένη. Η απώλεια ακεραιότητας μπορεί να οδηγήσει σε μη δυνατότητα πρόσβασης στο σύστημα διαχείρισης μάθησης.

Για την μείωση της επικινδυνότητας, οι χρήστες ενημερώνονται και εκπαιδεύονται για την επεξεργασία των δεδομένων σύμφωνα με τον ρόλο που τους έχει εκχωρηθεί. Επίσης, εφαρμόζεται πολιτική λήψης αντιγράφων ασφαλείας σύμφωνα με την οποία αυτά λαμβάνονται καθημερινά και διατηρούνται για πολλαπλές ημερομηνίες ώστε να γίνει επαναφορά των δεδομένων όποτε κριθεί απαραίτητο από τον διαχειριστή του συστήματος διαχείρισης μάθησης.

7.4.3. Απώλεια διαθεσιμότητας

Η επίπτωση που θα μπορούσε να έχει στο υποκείμενο μια μη εξουσιοδοτημένη καταστροφή ή απώλεια προσωπικών δεδομένων (απώλεια διαθεσιμότητας), εξαρτάται από την χρονική διάρκεια της απώλειας διαθεσιμότητας (θα μπορούσε να είναι αμελητέα ή περιορισμένη αν η απώλεια της διαθεσιμότητας ήταν μικρότερη ή μεγαλύτερη των 12 ωρών, αντίστοιχα). Η απώλεια διαθεσιμότητας μπορεί να οδηγήσει σε μη δυνατότητα πρόσβασης στο σύστημα διαχείρισης μάθησης και την έγκαιρη υποβολή δραστηριοτήτων και εργασιών προκειμένου να αξιολογηθούν από τους διδάσκοντες.

Για την μείωση της επικινδυνότητας υπάρχει τεχνικός ασφαλείας και διαχειριστής συστήματος που παρακολουθεί το σύστημα και δύναται να επέμβει σε οποιοδήποτε επίπεδο για να διορθώσει σφάλματα που έχουν προκαλέσει την μη διαθεσιμότητα αυτού.

7.4.4. Συνολική εκτίμηση επικινδυνότητας

Σύμφωνα με τα προηγούμενα, η συνολική επικινδυνότητα εκτιμάται ως περιορισμένη.

7.5. Εκτίμηση εμφάνισης απειλών

Στο στάδιο αυτό προσδιορίζεται το επίπεδο της πιθανότητας εμφάνισης απειλών συνολικά για κάθε περιοχή αξιολόγησης (Πίνακας 15). Για την ανάλυση ο υπεύθυνος επεξεργασίας καλείται να απαντήσει σε μια σειρά από ερωτήματα.

7.5.1. Δίκτυο και τεχνικοί πόροι (υλικό και λογισμικό)

- Γίνεται κάποιο μέρος της επεξεργασίας προσωπικών δεδομένων μέσω του διαδικτύου; ΝΑΙ
- Είναι δυνατή η παροχή απομακρυσμένης πρόσβασης μέσω του διαδικτύου; ΟΧΙ
- Είναι το σύστημα επεξεργασίας προσωπικών δεδομένων διασυνδεδεμένο με άλλο εξωτερικό ή εσωτερικό σύστημα ή υπηρεσία πληροφορικής; ΝΑΙ
- Μπορούν μη εξουσιοδοτημένα άτομα να έχουν εύκολη πρόσβαση στο περιβάλλον επεξεργασίας δεδομένων; ΟΧΙ

- Ακολουθούνται σχετικές τεκμηριωμένες βέλτιστες πρακτικές για την συντήρηση του συστήματος επεξεργασίας προσωπικών δεδομένων; ΝΑΙ

Με βάση τα παραπάνω ο συνολικός βαθμός πιθανότητας εμφάνισης απειλών εκτιμάται ως χαμηλός.

7.5.2. Διεργασίες/διαδικασίες που σχετίζονται με την επεξεργασία δεδομένων

- Είναι οι ρόλοι και οι αρμοδιότητες όσον αφορά την επεξεργασία προσωπικών δεδομένων ασαφείς ή δεν είναι σαφώς καθορισμένες; ΟΧΙ
- Είναι η αποδεκτή χρήση του δικτύου, του συστήματος και των φυσικών πόρων εντός του οργανισμού ασαφής ή δεν ορίζεται σαφώς; ΟΧΙ
- Επιτρέπεται στους εργαζόμενους να φέρουν και να χρησιμοποιούν τις δικές τους συσκευές για να συνδεθούν στο σύστημα επεξεργασίας προσωπικών δεδομένων; ΟΧΙ
- Επιτρέπεται στους εργαζόμενους να μεταφέρουν, να αποθηκεύουν ή να επεξεργάζονται με άλλο τρόπο προσωπικά δεδομένα εκτός των εγκαταστάσεων του οργανισμού; ΟΧΙ
- Μπορούν να πραγματοποιηθούν δραστηριότητες επεξεργασίας προσωπικών δεδομένων χωρίς τη δημιουργία αρχείων καταγραφής; ΟΧΙ

Με βάση τα παραπάνω ο συνολικός βαθμός πιθανότητας εμφάνισης απειλών εκτιμάται ως χαμηλός.

7.5.3. Διάφορα μέρη και άτομα που εμπλέκονται στη διαδικασία επεξεργασίας

- Η επεξεργασία προσωπικών δεδομένων πραγματοποιείται από απροσδιόριστο αριθμό εργαζομένων; ΟΧΙ
- Εκτελείται οποιοδήποτε μέρος της διαδικασίας επεξεργασίας δεδομένων από ανάδοχο/τρίτο μέρος (υπεύθυνος επεξεργασίας δεδομένων); ΟΧΙ
- Οι υποχρεώσεις των μερών/προσώπων που εμπλέκονται στην επεξεργασία προσωπικών δεδομένων είναι ασαφείς ή δεν δηλώνονται με σαφήνεια; ΟΧΙ
- Το προσωπικό που εμπλέκεται στην επεξεργασία προσωπικών δεδομένων δεν είναι εξοικειωμένο με θέματα ασφάλειας; ΟΧΙ

- Τα πρόσωπα/μέρη που εμπλέκονται στη λειτουργία επεξεργασίας δεδομένων παραμελούν την ασφαλή αποθήκευση και/ή καταστροφή προσωπικών δεδομένων; ΟΧΙ

Με βάση τα παραπάνω ο συνολικός βαθμός πιθανότητας εμφάνισης απειλών εκτιμάται ως χαμηλός.

7.5.4. Επιχειρηματικός τομέας και κλίμακα επεξεργασίας

- Θεωρείτε ότι ο τομέας της επιχείρησής σας είναι επιρρεπής σε κυβερνοεπιθέσεις; ΟΧΙ
- Ο οργανισμός σας έχει υποστεί κυβερνοεπίθεση ή άλλου είδους παραβίαση ασφάλειας τα τελευταία δύο χρόνια; ΟΧΙ
- Έχετε λάβει ειδοποιήσεις ή/και παράπονα σχετικά με την ασφάλεια του συστήματος που χρησιμοποιείται για την επεξεργασία προσωπικών δεδομένων τον τελευταίο χρόνο; ΟΧΙ
- Η λειτουργία επεξεργασίας σας αφορά μεγάλο όγκο προσώπων ή/και προσωπικών δεδομένων; ΝΑΙ
- Υπάρχουν βέλτιστες πρακτικές ασφαλείας ειδικά για τον επιχειρηματικό σας τομέα που δεν έχουν ακολουθηθεί επαρκώς; ΝΑΙ

Με βάση τα παραπάνω ο συνολικός βαθμός πιθανότητας εμφάνισης απειλών εκτιμάται ως Μέτριος.

7.5.5. Συνολική εκτίμηση εμφάνισης απειλών

Σύμφωνα με τα προηγούμενα, η συνολική επικινδυνότητα εμφάνισης απειλών εκτιμάται ως χαμηλή (Πίνακας 18).

Περιοχή αξιολόγησης	**Εκτίμηση Πιθανότητας**	
	Επίπεδο	**Τιμή**
Δίκτυο και τεχνικοί πόροι (υλικό και λογισμικό)	Υψηλή ☐ Μέτρια ☐ Χαμηλή ☒	3 2 1
Διεργασίες/διαδικασίες που σχετίζονται με την επεξεργασία δεδομένων	Υψηλή ☐ Μέτρια ☐	3 2

	Χαμηλή ☒	1
Διάφορα μέρη και άτομα που εμπλέκονται στη διαδικασία επεξεργασίας	Υψηλή ☐ Μέτρια ☐ Χαμηλή ☒	3 2 1
Επιχειρηματικός τομέας και κλίμακα επεξεργασίας	Υψηλή ☐ Μέτρια ☒ Χαμηλή ☐	3 2 1
Συνολική πιθανότητα εμφάνισης απειλών	Χαμηλή	5

Πίνακας 18 Μελέτη περίπτωσης: Εκτίμηση πιθανότητας εμφάνισης απειλών

7.6. Εκτίμηση επικινδυνότητας επεξεργασίας πληροφορικών

Μετά την εκτίμηση της επίπτωσης της επικινδυνότητας της επεξεργασίας των δεδομένων και της πιθανότητας εμφάνισης, το επίπεδο επικινδυνότητας υπολογίζεται ως μέτριο (Πίνακας 19).

Επίπτωση στα δεδομένα του υποκειμένου	Υψηλή			
	Μέτρια			
	Χαμηλή		**X**	
		Χαμηλή	Μέτρια	Υψηλή
		Πιθανότητα		

Πίνακας 19 Μελέτη περίπτωσης: Πίνακας επικινδυνότητας

7.7. Μέτρα για την διασφάλιση της προστασίας προσωπικών δεδομένων

Στη συνέχεια ακολουθεί ένας κατάλογος με προτεινόμενα τεχνικά και οργανωτικά μέτρα για τη λειτουργία επεξεργασίας των προσωπικών δεδομένων, το επίπεδο επικινδυνότητας της οποίας εκτιμήθηκε ως μέτριο, σύμφωνα με τις πληροφορίες που

παρασχέθηκαν προηγουμένως. Τα μέτρα έχουν συσχετιστεί με τους ελέγχους όπως ορίζονται στο πρότυπο ISO/IEC 27001:2013 [24].

Πολιτική και διαδικασίες ασφαλείας για την προστασία των προσωπικών δεδομένων (σχετικό με τον έλεγχο Α.5)

- Ο οργανισμός θα πρέπει να τεκμηριώνει μια ξεχωριστή ειδική πολιτική ασφαλείας όσον αφορά την επεξεργασία προσωπικών δεδομένων. Η πολιτική θα πρέπει να εγκρίνεται από τη διοίκηση και να κοινοποιείται σε όλους τους υπαλλήλους και τα σχετικά εξωτερικά μέρη.
- Η πολιτική ασφαλείας θα πρέπει τουλάχιστον να αναφέρεται: στους ρόλους και τις ευθύνες του προσωπικού, στα βασικά τεχνικά και οργανωτικά μέτρα που λαμβάνονται για την ασφάλεια των δεδομένων προσωπικού χαρακτήρα, στους εκτελούντες την επεξεργασία δεδομένων ή σε άλλα τρίτα μέρη που εμπλέκονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Θα πρέπει να δημιουργηθεί και να διατηρηθεί κατάλογος συγκεκριμένων πολιτικών/διαδικασιών που σχετίζονται με την ασφάλεια των προσωπικών δεδομένων, με βάση τη γενική πολιτική ασφάλειας.

Ρόλοι και οι αρμοδιότητες (σχετικό με τον έλεγχο Α.6.1.1)

- Θα πρέπει να πραγματοποιείται σαφής καθορισμός προσώπων που είναι επιφορτισμένα με συγκεκριμένα καθήκοντα ασφαλείας, συμπεριλαμβανομένων του υπευθύνου ασφαλείας.

Πολιτική ελέγχου πρόσβασης (σχετικό με τον έλεγχο Α.9.1.1)

- Μια πολιτική ελέγχου πρόσβασης πρέπει να είναι λεπτομερής και τεκμηριωμένη. Θα πρέπει να καθορίσει σε αυτό το έγγραφο τους κατάλληλους κανόνες ελέγχου πρόσβασης, την οργάνωση δικαιωμάτων πρόσβασης και τους περιορισμούς για συγκεκριμένους ρόλους χρηστών στις διαδικασίες και διαδικασίες που σχετίζονται με προσωπικά δεδομένα
- Θα πρέπει να πραγματοποιείται σαφής καθορισμός προσώπων που είναι επιφορτισμένα με συγκεκριμένα καθήκοντα ασφαλείας, συμπεριλαμβανομένων του υπευθύνου ασφαλείας.

Διαχείριση πόρων/περιουσιακών στοιχείων (σχετικό με τον έλεγχο Α.8)

- Οι ρόλοι που έχουν πρόσβαση σε ορισμένους πόρους πρέπει να ορίζονται και να τεκμηριώνονται.

Διαχείριση αλλαγών (σχετικό με τον έλεγχο Α.12.1)

- Θα πρέπει να υπάρχει μια λεπτομερής και τεκμηριωμένη πολιτική αλλαγής. Θα πρέπει να περιλαμβάνει: μια διαδικασία εισαγωγής αλλαγών, τους ρόλους/χρήστες που έχουν δικαιώματα αλλαγής, χρονοδιαγράμματα για την εισαγωγή αλλαγών. Η πολιτική αλλαγής θα πρέπει να ενημερώνεται τακτικά.

Εκτελών την επεξεργασία (σχετικό με τον έλεγχο Α.15)

- Ο υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να ελέγχει τακτικά τη συμμόρφωση του εκτελούντος την επεξεργασία δεδομένων με το συμφωνημένο επίπεδο απαιτήσεων και υποχρεώσεων.

Χειρισμός συμβάντων / Παραβιάσεις προσωπικών δεδομένων (σχετικό με τον έλεγχο Α.16)

- Το σχέδιο αντιμετώπισης συμβάντων θα πρέπει να τεκμηριώνεται, συμπεριλαμβανομένης μιας λίστας πιθανών ενεργειών μετριασμού και σαφούς ανάθεσης ρόλων.

Επιχειρησιακή συνέχεια (σχετικό με τον έλεγχο Α.17)

- Ένα πλάνο επιχειρησιακής συνέχειας πρέπει να είναι λεπτομερές και τεκμηριωμένο (σύμφωνα με τη γενική πολιτική ασφαλείας). Θα πρέπει να περιλαμβάνει σαφείς ενέργειες και ανάθεση ρόλων.
- Το επίπεδο εγγυημένης ποιότητας υπηρεσιών θα πρέπει να ορίζεται στο πλάνο επιχειρησιακής συνέχειας για τις βασικές επιχειρηματικές διαδικασίες που προβλέπουν την ασφάλεια των προσωπικών δεδομένων.

Εμπιστευτικότητα του προσωπικού (σχετικό με τον έλεγχο Α.7)

- Πριν από την ανάληψη των καθηκόντων τους, οι εργαζόμενοι θα πρέπει να κληθούν να επανεξετάσουν και να συμφωνήσουν σχετικά με την πολιτική

ασφάλειας του οργανισμού και να υπογράψουν αντίστοιχες συμφωνίες εμπιστευτικότητας και μη αποκάλυψης.

Κατάρτιση προσωπικού (σχετικό με τον έλεγχο Α.7.2.2)

- Ο οργανισμός θα πρέπει να έχει δομημένα και τακτικά προγράμματα κατάρτισης για το προσωπικό, συμπεριλαμβανομένων ειδικών προγραμματιστών για την εισαγωγή (σε θέματα προστασίας δεδομένων) νεοεισερχομένων.

Έλεγχος πρόσβασης και αυθεντικοποίηση (σχετικό με τον έλεγχο Α.9)

- Θα πρέπει να οριστεί και να τεκμηριωθεί μια συγκεκριμένη πολιτική κωδικού πρόσβασης. Η πολιτική θα πρέπει να περιλαμβάνει τουλάχιστον το μήκος, την πολυπλοκότητα και την περίοδο ισχύος του κωδικού πρόσβασης, καθώς και τον αριθμό των αποδεκτών αποτυχημένων προσπαθειών σύνδεσης.
- Οι κωδικοί πρόσβασης χρήστη πρέπει να αποθηκεύονται σε "κατακερματισμένη" μορφή (με εφαρμογή συνάρτησης κατακερματισμού που δεν αντιστρέφεται) ώστε ακόμα κι αν γίνει υποκλοπή, ο επιτιθέμενος να μην μπορεί να γνωρίζει τους αρχικούς κωδικούς πρόσβασης.

Καταγραφή και παρακολούθηση (σχετικό με τον έλεγχο Α.12.4)

- Οι ενέργειες των διαχειριστών και των χειριστών συστήματος, συμπεριλαμβανομένης της προσθήκης/διαγραφής/αλλαγής δικαιωμάτων χρήστη θα πρέπει να καταγράφονται.
- Δεν θα πρέπει να υπάρχει δυνατότητα διαγραφής ή τροποποίησης του περιεχομένου των αρχείων καταγραφής. Επίσης, η πρόσβαση στα αρχεία καταγραφής θα πρέπει να καταγράφεται, εκτός από την παρακολούθηση, για τον εντοπισμό ασυνήθιστης δραστηριότητας.
- Ένα σύστημα παρακολούθησης θα πρέπει να επεξεργάζεται τα αρχεία καταγραφής και να παράγει αναφορές για την κατάσταση του συστήματος και να ειδοποιεί για πιθανές ειδοποιήσεις.

Ασφάλεια διακομιστή/βάσης δεδομένων (σχετικό με τον έλεγχο Α.12)

- Οι λύσεις κρυπτογράφησης θα πρέπει να εξετάζονται σε συγκεκριμένα αρχεία ή εγγραφές μέσω εφαρμογής λογισμικού ή υλικού.
- Θα πρέπει να ληφθεί υπόψη η κρυπτογράφηση μονάδων αποθήκευσης.
- Οι τεχνικές ψευδωνυμοποίησης θα πρέπει να εφαρμόζονται μέσω του διαχωρισμού των δεδομένων από τα άμεσα αναγνωριστικά για να αποφευχθεί η σύνδεση με το υποκείμενο των δεδομένων χωρίς πρόσθετες πληροφορίες.

Ασφάλεια σταθμού εργασίας (σχετικό με τον έλεγχο Α.14.1)

- Οι εφαρμογές προστασίας από ιούς και οι υπογραφές ανίχνευσης θα πρέπει να διαμορφώνονται σε καθημερινή βάση.

Ασφάλεια δικτύου/επικοινωνιών (σχετικό με τον έλεγχο Α.13)

- Η ασύρματη πρόσβαση στο σύστημα θα πρέπει να επιτρέπεται μόνο για συγκεκριμένους χρήστες και διαδικασίες. Θα πρέπει να προστατεύεται από μηχανισμούς κρυπτογράφησης.
- Η απομακρυσμένη πρόσβαση στο σύστημα θα πρέπει γενικά να αποφεύγεται. Σε περιπτώσεις όπου αυτό είναι απολύτως απαραίτητο, θα πρέπει να εκτελείται μόνο υπό τον έλεγχο και την παρακολούθηση συγκεκριμένου ατόμου από τον οργανισμό (π.χ. διαχειριστή/υπεύθυνο ασφαλείας) μέσω προκαθορισμένων συσκευών.
- Η κίνηση από και προς το σύστημα θα πρέπει να παρακολουθείται και να ελέγχεται μέσω τειχών προστασίας και συστημάτων ανίχνευσης εισβολής.

Αντίγραφα ασφαλείας (σχετικό με τον έλεγχο Α.12.3)

- Τα πλήρη αντίγραφα ασφαλείας θα πρέπει να λαμβάνονται τακτικά.
- Τα εφεδρικά μέσα θα πρέπει να ελέγχονται τακτικά για να διασφαλίζεται ότι μπορείτε να βασιστείτε σε αυτά για χρήση έκτακτης ανάγκης.
- Τα προγραμματισμένα αυξητικά αντίγραφα ασφαλείας θα πρέπει να πραγματοποιούνται τουλάχιστον σε καθημερινή βάση.

- Αντίγραφα του αντιγράφου ασφαλείας θα πρέπει να αποθηκεύονται με ασφάλεια σε διαφορετικές τοποθεσίες.
- Σε περίπτωση που χρησιμοποιείται υπηρεσία τρίτου μέρους για δημιουργία αντιγράφων ασφαλείας, το αντίγραφο πρέπει να κρυπτογραφηθεί πριν μεταδοθεί από τον υπεύθυνο επεξεργασίας.

Κινητές/Φορητές συσκευές (σχετικό με τον έλεγχο Α.6.2)

- Οι συγκεκριμένοι ρόλοι και αρμοδιότητες σχετικά με τη διαχείριση κινητών και φορητών συσκευών θα πρέπει να καθοριστούν με σαφήνεια.
- Ο οργανισμός θα πρέπει να μπορεί να διαγράφει εξ αποστάσεως προσωπικά δεδομένα (που σχετίζονται με τη λειτουργία επεξεργασίας του) σε μια κινητή συσκευή που έχει παραβιαστεί.
- Οι κινητές συσκευές θα πρέπει να υποστηρίζουν τον διαχωρισμό της ιδιωτικής και επαγγελματικής χρήσης της συσκευής μέσω ασφαλών κοντέινερ λογισμικού.
- Οι φορητές συσκευές θα πρέπει να προστατεύονται φυσικά από κλοπή όταν δεν χρησιμοποιούνται.

Ασφάλεια κύκλου ζωής εφαρμογής (σχετικό με τον έλεγχο Α.12.6 και Α.14.2)

- Η αξιολόγηση τρωτότητας, οι δοκιμές διείσδυσης εφαρμογών και υποδομής θα πρέπει να εκτελούνται από αξιόπιστο τρίτο μέρος πριν από την επιχειρησιακή έγκριση. Η αίτηση δεν εγκρίνεται παρά μόνο εάν επιτευχθεί το απαιτούμενο επίπεδο ασφάλειας.
- Πρέπει να γίνεται περιοδικός έλεγχος διείσδυσης.
- Θα πρέπει να ληφθούν πληροφορίες σχετικά με τις τεχνικές ευπάθειες των συστημάτων πληροφοριών που χρησιμοποιούνται.
- Οι ενημερώσεις κώδικα λογισμικού θα πρέπει να ελέγχονται και να αξιολογούνται πριν εγκατασταθούν σε λειτουργικό περιβάλλον.

Διαγραφή/απόρριψη δεδομένων (σχετικό με τον έλεγχο Α.8.3.2)

- Θα πρέπει να εκτελούνται πολλαπλά περάσματα αντικατάστασης βάσει λογισμικού σε όλα τα μέσα πριν από την απόρριψη.

- Εάν οι υπηρεσίες τρίτου χρησιμοποιούνται για την ασφαλή απόρριψη εγγραφών μέσων ή χαρτιού, θα πρέπει να υπάρχει συμφωνία παροχής υπηρεσιών και να δημιουργείται αρχείο καταστροφής των εγγραφών, όπως αρμόζει.

Σωματική ασφάλεια (σχετικό με τον έλεγχο Α.11)

- θα πρέπει να δημιουργηθεί σαφής αναγνώριση, με κατάλληλα μέσα (π.χ. Σήματα ID), και κατά περίπτωση, για όλο το προσωπικό και τους επισκέπτες που έχουν πρόσβαση στις εγκαταστάσεις του οργανισμού.
- Οι ασφαλείς ζώνες θα πρέπει να ορίζονται και να προστατεύονται με κατάλληλους ελέγχους εισόδου. Επομένως, ένα φυσικό ημερολόγιο ή ηλεκτρονική διαδρομή ελέγχου κάθε πρόσβασης θα πρέπει να τηρείται και να παρακολουθείται με ασφάλεια.
- Σε όλες τις ζώνες ασφαλείας θα πρέπει να εγκατασταθούν συστήματα ανίχνευσης εισβολέων.
- Τα φυσικά εμπόδια θα πρέπει, κατά περίπτωση, να δημιουργούνται για να αποτρέπεται η μη εξουσιοδοτημένη φυσική πρόσβαση.
- Οι κενές ασφαλείς περιοχές θα πρέπει να κλειδώνονται φυσικά και να ελέγχονται περιοδικά
- Στο χώρο εγκατάστασης του διακομιστή (υπολογιστικό κέντρο, computer room) θα πρέπει να είναι εγκατεστημένο αυτόματο σύστημα πυρόσβεσης, αποκλειστικό σύστημα κλιματισμού κλειστού ελέγχου και αδιάλειπτο τροφοδοτικό τάσης (UPS).
- Το προσωπικό της υπηρεσίας υποστήριξης εξωτερικών μερών θα πρέπει να έχει περιορισμένη πρόσβαση σε ασφαλείς περιοχές.

8. Επίλογος

Αντικείμενο μελέτης της παρούσας εργασίας ήταν η διαχείριση της επικινδυνότητας στην επεξεργασία δεδομένων σύμφωνα με τις απαιτήσεις του διεθνούς προτύπου ISO/IEC 27001 που αφορά στην ασφάλεια της πληροφορίας και τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ, GDPR) που ισχύει στην Ευρωπαϊκή Ένωση από τον Μάιο του 2018. Παρουσιάστηκαν μοντέλα ασφάλεια της πληροφορίας, διαδικασίες και τεχνικές για την διαχείριση της επικινδυνότητας, τα στάδια εκτίμησης της επικινδυνότητας τόσο από την άποψη του ISO/IEC 27001 όσο και του ΓΚΠΔ, κα η μελέτη εκτίμηση του αντικτύπου στην επεξεργασία δεδομένων με εφαρμογή σε εκπαιδευτικά δεδομένα που διατηρούνται σε ένα εικονικό περιβάλλον μάθησης ενός πανεπιστημιακού ιδρύματος που προσφέρει εκπαίδευση από απόσταση.

Συμπερασματικά μπορούμε να αναφέρουμε την αναγκαιότητα της υιοθέτησης και εφαρμογής ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφορίας από κάθε επιχείρηση και οργανισμό που επεξεργάζεται δεδομένα υποκειμένων και τη συμμόρφωση του με το πρότυπο ISO/IEC 27701, διότι με αυτόν τον τρόπο πιστοποιείται αλλά και αυξάνεται η αξιοπιστία και το κύρος του, καθώς και τη συμμόρφωση του με τις κανονιστικές διατάξεις του ΓΚΠΔ, ο οποίος προσεγγίζει την ασφάλεια της πληροφορίας από τον πλευρά των υποκειμένων και φροντίζει για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Ο ΓΚΠΔ προσδιορίζει τις μορφές επεξεργασίας δεδομένων για τις οποίες απαιτείται η μελέτη εκτίμησης αντικτύπου για την προστασία των δεδομένων (ΕΑΠΔ, DPIA).

Πρόσφατες επιστημονικές εργασίες προτείνουν την εφαρμογή ενός ευρύτερου πλαισίου, που συμπεριλαμβάνει τόσο νομικές απαιτήσεις όσο και καλές πρακτικές για την αναγνώριση και την αντιμετώπιση της επικινδυνότητας στην ιδιωτικότητα των δεδομένων σε πρώιμα στάδια (δείτε για παράδειγμα το [50]), βοηθώντας οργανισμούς και επιχειρήσεις να υιοθετήσουν καλύτερες πολιτικές και συστήματα. Η μελέτη ενός τέτοιου πλαισίου και η εφαρμογή του, για παράδειγμα, σε ένα εκπαιδευτικό ίδρυμα ανώτατης εκπαίδευσης, θα μπορούσε να αποτελέσει μελλοντική εργασία.

Βιβλιογραφία

[1] 'ISO Guide 73:2009(en), Risk management — Vocabulary'. Ημερομηνία πρόσβασης: 25 Οκτώβριος 2022. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.iso.org/obp/ui/#iso:std:44651:en

[2] 'ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary', ISO. Ημερομηνία πρόσβασης: 8 Ιανουάριος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.iso.org/standard/73906.html

[3] Β. Βερύκιος, Σ. Κωτσιαντής, Η. Σταυρόπουλος, και Μ. Τζαγκαράκης, 'Η Επιστήμη των Δεδομένων - Βασικές Αρχές, Θεωρία & Εφαρμογές με τη Γλώσσα R.', Εκδόσεις Νέων Τεχνολογιών - New Tech Pub. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://newtech-pub.com/βιβλία/πληροφορική/γλώσσες-προγραμματισμού/η-επιστήμη-των-δεδομένων-βασικές-αρχέ/

[4] Ι. Μαυρίδης, *Ασφάλεια πληροφοριών στο διαδίκτυο*. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις, 2015. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://hdl.handle.net/11419/1024

[5] P. McClanahan, *Information Security*. Libre Texts Project, 2013. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://eng.libretexts.org/Courses/Delta_College/Information_Security

[6] 'Το Πανεπιστήμιο Θεσσαλίας Μετά Την Κακοκαιρία Daniel – Ενημέρωση Από Τον Πρύτανη | Τμήμα Κτηνιατρικής'. Ημερομηνία πρόσβασης: 14 Μάρτιος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.vet.uth.gr/?p=9547

[7] 'Common Data Threats and Vulnerabilities | Society Insurance'. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://societyinsurance.com/blog/common-data-threats-and-vulnerabilities/

[8] D. B. Parker, 'A comprehensive list of threats to information', *Inf. Syst. Secur.*, τ. 2, τχ. 2, σσ. 10–14, Ιανουαρίου 1993, doi: 10.1080/19393559308551348.

[9] 'ENISA Threat Landscape 2023', ENISA. Ημερομηνία πρόσβασης: 26 Φεβρουάριος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[10] G. Pender-Bey, 'THE PARKERIAN HEXAD The CIA Triad Model Expanded'.

[11] J. McCumber, 'Information Systems Security: A Comprehensive Model', στο *14th National Computer Security Conference*, Baltimore, MD: National Institute of Standards and Technology, Οκτωβρίου 1991.

[12] J. McCumber, *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*. Auerbach Publications, 2004.

[13] C. Easttom, 'Computer security fundamentals', 2019, Ημερομηνία πρόσβασης: 5 Ιανουάριος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.oreilly.com/library/view/computer-security-fundamentals/9780135774854/

[14] 'Προστασία δεδομένων - Ευρωπαϊκή Επιτροπή'. Ημερομηνία πρόσβασης: 8 Ιανουάριος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://commission.europa.eu/law/law-topic/data-protection_el

[15] 'ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/ 679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ - της 27ης Απριλίου 2016 - για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/ 46/ ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)'.

[16] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, τ. 119. 2016. Ημερομηνία πρόσβασης: 8 Ιανουάριος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: http://data.europa.eu/eli/reg/2016/679/oj/eng

[17] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, τ. 281. 1995. Ημερομηνία πρόσβασης: 8 Ιανουάριος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: http://data.europa.eu/eli/dir/1995/46/oj/eng

[18] 'JUSTICE AND CONSUMERS ARTICLE 29 - Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)'. Ημερομηνία πρόσβασης: 8 Ιανουάριος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/items/611236/en

[19] 'Αρχές νομιμότητας επεξεργασίας', dpa.gr. Ημερομηνία πρόσβασης: 12 Μάιος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: http://www.dpa.gr/el/foreis/arxes_nomimotitas

[20] Σ. Κάτσικας, Σ. Γκρίτζαλης, και Κ. Λαμπρινουδάκης, *Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο*. Εκδόσεις Νέων Τεχνολογιών, 2021.

[21] P. Bowen, J. Hash, και M. Wilson, 'SP 800-100, Information Security Handbook: A Guide for Managers | CSRC'. Ημερομηνία πρόσβασης: 8 Ιανουάριος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://csrc.nist.gov/pubs/sp/800/100/upd1/final

[22] 'ISO/IEC 27001:2022 - Information technology — Security techniques — Information security management systems — Requirements', ISO. Ημερομηνία πρόσβασης: 8 Ιανουάριος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.iso.org/standard/27001

[23] 'ISO/IEC 17065:2012', ISO. Ημερομηνία πρόσβασης: 9 Ιανουάριος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.iso.org/standard/46568.html

[24] 'ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements'. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.iso.org/standard/54534.html

[25] 'ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management', ISO. Ημερομηνία πρόσβασης: 8 Ιανουάριος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.iso.org/standard/75281.html

[26] 'ISO - ISO 31000:2018 - Risk management — Guidelines'. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.iso.org/standard/65694.html

[27] 'ISO - IEC 31010:2009 - Risk management — Risk assessment techniques'. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.iso.org/standard/51073.html
[28] 'ISO - IEC 31010:2019 - Risk management — Risk assessment techniques'. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.iso.org/standard/72140.html
[29] Δ. Γραφανάκης, *Στατιστικός Έλεγχος Ποιότητας*. Ελληνικό Ανοικτό Πανεπιστήμιο, 2000.
[30] Σ. Στεφανάτος, *Ολική Ποιότητα*. Ελληνικό Ανοικτό Πανεπιστήμιο, 2000.
[31] M. M. Grime και G. Wright, 'Delphi Method', στο *Wiley StatsRef: Statistics Reference Online*, Wiley, 2016, σσ. 1–6. doi: 10.1002/9781118445112.STAT07879.
[32] Κ. Κατσούλας, 'Ο προσδιορισμός των ικανοτήτων αποτελεσματικής διδασκαλίας στο πεδίο της δια βίου εκπαίδευσης από απόσταση με την τεχνική Delphi', *Διεθνές Συνέδριο Για Την Ανοικτή Εξ Αποστάσεως Εκπαίδευση*, τ. 7, τχ. 3Α, Ιουνίου 2013, doi: 10.12681/ICODL.606.
[33] Χ. Αγγελόπουλος, *Σχεδιασμός για την Ποιότητα*. Ελληνικό Ανοικτό Πανεπιστήμιο, 2000.
[34] 'What is HAZOP? Hazard and Operability Study | SafetyCulture'. Ημερομηνία πρόσβασης: 26 Οκτώβριος 2022. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://safetyculture.com/topics/hazop/
[35] C. Peace, 'The risk matrix: Uncertain results?', *Policy Pract. Health Saf.*, τ. 15, σσ. 1–14, Ιουλίου 2017, doi: 10.1080/14773996.2017.1348571.
[36] Ι. Μπακούρος, *Αξιοπιστία και Συντήρηση*. Ελληνικό Ανοικτό Πανεπιστήμιο, 2022.
[37] J. Watson, *Strategy: An Introduction to Game Theory*, Third edition. W. W. Norton & Company, 2013.
[38] Γ. Βαρουφάκης, *ΘΕΩΡΙΑ ΠΑΙΓΝΙΩΝ*. Ημερομηνία πρόσβασης: 27 Φεβρουάριος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.politeianet.gr/books/9789600111347-varoufakis-yanis-gutenberg-theoria-paignion-197385
[39] 'Layer of Protection Analysis: Simplified Process Risk Assessment'. Ημερομηνία πρόσβασης: 27 Φεβρουάριος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.aiche.org/resources/publications/books/layer-protection-analysis-simplified-process-risk-assessment
[40] J. R. Cristóbal, 'The S-curve envelope as a tool for monitoring and control of projects', *Procedia Comput. Sci.*, τ. 121, σσ. 756–761, Ιανουαρίου 2017, doi: 10.1016/j.procs.2017.11.097.
[41] D. Brauer και J. Cesarone, *Total Manufacturing Assurance: Controlling Product Quality, Reliability, and Safety*. CRC Press, 2022.
[42] 'Risk management: Expert guidance - ALARP at a glance'. Ημερομηνία πρόσβασης: 26 Φεβρουάριος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.hse.gov.uk/enforce/expert/alarpglance.htm
[43] N. T. Thomopoulos, *Essentials of Monte Carlo Simulation: Statistical Methods for Building Simulation Models*. New York, NY: Springer, 2013. doi: 10.1007/978-1-4614-6022-0.

[44] M. Dean, *A Practical Guide to Multi-Criteria Analysis*. 2022. doi: 10.13140/RG.2.2.15007.02722.

[45] B. e.V, 'Risk Assessment & Data Protection Impact Assessment | Leitfaden 2017 | Bitkom e. V.' Ημερομηνία πρόσβασης: 27 Μάρτιος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.bitkom.org/Bitkom/Publikationen/Risk-Assessment-Data-Protection-Impact-Assessment.html

[46] 'Handbook on Security of Personal Data Processing', ENISA. Ημερομηνία πρόσβασης: 17 Απρίλιος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

[47] 'ISO/IEC 29151:2017(en), Information technology — Security techniques — Code of practice for personally identifiable information protection'. Ημερομηνία πρόσβασης: 2 Απρίλιος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:29151:ed-1:v1:en

[48] 'What does data protection 'by design' and 'by default' mean? - European Commission'. Ημερομηνία πρόσβασης: 2 Απρίλιος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en

[49] 'Online Platform for Security of Personal Data Processing', ENISA. Ημερομηνία πρόσβασης: 17 Απρίλιος 2024. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-platform

[50] D. K. Pipyros, 'A mutli-attribute privacy maturity methodology for data protection risk assessment and management'.

Υπεύθυνη Δήλωση Συγγραφέα:

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν.1599/1986, η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης.