Α.Ε.Ι. ΠΕΙΡΑΙΑ Τ.Τ.
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΤΕ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
"Διαχείριση και Ενεργειακή Βελτιστοποίηση Συστημάτων"

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

"ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΤΑ ISO/IEC 27001:2013 ΣΕ ΥΠΗΡΕΣΙΕΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ"

"INFORMATION SECURITY MANAGEMENT ACCORDING TO ISO / IEC 27001: 2013 IN E-GOVERNANCE SERVICES"

Υπεύθυνος Καθηγητής: Καραϊσάς Πέτρος

Φοιτητής: Δούνιας Σταύρος

Αιγάλεω
Οκτώβριος – 2017

Η σελίδα αυτή σκοπίμως έμεινε κενή

Αιγάλεω
Οκτώβριος – 2017

ΕΥΧΑΡΙΣΤΙΕΣ

Με την περάτωση της εργασίας αυτής, αρχικά θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου Καραϊσά Πέτρο για τις πολύτιμες επιστημονικές συμβουλές του αλλά και για την αποτελεσματική καθοδήγηση του, η οποία ήταν καταλυτικής σημασίας για την εκπόνηση της παρούσας διπλωματικής εργασίας.

Ακόμη, θέλω να ευχαριστήσω ιδιαίτερα, τη σύζυγό μου Ελευθερία και τη κόρη μου Κατερίνα, που με την πολύτιμη συμπαράσταση και υποστήριξη τους, όλο αυτό το διάστημα των σπουδών μου, μου έδιναν δύναμη να συνεχίσω να εκπληρώνω τους στόχους μου.

Σταύρος Δούνιας

Οκτώβριος 2017

ΠΕΡΙΕΧΟΜΕΝΑ

Περιεχόμενα iii
Περιληψη vi
Executive Summary viii
Λίστα Εικόνων 1
Λίστα Πινάκων 2
Πρόλογος 3
ΚΕΦΑΛΑΙΟ 1 5
«ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ» 5
1.1 Ηλεκτρονική Διακυβέρνηση 5
1.2 Ορισμός Ηλεκτρονικής Διακυβέρνησης 6
1.3 Οφέλη της Ηλεκτρονικής διακυβέρνησης 7
1.3.1. Τα οφέλη της Ηλεκτρονικής Διακυβέρνησης για τον δημόσιο τομέα 8
1.3.2. Τα οφέλη της Ηλεκτρονικής Διακυβέρνησης για τον πολίτη 9
1.3.3. Τα οφέλη της Ηλεκτρονικής Διακυβέρνησης για τις επιχειρήσεις 9
1.4 Χαρακτηριστικά υπηρεσιών Ηλεκτρονικής Διακυβέρνησης 9
1.5 Μοντέλα Παροχής Υπηρεσιών 11
1.6 Παράγοντες επιτυχούς μετάβασης στην Ηλεκτρονική Διακυβέρνηση 13
1.7 Τα επίπεδα ανάπτυξης της Ηλεκτρονικής Διακυβέρνησης 14
1.8 Τεχνολογικά ζητήματα Ηλεκτρονικής Διακυβέρνησης 17
1.8.1. Προστασία δεδομένων 18
1.8.2. Πρόσβαση – Αυθεντικοποίηση 19
1.8.3. Διαθεσιμότητα – Απόδοση συστημάτων 21
1.8.4. Διαθεσιμότητα – Απόδοση εξυπηρετητών 21
1.8.5. Αντοχή σε κινδύνους φυσικής ασφάλειας 22
1.8.6. Προσβασιμότητα 23
1.9 Διαλειτουργικότητα 24
1.10 Διαλειτουργικότητα σε Πανευρωπαϊκό επίπεδο 26
1.10.1. Βασική αρχή 1: επικουρικότητα και αναλογικότητα: 28
1.10.2. Βασική αρχή 2: ανοικτός χαρακτήρας 29
1.10.3. Βασική αρχή 3: διαφάνεια 31
1.10.4. Βασική αρχή 4: δυνατότητα επαναχρησιμοποίησης 31
1.10.5. Βασική αρχή 5: τεχνολογική ουδετερότητα και φορητότητα των δεδομένων 32
1.10.6. Βασική αρχή 6: λειτουργία με επίκεντρο τον χρήστη 33
1.10.7. Βασική αρχή 7: ένταξη και προσβασιμότητα 34
1.10.8. Βασική αρχή 8: ασφάλεια και προστασία της ιδιωτικής ζωής 35
1.10.9. Βασική αρχή 9: πολυγλωσσία 35
1.10.10. Βασική αρχή 10: διοικητική απλούστευση 36
1.10.11. Βασική αρχή 11: διατήρηση των πληροφοριών 37
1.10.12. Βασική αρχή 12: αξιολόγηση αποτελεσματικότητας & αποδοτικότητας 37
1.11 Εξέλιξη της Ηλεκτρονικής Διακυβέρνησης παγκοσμίως 38

1.12 Η Ηλεκτρονική Διακυβέρνηση στην Ελλάδα 41
1.13 Εξέλιξη 20 βασικών υπηρεσιών Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα 44
ΚΕΦΑΛΑΙΟ 2 47
«ΘΕΜΑΤΑ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΙΣ ΥΠΗΡΕΣΙΕΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ» 47
2.1 Ιδιωτικότητα πληροφοριών σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης 47
2.2 Απαιτήσεις ασφαλείας και ιδιωτικότητας δεδομένων 49
2.3 Αρχές προστασίας της ιδιωτικότητας 51
2.4 Νομικό πλαίσιο προσωπικών δεδομένων 54
2.4.1. Ευρωπαϊκή Νομοθεσία 54
2.4.2. Ο Νέος Κανονισμός Ε.Ε. 2016/679 για την προστασία των Προσωπικών Δεδομένων 55
2.4.3. Ελληνική Νομοθεσία 57
2.5 Βασικές υποχρεώσεις της Διοίκησης για την διασφάλιση της Ιδιωτικότητας 59
ΚΕΦΑΛΑΙΟ 3 61
«ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ & ΣΥΣΤΗΜΑΤΑ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ» 61
3.1 Εισαγωγή στην ασφάλεια των πληροφοριών 61
3.2 Η ασφάλεια των πληροφοριών είναι μια διαδικασία 63
3.3 Η ασφάλεια είναι ευθύνη όλων 64
3.4 Η ασφάλεια των πληροφοριών περιλαμβάνει μια ανταλλαγή μεταξύ της ασφάλειας και της χρηστικότητας 65
3.5 Η ασφάλεια των πληροφοριών σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης 65
3.6 Εννοιολογική Θεμελίωση. 66
3.7 Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) 68
ΚΕΦΑΛΑΙΟ 4 75
«Η ΟΙΚΟΓΕΝΕΙΑ ΤΩΝ ΠΡΟΤΥΠΩΝ ΤΗΣ ΣΕΙΡΑΣ ISO/IEC 27000» 75
4.1 Εισαγωγή 75
4.2 Γενικά περί προτύπων συστημάτων διαχείρισης ISO 76
4.3 Η ιστορία των προτύπων ασφάλειας πληροφοριών ISO27K 79
4.3.1. Τέλη της δεκαετίας του '80: Ολλανδική Βασιλεία / Εγχειρίδιο Πολιτικής Ασφάλειας Πληροφοριών του ομίλου Shell 79
4.3.2. 1989: Κώδικας Πρακτικής Χρήσης του Υπουργείο Εμπορίου και Βιομηχανίας - Κέντρο Ασφάλειας Εμπορικών Υπολογιστών DTI CCSC (πρώτη δημοσίευση μετά την Shell). 79
4.3.3. 1993: BSI-DISC PD003 - Κώδικας Πρακτικής DTI για τη διαχείριση της ασφάλειας πληροφοριών - πρώτη δημόσια κυκλοφορία. 80
4.3.4. BS7799:1995 – Αρχική Έκδοση ως Βρετανικό Πρότυπο 80
4.3.5. BS 7799 Μέρος 1: 1998 – Μετονομασία 81
4.3.6. BS 7799 Μέρος 1: 1999 – Αναθεώρηση 81
4.3.7. ISO / IEC 17799: 2000 - πρώτη έκδοση ISO / IEC του BS7799-1 81
4.3.8. ISO / IEC 17799:2005 81
4.3.9. ISO/IEC 27002:2005 81
4.3.10. ISO / IEC 27001:2013 και 27002:2013 - νέες εκδόσεις 82
4.4 Η σειρά των προτύπων ISO27K 84
4.5 ISO / IEC 27000: 2016 92
4.5.1. Εισαγωγή και πεδίο εφαρμογής 93

4.5.2. ISMS / ISO27K τμήμα λεξιλογίου 93
4.5.3. ISMS / ISO27K τμήμα επισκόπησης 94
4.6 ISO / IEC 27001:2013 96
4.6.1. Εισαγωγή 96
4.6.2. Δομή του Προτύπου 97
4.6.3. Υποχρεωτικές απαιτήσεις πιστοποίησης 99
4.6.4. Το πεδίο εφαρμογής ΣΔΑΠ - ISMS και Δήλωση Εφαρμοσιμότητας – SoA (Statement of Applicability) 101
4.6.5. Μετρήσεις 102
4.6.6. Γενικά επί της πιστοποίησης 102
4.7 ISO / IEC 27002:2013 104
4.7.1. Εισαγωγή 104
4.7.2. Σκοπός του προτύπου 104
4.7.3. Σχέση μεταξύ του ISO27001 και του ISO27002 105
4.7.4. Δομή και μορφή του προτύπου ISO/IEC 27002:2013 105
4.7.5. Περιεχόμενο του ISO/IEC 27002:2013 106
ΚΕΦΑΛΑΙΟ 5 118
«ΠΑΡΑΔΕΙΓΜΑ ΑΝΑΠΤΥΞΗΣ ΣΔΑΠ ΚΑΤΑ ISO/IEC 27001:2013 ΣΕ ΕΝΑΝ ΟΡΓΑΝΙΣΜΟ» 118
5.1 Ανάπτυξη ΣΔΑΠ σε έναν οργανισμό 118
5.1.1. Φάση 1 (Σχεδιασμός): Θέσπιση του ΣΔΑΠ 118
5.1.2. Φάση 2 (Υλοποίηση): Υλοποίηση και λειτουργία του ΣΔΑΠ 119
5.1.3. Φάση 3 (Έλεγχος): Παρακολούθηση του ΣΔΑΠ 120
5.1.4. Φάση 4 (Διόρθωση): Συντήρηση και βελτίωση του ΣΔΑΠ 121
5.2 Διαδικασίες ανάπτυξης ΣΔΑΠ 121
5.3 Τεκμηρίωση του ΣΔΑΠ 129
5.4 Προκαταρκτική αξιολόγηση και ενέργειες μετά την πιστοποίηση. 130
ΚΕΦΑΛΑΙΟ 6 131
«ΣΥΜΠΕΡΑΣΜΑΤΑ» 131
6.1 Συμπεράσματα 131
ΠΑΡΑΡΤΗΜΑ Ι 134
Βιβλιογραφια 150

ΠΕΡΙΛΗΨΗ

Στα πλαίσια του μεταπτυχιακού προγράμματος σπουδών "Διαχείριση και Ενεργειακή Βελτιστοποίηση Συστημάτων" μιλήσαμε εκτενώς για τα διεθνή πρότυπα συστημάτων διαχείρισης ISO και την σημασία που έχει η εφαρμογή τους σε μια επιχείρηση ή έναν οργανισμό. Σκοπός της παρούσας διπλωματικής είναι η μελέτη του προτύπου ISO/IEC 27001:2013 «Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών – Απαιτήσεις», ενός προτύπου σχετικά καινούργιου όπως φαίνεται από την χρονολογία του αλλά η ιστορία του ξεκινάει από πολύ παλιά, το οποίο όμως γίνεται πολύ επίκαιρο με την εφαρμογή του νέου Γενικού Κανονισμού Προστασίας Δεδομένων (General Data Protection Regulation – GDPR) της Ε.Ε. που θα τεθεί σε πλήρη εφαρμογή από τον Μάιο του 2018. Μέσω της βιβλιογραφικής έρευνας θα επιχειρήσουμε να συλλέξουμε και αναλύσουμε όλα τα δεδομένα για το πως το συγκεκριμένο πρότυπο θα μπορούσε να εφαρμοστεί σε μια υπηρεσία Ηλεκτρονικής Διακυβέρνησης αλλά και γενικότερα στον ευρύτερο Δημόσιο Τομέα.

Η παρούσα διπλωματική απαρτίζεται από 6 κεφάλαια, τα οποία δομούνται ως εξής:

- Στο Κεφάλαιο 1 παρατίθενται οι επίσημοι ορισμοί που έχουν δοθεί για την Ηλεκτρονική Διακυβέρνηση. Στην συνέχεια καταγράφονται τα οφέλη από την εφαρμογή των ηλεκτρονικών υπηρεσιών αλλά και τα τεχνολογικά ζητήματα που προκύπτουν. Επίσης, γίνεται εισαγωγή στην έννοια της Διαλειτουργικότητας και τι ισχύει σε Ευρωπαϊκό επίπεδο ενώ στο τέλος εξετάζεται η εξέλιξη της Ηλεκτρονικής Διακυβέρνησης παγκοσμίως και στην Ελλάδα.

- Στο Κεφάλαιο 2 τίθενται τα θέματα ιδιωτικότητας που προκύπτουν στις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης και η ανάγκη για την διασφάλιση της. Οι αρχές που ισχύουν για την προστασία της ιδιωτικότητας καθώς και το νομικό και κανονιστικό πλαίσιο σε Ευρωπαϊκό και Εθνικό επίπεδο.

- Στο Κεφάλαιο 3 γίνεται εισαγωγή στην έννοια της ασφάλειας των πληροφοριών, την σημασία που έχει η διασφάλιση της πληροφορίας καθώς και στον τρόπο διαχείρισης της. Επίσης γίνεται αναφορά στα Συστήματα

Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) καθώς και στις μεθόδους που υπάρχουν για την ανάπτυξη τους.

- Στο Κεφάλαιο 4 θα προσπαθήσουμε να γνωρίσουμε την οικογένεια των προτύπων της σειράς ISO/IEC 27000 και πως δημιουργήθηκαν μέσω εκτενής βιβλιογραφικής ιστορικής αναδρομής. Στην συνέχεια εξετάζουμε την δομή, το πεδίο εφαρμογής και το περιεχόμενο των κυριότερων προτύπων της σειράς που μας ενδιαφέρουν και συγκεκριμένα των: ISO/IEC 27000:2016, ISO/IEC 27001:2013 και ISO/IEC 27002:2013.

- Στο Κεφάλαιο 5 δίνεται ένα πολύ επιγραμματικό παράδειγμα ανάπτυξης ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) σε έναν οργανισμό και πως κατ' επέκταση θα μπορούσε να εφαρμοστεί σε μια υπηρεσία Ηλεκτρονικής Διακυβέρνησης, ακολουθώντας τα βήματα που μας παρέχει το πρότυπο ISO/IEC 27001:2013 και ISO/IEC 27002:2013.

- Στο Κεφάλαιο 6 διατυπώνονται τα συμπεράσματα της συγκεκριμένης διπλωματικής σχετικά με την ασφάλεια των πληροφοριών, την Ηλεκτρονική Διακυβέρνηση και την δυνατότητα εφαρμογής του προτύπου ISO/IEC 27001:2013 γενικά στην Δημόσια Διοίκηση.

- Τέλος, στο Παράρτημα Ι γίνεται μια προσπάθεια αντιπαραβολής των άρθρων που περιέχει ο νέος Γενικός Κανονισμός Προστασίας Δεδομένων – General Data Protection Regulation της Ε.Ε. με αυτά που εμπεριέχονται στην οικογένεια των προτύπων ISO27K προκειμένου να διαπιστώσουμε την σύγκλιση τους σε πολλά σημεία.

Στο σημείο αυτό, πρέπει να τονισθεί ότι η έκταση του προτύπου είναι πολύ μεγάλη, στην παρούσα διπλωματική εργασία αποτυπώνεται ένα μέρος του και ως εκ τούτου, είναι αδύνατον να αποτυπωθούν όλες οι λεπτομέρειες του σε βάθος. Κύριος σκοπός του παρόντος έργου είναι η αποτύπωση των γενικών αρχών του, η γενικότερη μεθοδολογία που ισχύει για την εφαρμογή του και τα οφέλη εφαρμογής του σ' έναν οργανισμό γενικά.

EXECUTIVE SUMMARY

In the framework of the postgraduate program "Management and Energy Optimization Systems", we have talked extensively about the international standards of ISO management systems and the importance of their application to a company or organization. The purpose of this diploma thesis is to study the standard ISO / IEC 27001: 2013 "Information Security Systems - Requirements". A standard relatively new as seen from its date, but its history starts from the past but it is very timely with the implementation of the new General Data Protection Regulation (GDPR) of the EU, which be fully implemented from May 2018. We will attempt through bibliographic research to collect and analyze all data on how this standard could apply to an eGovernment service and more generally to the wider Public Sector.

This diploma consists of six chapters, which structured as follows:

• Chapter 1 lists the official definitions for eGovernment. The benefits from the implementation of e-services and the technical issues that arise. In addition, we make a general introduction to Interoperability Framework and who is the current European Interoperability Framework. Finally, we examine the evolution of eGovernment worldwide and in Greece.

• Chapter 2 sets out the issues of privacy that arise in eGovernment services and the need to ensure it. Then we examine the principles of privacy protection as well as the legal and regulatory framework at European and national level.

• Chapter 3 introduces the concept of information security, the importance of information security and how is managed. In addition, we make an introduction to Information Security Management Systems (ISMS) and the methods usually used to develop them.

• In Chapter 4, we will try to get to know the family of ISO / IEC 27000 series standards through an extensive bibliographic historical review. In addition, we refer to the structure, scope and content of the main standards of the series: ISO / IEC 27000: 2016, ISO / IEC 27001: 2013 and ISO / IEC 27002: 2013.

• In Chapter 5, we will try to give a very succinct example of developing an Information Security Management System (ISMS) to an organization and an

extension of an eGovernment service, following the steps provided by ISO / IEC 27001: 2013 and ISO / IEC 27002: 2013.

• Chapter 6 sets out the conclusions of this diploma thesis on information security, eGovernment and the applicability of the ISO / IEC 27001: 2013 standard in general to the Public Administration.

• Finally, Annex I attempts a mapping between the articles contained in the new General Data Protection Regulation and those that included in the family of ISO27K standards in order to see their convergence.

At this point, it should stress that the range of the standard is very large, in this diploma thesis only a part of it is imprinted and therefore it is impossible to imprint all the details in depth. The main purpose of this diploma thesis is to outline its general principles, the general methodology for its implementation and the benefits of its application to an organization in general.

Keywords: eGovernance, Information Security, Information Security Management Systems, ISO / IEC 27001: 2013, Interoperability, General Data Protection Regulation

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

ΣΧΗΜΑ 2-1. ΤΟΜΕΙΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ 13

ΣΧΗΜΑ 2-2.ΕΠΙΠΕΔΑ ΩΡΙΜΟΤΗΤΑΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ 17

ΣΧΗΜΑ 2-3.ΔΙΑΣΤΑΣΕΙΣ ΚΑΙ ΕΠΙΠΕΔΑ ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑΣ 26

ΣΧΗΜΑ 2-4.ΑΡΧΕΣ ΕΥΡΩΠΑΪΚΗΣ ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑΣ 28

ΣΧΗΜΑ 2-5.ΔΕΙΚΤΗΣ ΑΝΑΠΤΥΞΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ 20 ΠΡΩΤΩΝ ΧΩΡΩΝ ΠΑΓΚΟΣΜΙΩΣ 40

ΣΧΗΜΑ 2-6.ΔΕΙΚΤΗΣ ΑΝΑΠΤΥΞΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΑΝΑ ΉΠΕΙΡΟ 41

ΣΧΗΜΑ 2.7.ΠΥΛΩΝΕΣ ΑΝΑΠΤΥΞΗΣ ΤΗΣ ΕΘΝΙΚΗΣ ΣΤΡΑΤΗΓΙΚΗΣ ΓΙΑ ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗΣ 44

ΣΧΗΜΑ 3-1. ΟΙ 3 ΑΚΡΟΓΩΝΙΑΙΟΙ ΛΙΘΟΙ ΤΗΣ ΑΣΦΑΛΕΙΑΣ 63

ΣΧΗΜΑ 3-2. ΣΥΣΧΕΤΙΣΕΙΣ ΜΕΤΑΞΥ ΟΡΩΝ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ 66

ΣΧΗΜΑ 3-3. Ο ΚΥΚΛΟΣ ΤΟΥ DEMING 70

ΣΧΗΜΑ 3-4. ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΤΑ ISO/IEC 27001:2005 73

ΣΧΗΜΑ 3-5 ΣΥΓΚΡΙΣΗ ΚΥΚΛΩΝ PCDA ISO/IEC 27001:2005 & ISO/IEC 27001: 2013 74

ΣΧΗΜΑ 4-1.ΙΣΤΟΡΙΚΗ ΕΞΕΛΙΞΗ ΤΟΥ ΠΡΟΤΥΠΟΥ ISO27K 83

ΣΧΗΜΑ 4-2.Η ΟΙΚΟΓΕΝΕΙΑ ΤΩΝ ΠΡΟΤΥΠΩΝ ΣΔΑΠ ΚΑΙ ΟΙ ΣΧΕΣΕΙΣ ΜΕΤΑΞΥ ΤΟΥΣ. 95

ΣΧΗΜΑ 4-3.ΚΑΤΑΝΟΜΗ ΠΡΟΤΥΠΟΥ ISO27001 ΑΝΑ ΤΗΝ ΥΦΗΛΙΟ 2006 -2015 103

ΣΧΗΜΑ 4-4.ΤΟΜΕΙΣ ΤΟΥ ISO27002:2013 107

ΣΧΗΜΑ 5-1 Η ΔΙΑΔΙΚΑΣΙΑ ΑΝΑΠΤΥΞΗΣ ΕΝΟΣ ΣΔΑΠ 122

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

ΠΙΝΑΚΑΣ 1-1.ΒΑΣΙΚΕΣ ΔΗΜΟΣΙΕΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΗΡΕΣΙΕΣ 46

ΠΙΝΑΚΑΣ 2-1.ΕΥΡΩΠΑΪΚΗ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ 55

ΠΙΝΑΚΑΣ 2-2.ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ 58

ΠΙΝΑΚΑΣ 4.1. ΤΑ ΠΡΟΤΥΠΑ ΚΑΙ ΤΑ ΠΡΟΣΧΕΔΙΑ ΤΗΣ ΣΕΙΡΑΣ ISO27K 92

ΠΙΝΑΚΑΣ 5.1 ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΠΑΡΑΡΤΗΜΑ Α΄ ΤΟΥ ISO/IEC 27001 128

ΠΙΝΑΚΑΣ ΠΑΡΑΡΤΗΜΑΤΟΣ Ι ΑΝΤΙΠΑΡΑΒΟΛΗ GDPR ΚΑΙ ISO27001 149

ΠΡΟΛΟΓΟΣ

Το πρόβλημα της διαχείρισης της ασφάλειας πληροφοριών (information security management) αποτελεί ένα ιδιαίτερα σημαντικό ζήτημα όχι μόνο για τα σύγχρονα πληροφοριακά συστήματα, καθώς επηρεάζει σε παγκόσμια κλίμακα το ηλεκτρονικό επιχειρείν και την ανάπτυξη εθνικών και διεθνών κρίσιμων υποδομών αλλά και για την ίδια την επιχείρηση και τον οργανισμό. Η αξιοποίηση όλο και πιο προηγμένων τεχνολογιών, όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων, τα δίκτυα και το Διαδίκτυο, προσφέρει σημαντικές δυνατότητες, αλλά αυξάνει ανάλογα και τα προβλήματα που αφορούν την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.

Η άνοδος της Ηλεκτρονικής Διακυβέρνησης ήταν μία από τις πιο σημαντικές εντυπωσιακές εξελίξεις του παγκόσμιου ιστού. Δεδομένου ότι οι υπηρεσίες Ηλεκτρονικής Διακυβέρνησης στηρίζονται στο Διαδίκτυο, οι ψηφιακές κοινότητες εξελίσσονται και μεγαλώνουν με ταχύτατους ρυθμούς ενσωματώνοντας πολίτες όχι μόνο της ίδιας της χώρας αλλά και απ’ όλο τον κόσμο γεγονός που δημιούργησε στις εθνικές κυβερνήσεις ορισμένες προκλήσεις και ευκαιρίες. Σε μια υπηρεσία Ηλεκτρονικής Διακυβέρνησης, διατηρείται σημαντικός όγκος πληροφορίας όπως π.χ. είναι η τήρηση των αρχείων γης του κτηματολογίου, τα αρχεία της αστυνομίας και ούτω καθεξής. Κάθε τμήμα της υπηρεσίας είναι κρίσιμο, έτσι ώστε μόνο οι εξουσιοδοτημένοι άνθρωποι πρέπει να μπαίνουν στο δίκτυο και να έχουν πρόσβαση στις πληροφορίες. Η κατανόηση της έννοιας της ασφάλειας των πληροφοριών και η ανάγκη για την υλοποίησή της είναι καθοριστικής σημασίας για την ασφαλέστερη και ομαλή λειτουργία μιας υπηρεσίας ηλεκτρονικής διακυβέρνησης (Singh & Karaulia, 2011).

Η ανάγκη λοιπόν για ασφαλή διαχείριση της πληροφορίας, των συστημάτων και των χρηστών, οδήγησε στη δημιουργία προτύπων ασφαλείας τα οποία καθοδηγούν μια επιχείρηση, έναν οργανισμό κ.τ.λ., να εξασφαλίσει ότι τα δεδομένα είναι ασφαλή. Το πρότυπο ISO/IEC 27001:2013 «Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών – Απαιτήσεις» και γενικότερα τα πρότυπα της οικογένειας ISO27K ανήκουν σε αυτή την κατηγορία. Μέσα από την βιβλιογραφική ανασκόπηση και θεωρητική ανάλυση του προτύπου θα προσπαθήσουμε να ερευνήσουμε πως αυτό θα μπορούσε να

εφαρμοστεί στο τομέα της Ηλεκτρονικής Διακυβέρνησης αλλά γενικότερα σ' έναν δημόσιο οργανισμό ή υπηρεσία, όπου η ασφάλεια και διαχείριση των πληροφοριών θεωρείται κρίσιμη.

Λέξεις κλειδιά: Ηλεκτρονική Διακυβέρνηση, ασφάλεια πληροφοριών, Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών, ISO/IEC 27001:2013, Διαλειτουργικότητα, Γενικός Κανονισμός Προστασίας Δεδομένων.

ΚΕΦΑΛΑΙΟ 1

«ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ»

1.1 Ηλεκτρονική Διακυβέρνηση

Η Ηλεκτρονική Διακυβέρνηση είναι γνωστή με διάφορα ονόματα όπως είναι: Ηλεκτρονική Κυβέρνηση (Electronic Government), Ηλεκτρονική Διακυβέρνηση (Electronic Governance), Ψηφιακή Κυβέρνηση (Digital Government), Online Κυβέρνηση, e-Gov κλπ. (Grönlund & Horan, 2005).

Ο όρος χρησιμοποιείται για να περιγράψει τη χρήση και εφαρμογή Τεχνολογιών Πληροφοριών και Επικοινωνιών (ΤΠΕ) σε διαδικασίες και υπηρεσίες της Δημόσιας Διοίκησης. Η χρήση τους δεν μπορεί να θεωρηθεί ως κάτι καινούργιο ή καινοτόμο, καθώς εφαρμόζεται αρκετές δεκαετίες τώρα σε διάφορους επιμέρους τομείς ή διαδικασίες της Δημόσιας Διοίκησης. Ο συγκεκριμένος όρος μπορεί να εμφανίστηκε στα τέλη της δεκαετίας του 1990, αλλά η αλληλεπίδραση προϋπήρχε, σχεδόν από την εμφάνιση των πρώτων Πληροφοριακών Συστημάτων (Grönlund & Horan, 2005; Danziger & Andersen, 2002).

Για να καταλάβει κάποιος την ιδέα της Ηλεκτρονικής Διακυβέρνησης, θα πρέπει πρώτα να έχει καταλάβει την έννοια της Διακυβέρνησης γενικά. Διακυβέρνηση είναι στην πραγματικότητα ένα δυναμικό μίγμα στόχων, δομών και λειτουργιών (Pardo, 2000). Η Ηλεκτρονική Διακυβέρνηση είναι κάτι περισσότερο από μια ιστοσελίδα, ηλεκτρονικό ταχυδρομείο ή εκτέλεση συναλλαγών μέσω του Διαδικτύου, είναι μια φυσική επέκταση της τεχνολογικής επανάστασης που συνοδεύει τη γνώση της κοινωνίας και πρόσθεσε νέες έννοιες όπως: διαφάνεια, ευθύνη, συμμετοχή των πολιτών στην αξιολόγηση της απόδοσης της κυβέρνησης. (Mohammad, Almarabeh, & Ali, 2009)

Ένα πρόγραμμα Ηλεκτρονικής Διακυβέρνησης επιδιώκει να επιτύχει μεγαλύτερη αποτελεσματικότητα των κυβερνητικών επιδόσεων, μέσου της αύξησης της απόδοσης

των υπηρεσιών για τους δικαιούχους και τους επενδυτές από όλα τα τμήματα της κοινωνίας εύκολα, με ακρίβεια και αποτελεσματικότητα και να γίνει ένας νέος τύπος εκτέλεσης των επίσημων κυβερνητικών συναλλαγών. Οι διαδραστικές διαδικτυακές υπηρεσίες μπορούν να περιλαμβάνουν υπηρεσίες όπως είναι υποβολής αιτημάτων, καταβολής πληρωμών, χορήγηση αδειών ή ερωτήσεις πληροφοριών (Almarabeh & AbuAli, 2010; Middleton, 2007).

1.2 Ορισμός Ηλεκτρονικής Διακυβέρνησης

Στην πραγματικότητα, υπάρχουν πολλοί ορισμοί για τον όρο Ηλεκτρονική Διακυβέρνηση και οι διαφορές τους αντικατοπτρίζουν τις προτεραιότητες στις κυβερνητικές στρατηγικές (Field, 2003), κάποιοι από αυτούς παραθέτονται παρακάτω:

- Ηλεκτρονική Διακυβέρνηση είναι η εφαρμογή των εργαλείων και των τεχνικών του ηλεκτρονικού εμπορίου στο έργο της κυβέρνησης με σκοπό να εξυπηρετήσουν τόσο την ίδια όσο και τους πολίτες της (Howard, 2001).

- Ευρωπαϊκή Επιτροπή: «Ηλεκτρονική Διακυβέρνηση ορίζεται η χρήση των τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ) στις δημόσιες διοικήσεις, σε συνδυασμό με οργανωτικές αλλαγές, νέες διοικητικές πρακτικές και νέες δεξιότητες του προσωπικού. Σκοπός, είναι η βελτίωση των δημόσιων υπηρεσιών, καθώς και η ενίσχυση των δημοκρατικών διαδικασιών και των διαδικασιών στήριξης των δημόσιων πολιτικών». (EUR-Lex, 2017)

- Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ): «Ηλεκτρονική Διακυβέρνηση είναι η χρήση των τεχνολογιών της πληροφορίας και των τηλεπικοινωνιών, ειδικά του Διαδικτύου ως εργαλείο για καλύτερη Διακυβέρνηση» (Field, 2003).

- Παγκόσμια Τράπεζα: «Η ηλεκτρονική διακυβέρνηση αφορά τη χρήση τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ) από κυβερνητικούς φορείς, οι οποίες έχουν τη δυνατότητα να μεταμορφώσουν τις σχέσεις των

φορέων αυτών με τους πολίτες, τις επιχειρήσεις και άλλους τομείς του κράτους» (The World Bank, 2001).

Το κοινό στοιχείο όλων αυτών των ορισμών είναι η χρήση τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ) για την επανεξέταση του δημόσιου τομέα με τη μετατροπή του εσωτερικού και του εξωτερικού τρόπου διεξαγωγής των πράξεων και των σχέσεων του με τους πελάτες και την επιχειρηματική κοινότητα. Η ανάλυση αυτών των ορισμών μας επιτρέπει να αναφέρουμε τα βασικά ζητήματα και τα συστατικά που χαρακτηρίζουν το πλαίσιο της Ηλεκτρονικής Διακυβέρνησης, όπως:

- Περιοχές μετασχηματισμού (εσωτερική, εξωτερική, σχεσιακή).
- Χρήστες, πελάτες, και οι αλληλεπιδράσεις τους (πολίτες, επιχειρήσεις, κυβερνητικές οργανώσεις, εργαζόμενοι).
- Τομείς εφαρμογών ηλεκτρονικής διακυβέρνησης (ηλεκτρονικές υπηρεσίες, ηλεκτρονική δημοκρατία, ηλεκτρονική διοίκηση). (Ndou, 2004).

Εν κατακλείδι είναι αρκετά δύσκολο να δοθεί ένας ξεκάθαρος και πλήρης ορισμός για την ηλεκτρονική διακυβέρνηση, καθώς πρόκειται για μια πολυδιάστατη έννοια, η οποία εμπερικλείει πολλές αλληλοεξαρτώμενες συνιστώσες – κοινωνικές, πολιτικές, διοικητικές, τεχνολογικές, οικονομικές, νομικές. Το βασικότερο σημείο που πρέπει να γίνει αντιληπτό είναι ότι η ηλεκτρονική διακυβέρνηση αφορά την συθέμελη αναδιαμόρφωση του τρόπου λειτουργίας της κυβέρνησης και της διακυβέρνησης σε παρόμοια κλίμακα με αυτή της βιομηχανικής επανάστασης (Γιαννουκάκου, 2011).

1.3 Οφέλη της Ηλεκτρονικής διακυβέρνησης

Η Ηλεκτρονική Διακυβέρνηση στοχεύει στην βελτίωση της Δημόσιας Διοίκησης εκτός όμως από το ευρύτερο δημόσιο τομέα η εφαρμογή της έχει πολλαπλά οφέλη και στους πολίτες και τις επιχειρήσεις. Ειδικότερα, στοχεύει στο να εφαρμόσει συστήματα που θα επιτρέπουν στο σύνολο του πληθυσμού ακόμη και σε ηλικιωμένα άτομα, άτομα με αναπηρίες ή ομάδες πληθυσμού που κατοικούν σε δυσπρόσιτες περιοχές, να έχουν εύκολη πρόσβαση στις υπηρεσίες της κοινωνίας της πληροφορίας.

Σε γενικές γραμμές τα προσδοκώμενα οφέλη είναι τα εξής (Κιοσσέ, 2011; Παπαδάκης, Μαυροειδής, & Ρηγοπούλου, 2012):

Μείωση του κόστους των δημοσίων υπηρεσιών.

1. Βελτίωση της ποιότητας των παρεχόμενων υπηρεσιών.
2. Η αναδιοργάνωση και ο εξορθολογισμός των διεργασιών της δημόσιας διοίκησης.
3. Αύξηση της αποδοτικότητας και της αποτελεσματικότητας των δημοσίων υπηρεσιών.
4. Η ελάττωση της άμεσης επαφής των πολιτών με τις δημόσιες υπηρεσίες.
5. Μείωση του χρόνου διεκπεραίωση των διαδικασιών και επέκταση της διαθεσιμότητας των δημόσιων υπηρεσιών (24 ώρες την ημέρα – 7 ημέρες την εβδομάδα).
6. Συμμετοχή του κοινωνικού συνόλου στην διαμόρφωση των δημοσίων πολιτικών.
7. Η δυνατότητα ελέγχου και απόδοσης ευθυνών στη δημόσια διοίκηση.

Τα παραπάνω οφέλη θα μπορούσαμε να τα κατηγοριοποιήσουμε ανάλογα τον αποδέκτη:

1.3.1. Τα οφέλη της Ηλεκτρονικής Διακυβέρνησης για τον δημόσιο τομέα

Η ανάπτυξη υπηρεσιών ηλεκτρονικής διακυβέρνησης (e-government) επιτρέπει την αποδοτικότερη αλληλεπίδραση μεταξύ δημόσιων υπηρεσιών και πολιτών, μέσω αυτοματοποιημένων διαδικασιών. Με τον τρόπο αυτό μπορούν να βελτιωθούν και να απλοποιηθούν σημαντικά οι παρεχόμενες υπηρεσίες του κράτους προς τους πολίτες και τις επιχειρήσεις. Επίσης, με την εξασφάλιση των κατάλληλων υποδομών παρέχεται η δυνατότητα αξιοποίησης νέων εφαρμογών και υπηρεσιών, γεγονός που έχει θετικές επιδράσεις στις εκπαιδευτικές και ερευνητικές δραστηριότητες. Οι εφαρμογές της ΗΔ στον δημόσιο τομέα θα επιφέρει δραστική μείωση του κόστους των παρεχόμενων υπηρεσιών στους

πολίτες σε σχέση με παλαιότερες διαδικασίες συναλλαγής, καθώς η άντληση και επεξεργασία πληροφοριών και δεδομένων από φορείς δημόσιας διοίκησης μέσα από τη χρήση κοινών πηγών θα γίνεται σε μικρότερο χρονικό διάστημα. Έτσι αυξάνεται η αποδοτικότητα και η αποτελεσματικότητα του δημόσιου λειτουργού, η οποία προκύπτει από την εξοικονόμηση χρόνου.

1.3.2. Τα οφέλη της Ηλεκτρονικής Διακυβέρνησης για τον πολίτη

Το κυριότερο όφελος για τον πολίτη από την εφαρμογή της Ηλεκτρονικής Διακυβέρνησης είναι η ποιοτικότερη παροχή ηλεκτρονικών υπηρεσιών από το κράτος και τις επιχειρήσεις. Τα οφέλη για τον πολίτη είναι η δυνατότητα πρόσβασης του στις υπηρεσίες 24 ώρες καθημερινά, η χρήση προσυμπληρωμένων φορμών μειώνει τόσο το χρόνο συναλλαγής όσο και το χρόνο που πρέπει να διαθέσουν για τη διεκπεραίωση των υποθέσεων του, η μείωση του κόστους συναλλαγής καθώς δεν απαιτείται φυσική παρουσία, καλύτερη, γρηγορότερη και πιο πλήρη εξυπηρέτηση. Τέλος, μπορεί να γίνει άμεσος έλεγχος από τον πολίτη για όποια διαδικασία συναλλαγής έχει αλλά και τη μείωση της γραφειοκρατίας.

1.3.3. Τα οφέλη της Ηλεκτρονικής Διακυβέρνησης για τις επιχειρήσεις

Οι επιχειρήσεις εξοικονομούν χρόνο και μειώνουν το κόστος λειτουργίας τους χρησιμοποιώντας τις ηλεκτρονικές υπηρεσίες για την διεκπεραίωση των περισσότερων συναλλαγών τους με το δημόσιο, όπως εγγραφές σε διάφορους δημόσιους τομείς (έναρξη και λήξη εργασιών), λήψη διάφορων πιστοποιητικών από δημόσιους φορείς (ασφαλιστική – φορολογική ενημερότητα), υποβολή δηλώσεων (Φ.Π.Α., Α.Π.Δ.) αλλά και πληρωμές. Έτσι επιτυγχάνεται η μείωση του λειτουργικού τους κόστους, απαραίτητο για τη βιωσιμότητα τους αλλά και τη μείωση της γραφειοκρατίας.

1.4 Χαρακτηριστικά υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Σύμφωνα με το άρθρο 4 της κοινοτικής οδηγίας 2006/123/ΕΚ (Ευρωπαϊκό Κοινοβούλιο, 2006) δίνονται οι εξής ορισμοί:

- Ο όρος *Υπηρεσία* αναφέρεται στην παροχή ενός συγκεκριμένου αποτελέσματος που επιθυμεί να λάβει ένας πολίτης ή μία επιχείρηση από έναν οργανισμό του Δημόσιου Τομέα.

- Η ολοκλήρωση μίας Υπηρεσίας συνίσταται στην εκτέλεση των *Διαδικασιών* (ή βημάτων) που απαιτούνται γι' αυτή.

- Οι *Αιτούντες/ Αποδέκτες* μπορεί να είναι φυσικά ή νομικά πρόσωπα, δηλαδή απλοί πολίτες ή επιχειρήσεις, οργανισμοί, ιδρύματα, κλπ. Στις περισσότερες περιπτώσεις, μπορεί να είναι και εξουσιοδοτημένοι εκπρόσωποι.

- Οι *Φορείς της Δημόσιας Διοίκησης* παρέχουν Υπηρεσίες προς τους Αιτούντες/ Αποδέκτες. Ο όρος Φορέας αναφέρεται στο οργανωτικό τμήμα του Δημοσίου που είναι αρμόδιο και υπεύθυνο για την παροχή μίας συγκεκριμένης υπηρεσίας.

- Ο *Αρμόδιος Φορέας* για την εκτέλεση μίας υπηρεσίας μπορεί να ορίζεται μονοσήμαντα από τη φύση και τα στοιχεία μίας υπηρεσίας, ή να είναι ευέλικτα γενικός (π.χ. οποιοδήποτε Αστυνομικό Τμήμα) και να προσδιορίζεται από τα στοιχεία του αιτούντος και της υπηρεσίας.

- Το *σημείο επαφής* για την παροχή μίας υπηρεσίας δεν ταυτίζεται απαραίτητα με τον Αρμόδιο Φορέα εκτέλεσης μίας υπηρεσίας. Πρόκειται για μία γενικότερη έννοια, η οποία αφορά στον προσδιορισμό του σημείου για την υποβολή του αιτήματός του ή/και την παραλαβή του αποτελέσματος. Για παράδειγμα, η αίτηση για έκδοση πιστοποιητικού στρατολογικής κατάστασης μπορεί να υποβάλλεται σε οποιοδήποτε ΚΕΠ, αλλά Αρμόδιος Φορέας έκδοσής του είναι το αντίστοιχο Στρατολογικό Γραφείο του Υπουργείου Εθνικής Αμύνης.

Σύμφωνα με τα πορίσματα της ομάδας εργασίας ΣΤ-5 (Διακονικολάου & Μυλωνόπουλος, 2004) «E-business Forum» σχετικά με «Το παρόν και το μέλλον των Ηλεκτρονικών Υπηρεσιών του Κράτους προς τις Επιχειρήσεις (Government to Business) στην Ελλάδα» μία τυπική υπηρεσία διακυβέρνησης έχει τα ακόλουθα χαρακτηριστικά, τα οποία και τη διαφοροποιούν από μία διαδικασία, διεργασία ή απλά μία εργασία ενός φορέα:

i. *Έχει χρήστη:* Ο χρήστης μπορεί να είναι ο πολίτης, η επιχείρηση ή άλλος φορέας της Δημόσιας Διοίκησης. Κατ' εξαίρεση, για πολύπλοκες υπηρεσίες και δομές, προσεγγίζονται ως χρήστες άλλες υπηρεσιακές μονάδες ή στελέχη του ιδίου Φορέα.

ii. *Έχει παραδοτέο:* Το παραδοτέο πρέπει να είναι αυτοτελές. Ο χρήστης που το παραλαμβάνει μπορεί να το αξιοποιήσει χωρίς να απαιτούνται επιπλέον εργασίες, συναλλαγές ή παραδοτέα.

iii. *Έχει πάροχο:* Μία Υπηρεσιακή Μονάδα ενός Φορέα της Δημόσιας Διοίκησης παρέχει την υπηρεσία (π.χ. Διεύθυνση Υπουργείου, Νομαρχιακή Αυτοδιοίκηση ή ΚΕΠ).

iv. *Έχει ρυθμιστή:* Υπάρχει τουλάχιστον μια Υπηρεσιακή Μονάδα ενός Φορέα της Δημόσιας Διοίκησης που είναι αρμόδια για το ρυθμιστικό πλαίσιο της υπηρεσίας.

1.5 Μοντέλα Παροχής Υπηρεσιών

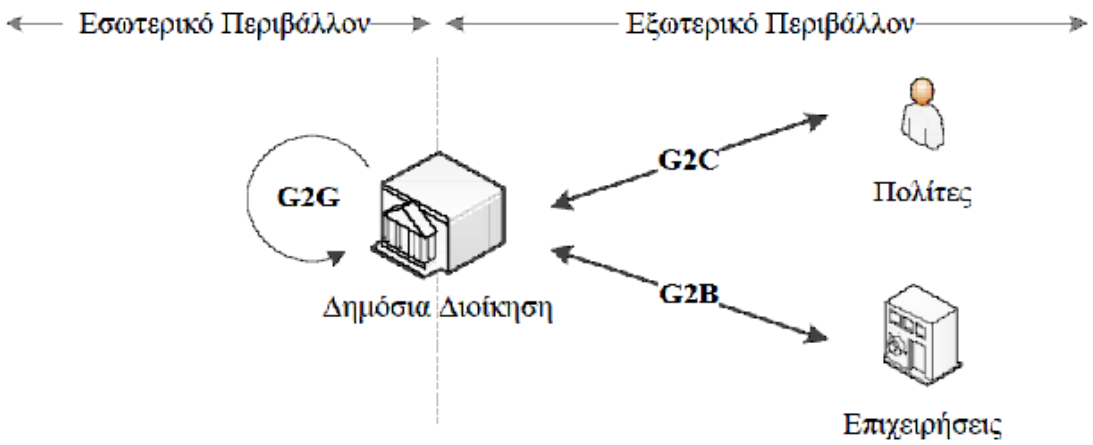
Στη διεθνή βιβλιογραφία αναγνωρίζονται τρία (3) βασικά μοντέλα σχέσεων στην Ηλεκτρονική Διακυβέρνησης που κατηγοριοποιούνται ανάλογα με τον δέκτη της αλληλεπίδρασης και επικοινωνίας που στέκεται απέναντι από την κρατική δομή. Παρόλα αυτά σε όλα τα μοντέλα σχέσεων ο απώτερος σκοπός είναι ο ίδιος, δηλαδή η μείωση των επαναλαμβανόμενων διοικητικών λειτουργιών και η βελτιστοποίηση της επικοινωνίας τόσο εσωτερικά ανάμεσα στις κρατικές υπηρεσίες αυτές καθαυτές όσο και στις σχέσεις με τις επιχειρήσεις και τους πολίτες (Seifert & Petersen, 2002) :

- ***Κυβέρνηση-προς-κυβέρνηση (Government-to-Government – G2G):*** αναφέρεται στην εσωτερική επικοινωνία των κρατικών υπηρεσιών και την ενδοϋπηρεσιακή συνεργασία, που είναι και το σημείο αναφοράς και ο απώτερος στόχος της ηλεκτρονικής διακυβέρνησης. Κύριο μέλημα του μοντέλου αυτού είναι ο ανασχεδιασμός των οργανωτικών δομών και διαδικασιών με τη μεταστροφή από την ιεραρχική υπηρεσιο-κεντρική δημόσια διοίκηση στην εναλλακτική οριζόντια και πελατοκεντρική.

- ***Κυβέρνηση-προς-πολίτη (Government-to-Citizen – G2C):*** αναφέρεται στον εκσυγχρονισμό της επικοινωνίας και συναλλαγής των επιχειρήσεων με τις κρατικές υπηρεσίες. Υπάρχουν δύο μεγάλες κατηγορίες υπηρεσιών που εμπίπτουν σε αυτή την κατηγορία, από τη μια μεριά είναι οι ηλεκτρονικές προμήθειες (e-procurement) που αφορούν την κατάθεση προσφορών για τη σύναψη εμπορικών συναλλαγών με δημόσιες υπηρεσίες ηλεκτρονικά επιφέροντας μείωση κόστους και διαφάνεια των ενεργειών και από την άλλη υπηρεσίες που διευκολύνουν τις συναλλαγές των επιχειρήσεων με το κράτος επιφέροντας αύξηση της παραγωγικότητας και της ανάπτυξης, όπως για παράδειγμα η ηλεκτρονική υποβολή ΦΠΑ και η online παροχή φορολογικής ενημερότητας.

- ***Κυβέρνηση-προς-Πολίτες (Government-to-Citizen – G2C):*** είναι η άμεση εξαγγελία της ηλεκτρονικής διακυβέρνησης και αυτή που οι εφαρμογές της φέρνουν τα πιο ορατά και άμεσα αποτελέσματα. Στόχος είναι η διάθεση στον πολίτη απλοποιημένων υπηρεσιών που να διευκολύνουν τη συνδιαλλαγή του με τις κρατικές δομές, οι οποίες θα είναι υπηρεσιακά ανεξάρτητες και δεν θα αντικατοπτρίζουν το οργανόγραμμα της κρατικής δομής, ενώ ταυτόχρονα θα μειώνουν τον χρόνο διεκπεραίωσης και θα ενισχύουν την προσβασιμότητα των πολιτών σε πληροφορίες και υπηρεσίες. Το πετυχημένο μοντέλο G2C, επίσης, ενδυναμώνει την εμπιστοσύνη του πολίτη προς την κυβέρνηση και τις δομές της ενθαρρύνοντας την ενεργή συμμετοχή στα κοινά μέσω περισσότερο ανοικτών και διαφανών διαδικασιών ανοίγοντας έτσι το δρόμο προς την υλοποίηση της ηλεκτρονικής δημοκρατίας.

Από τους παραπάνω τομείς οι G2B και G2C αποτελούν το «Εξωτερικό Περιβάλλον Ηλεκτρονικής Διακυβέρνησης» (external e-Government), ενώ ο G2G το «Εσωτερικό Περιβάλλον Ηλεκτρονικής Διακυβέρνησης» (internal e - Government). Σε κάποιες περιπτώσεις χρησιμοποιείται και ένας ακόμη διαχωρισμός στο εσωτερικό περιβάλλον, ο οποίος αναφέρεται στις αλληλεπιδράσεις της Δημόσιας Διοίκησης με Δημόσιους Φορείς, αλλά άλλων κρατών (Δημόσια Διοίκηση Κράτους – Δημόσια Διοίκηση Κράτους, Administration to Administration – A2A). Στο Σχήμα 2-1 απεικονίζονται αυτοί οι τομείς.



ΣΧΗΜΑ 2-1. ΤΟΜΕΙΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

(Πηγή: (Δρογκάρης, 2013))

Επίσης κάποιος θα συναντήσει στην διεθνή βιβλιογραφία ότι πολλοί ερευνητές αναγνωρίζουν κάποια επιπλέον σχεσιακά μοντέλα όπως Πολίτης-προς-Κυβέρνηση (Citizen-to-Government – C2G), Επιχείρηση-προς-Κυβέρνηση (Business-to-Government – B2G), Κυβέρνηση-προς-Μη Κερδοσκοπικούς Οργανισμούς (Government-to-NonProfit – G2N), Μη Κυβερνητικοί Οργανισμοί-προς- Κυβέρνηση (NonProfit-to-Government – N2G) και Κυβέρνηση-προς-Υπάλληλο (Government-to-Employee – G2E). Πέραν του τελευταίου μοντέλου G2E που κερδίζει έδαφος στις μελέτες και την αρθρογραφία, επί του παρόντος για τα υπόλοιπα 4 θεωρείται πρώιμη η επισημοποίησή τους, καθώς αφενός θεωρείται ότι εμπίπτουν στις αναφερθείσες κατηγορίες και αφετέρου γιατί παγκοσμίως η έμφαση δίνεται στην ανάπτυξη και εφαρμογή υπηρεσιών για G2G, G2B και G2C (Γιαννουκάκου, 2011).

1.6 Παράγοντες επιτυχούς μετάβασης στην Ηλεκτρονική Διακυβέρνηση

Για την επιτυχή μετάβαση σε ένα μοντέλο ηλεκτρονικής διακυβέρνησης, πρέπει να συντρέχουν οι εξής τέσσερις καθοριστικές προϋποθέσεις (Παρασκευάς, Ασημακόπουλος, & Τριανταφύλλου, 2015):

1. Η ύπαρξη καλά οργανωμένων διαδικασιών από αυτόν που θα παρέχει την ηλεκτρονική υπηρεσία (κεντρικό κράτος, αυτοδιοίκηση, οργανισμοί κ.ά.).

Όπως σημειώνεται στη βιβλιογραφία και διαπιστώνεται από έρευνες, η εισαγωγή και η χρήση των νέων τεχνολογιών σε οργανισμούς με καλή εσωτερική οργάνωση και δομή βελτίωσαν τη λειτουργία τους, ενώ σε οργανισμούς χωρίς καλή εσωτερική οργάνωση και δομή έφερα τα αντίθετα αποτελέσματα.

2. Το άρτια εκπαιδευμένο προσωπικό, το οποίο θα κληθεί να χειριστεί τα εσωτερικά (BackOffice) πληροφοριακά συστήματα που θα διαχειριστούν και θα εξυπηρετήσουν τα αιτήματα των πολιτών. Η εκπαίδευση του προσωπικού δεν είναι πάντα εύκολη υπόθεση, καθώς τις περισσότερες φορές χρειάζεται να δημιουργηθούν και άλλες ευνοϊκές συνθήκες, όπως κίνητρα για την αποδοχή των νέων τεχνολογιών από την πλευρά του προσωπικού.

3. Η χρήση ώριμων τεχνολογιών, υψηλών και ανοιχτών προδιαγραφών και προτύπων, οι οποίες θα εξασφαλίζουν τη διαλειτουργικότητα (Interoperability) ανάμεσα στα πληροφοριακά συστήματα και την επαναχρησιμοποίησή τους (Reusability).

4. Οι ψηφιακά εγγράμματοι πολίτες, δηλαδή οι πολίτες που θα μπορούν να χρησιμοποιούν τις νέες τεχνολογίες επικοινωνίας.

Σημείο-κλειδί για την επιτυχία αποτελεί η λειτουργική ενοποίηση του backoffice, δηλαδή του συνόλου των εσωτερικών πληροφοριακών συστημάτων (π.χ. δικτυακών, υπολογιστικών υποδομών και συσκευών πρόσβασης).

1.7 Τα επίπεδα ανάπτυξης της Ηλεκτρονικής Διακυβέρνησης

Όπως είδαμε παραπάνω για την εφαρμογή, ανάπτυξη και επιτυχία της Ηλεκτρονικής Διακυβέρνησης είναι απαραίτητος ο σωστός σχεδιασμός. Για την επίτευξη όμως μιας πλήρως ολοκληρωμένης συνεργασίας μεταξύ όλων των δημοσίων οργανισμών είναι απαραίτητο η εφαρμογή των ηλεκτρονικών υπηρεσιών να ακολουθήσει ορισμένα κύρια στάδια με διαφορετικά επίπεδα δυσκολίας και πληρότητας. Τα στάδια αυτά είναι μια μέθοδος για την αξιολόγηση του επιπέδου ανάπτυξης της Ηλεκτρονικής Διακυβέρνησης (Πετροπούλου, 2015).

Μια πληθώρα μοντέλων έχουν αναπτυχθεί, προταθεί και υιοθετηθεί από διεθνείς φορείς (European Commission, United Nations, Worldbank) και μεμονωμένους ερευνητές (Andersen and Henriksen, 2006; Klievink and Janssen, 2009; Layne and Lee, 2001; Lee, 2010; Moon, 2002; Siau and Long, 2005) με στόχο την καλύτερη μελέτη και εκτίμηση της ανάπτυξης ενός δημόσιου φορέα ειδικότερα και του δημόσιου τομέα συνολικότερα όσον αφορά την ηλεκτρονική διακυβέρνηση (Καλογήρου, Παναγιωτόπουλος, Τσακανίκας, & Σιώκας, 2015).

Σύμφωνα με την αναφορά των Ηνωμένων Εθνών τα στάδια-επίπεδα εξέλιξης που προτείνονται για την Ηλεκτρονική Διακυβέρνηση είναι 5 (Ronaghan, 2002). Τα επίπεδα ωριμότητας της ηλεκτρονικής διακυβέρνησης κλιμακώνονται, από την «απλή πληροφόρηση», επίπεδο στο οποίο ο πολίτης χρησιμοποιεί το διαδίκτυο προκειμένου να ενημερωθεί για τις δραστηριότητες των υπηρεσιών του κράτους ή των Οργανισμών Τοπικής Αυτοδιοίκησης (ΟΤΑ), έως τις «ηλεκτρονικές συναλλαγές», επίπεδο στο οποίο όλες οι φάσεις για την ολοκλήρωση μιας εργασίας πραγματοποιούνται ηλεκτρονικά. Αναλυτικότερα, τα επίπεδα ωριμότητας των υπηρεσιών της ηλεκτρονικής διακυβέρνησης είναι τα εξής:

- **Επίπεδο 1 : Πληροφόρηση (Emerging Presence)**. Στο επίπεδο αυτό, της ηλεκτρονικής πληροφόρησης για τις παρεχόμενες υπηρεσίες και τον τρόπο διεκπεραίωσης μιας υπηρεσίας από μια υπηρεσία της κεντρικής ή της γενικής κυβέρνησης, ο πολίτης λαμβάνει πληροφορίες σχετικά με τα δικαιολογητικά που πρέπει να προσκομίσει, τους εμπλεκόμενους φορείς στην ολοκλήρωση της υπηρεσίας που επιθυμεί να λάβει, τη σειρά εκτέλεσης των συναλλαγών που περιλαμβάνει η υπηρεσία κτλ.

- **Επίπεδο 2 : Αλληλεπίδραση (Enhanced Presence)**. Στο επίπεδο αυτό, της λήψης εντύπων, ο πολίτης λαμβάνει πληροφοριακό υλικό για τον τρόπο διεκπεραίωσης μιας υπηρεσίας, καθώς και επίσημο υλικό (πρότυπα αιτήσεων, βεβαιώσεων κτλ.), το οποίο μπορεί να κατεβάσει στον υπολογιστή του, να το τυπώσει και να το χρησιμοποιήσει κατά τη συναλλαγή του με τον δημόσιο φορέα.

- **Επίπεδο 3: Αμφίδρομη αλληλεπίδραση (Interactive Presence)**. Στο επίπεδο αυτό, της επεξεργασίας εντύπων για την ταυτοποίησή του, ο πολίτης λαμβάνει

όλες τις παραπάνω υπηρεσίες, αλλά και ηλεκτρονικές (*Online*) φόρμες, για συμπλήρωση και ηλεκτρονική αποστολή τους μέσω του συστήματος, καθώς και μηχανισμούς για την ταυτοποίησή του και την προστασία των δεδομένων που αυτός αποστέλλει.

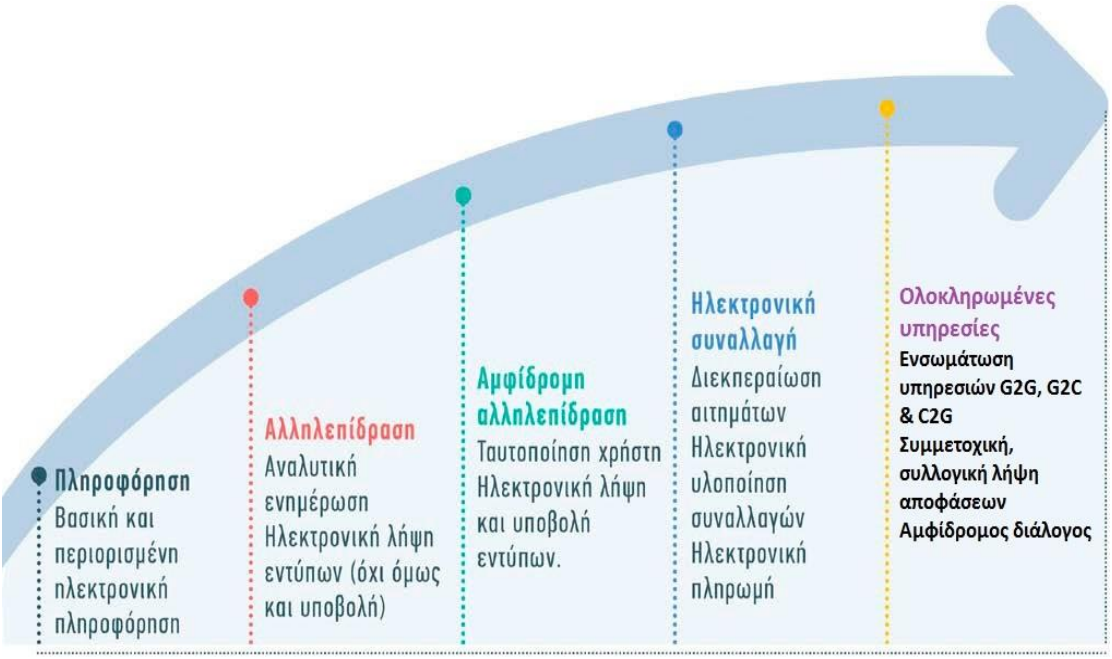
- **Επίπεδο 4: Ηλεκτρονική συναλλαγή (Transactional Presence)**. Στο επίπεδο αυτό, της διεκπεραίωσης αιτημάτων, της υλοποίησης συναλλαγών και της πληρωμής, ο πολίτης λαμβάνει όλες τις παραπάνω υπηρεσίες, αλλά και αυτές με τις οποίες θα μπορεί να χειρίζεται πλήρως την αντίστοιχη μη ηλεκτρονική υπηρεσία. Αυτό έχει αποτέλεσμα η μη ηλεκτρονική υπηρεσία να υποκαθίσταται πλήρως και ισοδύναμα από την αντίστοιχη ηλεκτρονική.

- **Επίπεδο 5: Ολοκληρωμένες υπηρεσίες (Networked Presence)**. Το επίπεδο αυτό διαφέρει από τα προηγούμενα τρία στο γεγονός ότι αφορά την παροχή ηλεκτρονικών υπηρεσιών, στις οποίες εμπλέκονται περισσότεροι από ένας δημόσιοι φορείς-οργανισμοί. Οι δημόσιοι οργανισμοί, δηλαδή, επιτυγχάνουν τέτοιο βαθμό διασύνδεσης, επικοινωνίας, συνεργασίας και συντονισμού που τους επιτρέπει να ανταλλάσσουν με αποτελεσματικό τρόπο δεδομένα και πληροφορίες, και να ενορχηστρώνουν τις διαδικασίες τους ώστε να είναι σε θέση να παρέχουν ολοκληρωμένες αλλά και εξατομικευμένες υπηρεσίες στους πολίτες και επιχειρήσεις. Ενδεικτικά, όταν ένας πολίτης επιθυμεί να του παρασχεθεί μια υπηρεσία από έναν συγκεκριμένο δημόσιο φορέα, η οποία απαιτεί την υποβολή και δικαιολογητικών που δίνονται από άλλους φορείς, τότε αυτό το επίπεδο ηλεκτρονικής διακυβέρνησης συνεπάγεται ότι ο πολίτης δεν είναι αναγκασμένος να μετακινείται από φορέα σε φορέα (ή/και από διεύθυνση σε διεύθυνση στο εσωτερικό ενός φορέα) για να λάβει τα απαραίτητα δικαιολογητικά αλλά αυτά αναλαμβάνει να τα αναζητήσει ο ίδιος ο φορέας, ο οποίος θα του παράσχει την τελική υπηρεσία.

Το κράτος, δηλαδή, απαντά ολοκληρωμένα σε μια συγκεκριμένη ανάγκη του χρήστη βελτιώνοντας ουσιαστικά την εξυπηρέτησή του, και αποκομίζοντας και το ίδιο ένα σημαντικό συνολικό όφελος παραγωγικότητας. Η ολοκλήρωση των σχέσεων των διαφορετικών οντοτήτων του κράτους είναι τόσο κάθετη, δηλαδή αφορά φορείς διαφορετικών κυβερνητικών επιπέδων (δήμοι, περιφέρειες, κεντρικό κράτος) όσο και οριζόντια, δηλαδή αφορά διαφορετικές λειτουργίες του κράτους υγεία, παιδεία,

ασφάλιση, φορολογικοί μηχανισμοί κ.ά.). Επιπρόσθετα, αναφέρουμε ότι ένα εξελιγμένο στάδιο αυτού του επιπέδου ηλεκτρονικής διακυβέρνησης αποτελεί ο συντονισμός και η συνεργασία μεταξύ δημόσιων οργανισμών διαφορετικών χωρών (π.χ. χωρών της ΕΕ) για την παροχή ενοποιημένων υπηρεσιών σε έναν πολίτη μιας χώρας που ζει και εργάζεται σε μια άλλη χώρα) (Καλογήρου και συν., 2015).

Στο Σχήμα 2-2 βλέπουμε τα επίπεδα ωριμότητας της Ηλεκτρονικής Διακυβέρνησης. Τα επίπεδα 1 και 2 αφορούν το στάδιο της δημοσίευσης πληροφορίας, το επίπεδο 3 το στάδιο αλληλεπίδρασης και τα επίπεδα 4 και 5 το στάδιο συναλλαγής του πολίτη με τον δημόσιο τομέα.



ΣΧΗΜΑ 2-2.ΕΠΙΠΕΔΑ ΩΡΙΜΟΤΗΤΑΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

(Πηγή: http://www.tkgweb.com/blog/wp-content/uploads/2012/06/5-Stages-of-e-Government2.jpg)

1.8 Τεχνολογικά ζητήματα Ηλεκτρονικής Διακυβέρνησης

Οι φορείς της Δημόσιας Διοίκησης κατά τον σχεδιασμό των Δημόσιων Διαδικτυακών Τόπων (ΔΔΤ) χρειάζεται να επικεντρωθούν σε δύο τεχνολογικά ζητήματα που είναι πολύ σημαντικά και τα οποία έχουν να κάνουν: α) με την διαλειτουργικότητα των ΔΔΤ και β) την αυθεντικοποίηση – προστασία των δεδομένων των χρηστών. Τα δύο αυτά ζητήματα αφορούν την γρήγορη εξυπηρέτηση,

αλλά και το αίσθημα εμπιστοσύνης και ασφαλείας, που πρέπει να αισθάνεται ο χρήστης του διαδικτυακού τόπου (Tsoumas, 2007).

Εκτός από τα παραπάνω ζητήματα για να θεωρηθεί ένας ΔΔΤ αξιόπιστος θα πρέπει να είναι πάντα διαθέσιμος, γεγονός που εξασφαλίζεται σε επίπεδο τεχνολογικών υποδομών από διάφορες παραμέτρους όπως είναι οι δικτυακές υποδομές που υποστηρίζουν την λειτουργία του, το λογισμικό του, το υλικό σύστημα και την αντοχή – ανοχή του σε παράγοντες κινδύνου, όπως είναι οι διακοπές παροχής ηλεκτρικής ενέργειας, οι φυσικές καταστροφές κ.ά. Τέλος, μια άλλη παράμετρος που επηρεάζει την διαθεσιμότητα του διαδικτυακού τόπου στους πιθανούς επισκέπτες του, είναι η διαθεσιμότητα της πρόσβασης των χρηστών σε αυτόν (Vrakas, Kalloniatis, & Lambrinoudakis, 2010).

1.8.1. Προστασία δεδομένων

Άμεσα συνυφασμένη με την ασφάλεια των ΔΔΤ, είναι η αξιοπιστία τους και η αποδοχή τους και η από μέρους των επισκεπτών – χρηστών. Οι ΔΔΤ θα πρέπει να παρέχουν ικανοποιητική ασφάλεια και αξιοπιστία, εξασφαλίζοντας τις παρακάτω παραμέτρους (Βεργή, 2009):

- ***Την ακεραιότητα (integrity)***: που αφορά την εξασφάλιση του γεγονότος ότι η πληροφορία η οποία διακινείται, δημοσιεύεται, αποθηκεύεται και επεξεργάζεται, παραμένει αναλλοίωτη.

- ***Η αναγνώριση (identification)***: που αναφέρεται στον προσδιορισμό της ταυτότητας του χρήστη.

- ***Η εμπιστευτικότητα (confidentiality)***: που αναφέρεται στην πρόσβαση στην πληροφορία μόνο αυτών που διαθέτουν την κατάλληλη εξουσιοδότηση.

- ***Η πιστοποίηση ταυτότητας (authentication)***: αναφέρεται στην συγκεκριμένη ενέργεια η οποία διασφαλίζει ότι η ταυτότητα την οποία δηλώνει ο χρήστης, αντιστοιχεί πράγματι σε αυτόν.

- ***Η εξουσιοδότηση (authorization)***: που αφορά την εξασφάλιση ότι κάθε οντότητα έχει πρόσβαση σε εκείνους τους πόρους του συστήματος που της έχει επιτραπεί η είσοδος.

- ***Η διαθεσιμότητα (availability)***: που αφορά την διαθεσιμότητα της πληροφορίας οποτεδήποτε ένας εξουσιοδοτημένος χρήστης επιχειρήσει να αποκτήσει πρόσβαση σε αυτήν.

- ***Η μη άρνηση συμμετοχής (non-repudiation)***: που αφορά την μη δυνατότητα άρνησης ενός χρήστη, ότι εκτέλεσε κάποια ενέργεια σχετική με την πρόσβαση, την καταχώρηση και την επεξεργασία της πληροφορίας. Η ασφάλεια των ΔΔΤ συνιστάτε σε ένα σύνθετο πλαίσιο οδηγιών και κανόνων, που έχουν σχέση με την οργάνωση του φορέα του δικτυακού τόπου, αλλά και του παρόχου ο οποίος φιλοξενεί, τις διαδικασίες τις οποίες εφαρμόζει, τις υπηρεσίες τις οποίες παρέχει, τις τεχνικές υποδομές που διαθέτει και τέλος, το νομικό πλαίσιο για προστασία προσωπικών δεδομένων και για ασφάλεια επικοινωνιών.

1.8.2. Πρόσβαση – Αυθεντικοποίηση

Η δημόσια πληροφορία είναι επί το πλείστων ο κυρίως όγκος του περιεχομένου των ΔΔΤ ο οποίος είναι και αρκετά μεγάλος. Οι ηλεκτρονικές υπηρεσίες οι παρέχονται από τους ΔΔΤ, είναι δυνατόν να περιλαμβάνουν προσωπικά στοιχεία χρηστών, πρόσβαση σε δεδομένα τα οποία τους αφορούν, υποβολή αιτήσεων και διάφορες άλλες ενέργειες που σχετίζονται γενικά με την πρόσβαση, την καταχώριση, αλλά και την τροποποίηση δεδομένων, τα οποία αποτελούν δημόσια πληροφορία, συνδέονται όμως άμεσα με τον κάθε χρήστη (Tsoumas, 2007).

Η πρόσβαση σε δεδομένα και υπηρεσίες τα οποία έχουν δημόσιο χαρακτήρα, πρέπει οπωσδήποτε να ελέγχεται. Ακόμη, οι υπηρεσίες και το περιεχόμενο τα οποία διατίθενται μέσω ενός ΔΔΤ, θα πρέπει να ταξινομείται ανάλογα με το επίπεδο ευαισθησίας και διαβάθμισής του ανάλογα με τις ομάδες χρηστών στις οποίες απευθύνεται. Οι αρχές οι οποίες γενικά θα πρέπει να ακολουθούνται, είναι οι εξής (Vrakas et al., 2010):

- Η ταυτοποίηση των χρηστών δεν πρέπει να είναι απαραίτητη κατά την πρόσβαση σε λειτουργίες του ΔΔΤ ή σε δημόσια πληροφορία, όπως π.χ. υπηρεσίες επιπέδων 1 και 2 ή αναζήτηση πληροφορίας.

- Για πρόσβαση σε πληροφορίες οι οποίες αφορούν τον χρήστη, είτε αυτός είναι επιχείρηση, είτε πολίτης ή φορέας και υπηρεσίες που αφορούν τα επίπεδα 3 και 4, θα πρέπει προηγουμένως να γίνεται εξακρίβωση της ταυτότητας του. Το επίπεδο ασφαλείας είναι ανάλογα με την κρισιμότητα ή την ευαισθησία των υπηρεσιών και των δεδομένων. Πιο συγκεκριμένα: α) για τις υπηρεσίες για τις οποίες η διαδικασία εξυπηρέτησης αρχίζει με την ηλεκτρονική υποβολή εγγράφων ή στοιχείων μέσω του ΔΔΤ, η ολοκλήρωση τους όμως γίνεται με μη ηλεκτρονικό τρόπο, όπως π.χ. παραλαβή πιστοποιητικού ή βεβαίωσης αυτοπροσώπως μέσω ταχυδρομείου ή ΚΕΠ σαν διακριτικά για την ασφάλεια του χρήστη είναι δυνατόν να χρησιμοποιηθούν το όνομα (username) και το συνθηματικό (password) και β) για υπηρεσίες των οποίων η διαδικασία εξυπηρέτησης γίνεται εξολοκλήρου με ηλεκτρονικό τρόπο (επίπεδο 4), θα πρέπει να γίνεται χρήση ισχυρότερων δήλωσης και εξακρίβωσης της ταυτότητας π.χ. έγγραφα που εκδίδονται από υποδομές δημοσίου κλειδιού (Public Key Infrastracture - PKI).

Σύμφωνα με όλα τα παραπάνω οι χρήστες των ηλεκτρονικών υπηρεσιών του ΔΔΤ αρχίζουν να εξυπηρετούνται δηλώνοντας την ταυτότητα τους, τα στοιχεία της οποίας εξακριβώνονται από τα συστήματα του φορέα. Η επεξεργασία των δεδομένων που εισάγονται από τους χρήστες, η διεκπεραίωση και η εμφάνιση των αποτελεσμάτων γίνεται παράλληλα με την συμμετοχή και αρκετών συστημάτων υποστήριξης (back-office) (Αποστολάκης, Λουκής, & Χάλαρης, 2004), τα οποία μπορεί να απαιτούν από τον χρήστη να πιστοποιήσει την ταυτότητα του προκειμένου να διεκπεραιώσουν την υπόθεση του.

Επίσης οι φορείς της δημόσιας διοίκησης θα πρέπει να εξασφαλίζουν ότι τα στοιχεία που καταθέτει ο πολίτης για να έχει πρόσβαση στις ηλεκτρονικές υπηρεσίες μέσω των ΔΔΤ, είναι αρκετά για την εξακρίβωση της ταυτότητας του και στη συνέχεια την διεκπεραίωση των υπηρεσιών. Τέλος, τα στοιχεία τα οποία καταθέτει ο χρήστης όταν επικοινωνεί με ένα ΔΔΤ, θα πρέπει να προστατεύονται

πλήρως με χρήση πρωτοκόλλου και συγκεκριμένα του πρωτοκόλλου HTTPS (Hyper Text Transfer Protocol Secure) (Ράπτης, 2016).

1.8.3. Διαθεσιμότητα – Απόδοση συστημάτων

Το εσωτερικό δίκτυο ενός φορέα που χρησιμεύει για την σύνδεση ενός ΔΔΤ με τα υποστηρικτικά του συστήματα, αποτελείται από ενεργά και παθητικά στοιχεία. Ενεργά στοιχεία είναι π.χ. οι δρομολογητές και οι μεταγωγείς, ενώ παθητικά η δομημένη καλωδίωση. Γίνεται λοιπόν φανερό ότι η απόδοση και η διαθεσιμότητα του ΔΔΤ από πλευράς υποδομών, εξαρτάται από την απόδοση και την διαθεσιμότητα των παθητικών και των ενεργητικών στοιχείων του. Δεδομένου ότι ραχοκοκαλιά της διαδικτυακής υποδομής ενός φορέα είναι η δομημένη του καλωδίωση η οποία έχει σημαντικό κόστος και δεν είναι δυνατόν να αντικαθίσταται συχνά, ο φορέας θα πρέπει να μεριμνά έγκαιρα για την εξυπηρέτηση των βραχυπρόθεσμων αλλά και των μακροπρόθεσμων αναγκών του (Αποστολάκης και συν., 2004), η παραπάνω απαίτηση ικανοποιείται με την συμμόρφωση του φορέα σύμφωνα με πρότυπα διεθνώς αναγνωρισμένα και την χρήση υψηλών ποιοτικά υλικών.

Επίσης, τα ενεργά στοιχεία του δικτύου που θα χρησιμοποιηθούν για να συνδέσουν τον ΔΔΤ με τα υποστηρικτικά συστήματα θα πρέπει να καλύπτουν πλήρως τις ανάγκες του φορέα, τόσο ως προς τον αριθμό των χρηστών, όσο και ως προς τον όγκο των διακινούμενων δεδομένων. Για τον λόγο αυτό συνήθως προτείνεται το εσωτερικό δίκτυο του φορέα να περιλαμβάνει περισσότερα ενεργά στοιχεία από όσα χρειάζονται για την σύνδεση του ΔΔΤ με τα υποστηρικτικά συστήματα του και μάλιστα σε διάταξη υψηλής διαθεσιμότητας προκειμένου να διασφαλίζεται η λειτουργία του δικτύου ακόμα και σε περίπτωση εμφάνισης προβλήματος σ’ ένα από τα στοιχεία του (Ράπτης, 2016).

1.8.4. Διαθεσιμότητα – Απόδοση εξυπηρετητών

Για την λειτουργία ενός ΔΔΤ οι εξυπηρετητές που χρειάζονται για την ορθή λειτουργία του είναι οι παρακάτω:

- Ο εξυπηρετητής διαδικτύου (web server), ο οποίος υποστηρίζει την διεπαφή των χρηστών με το ΔΔΤ και την παρουσία του ΔΔΤ στο διαδίκτυο.

- Ο εξυπηρετητής εφαρμογών (application server), ο οποίος περιέχει όλες τις απαραίτητες εφαρμογές οι οποίες χρειάζονται για την λειτουργία του ΔΔΤ καθώς και τις υπηρεσίες που παρέχει.

- Ο εξυπηρετητής βάσεων δεδομένων (database server), ο οποίος περιέχει όλα τα δεδομένα από τις διάφορες εφαρμογές.

Προκειμένου οι παραπάνω εξυπηρετητές να καλύπτουν επαρκώς τις ανάγκες τόσο του φορέα όσο και των επισκεπτών του ΔΔΤ, ανεξαρτήτως αριθμού χρηστών και όγκου δεδομένων που διακινούνται μέσα σ΄αυτόν, οι φορείς του δημοσίου θα πρέπει να προβαίνουν σε εκτίμηση των παραπάνω αναγκών και στην συνέχεια να προχωρούν στην προμήθεια των συστημάτων τα οποία θα υποστηρίξουν την λειτουργία του ΔΔΤ. Όπως και προηγουμένως έτσι και εδώ θα πρέπει να περιλαμβάνονται πλεονάζοντες εξυπηρετητές σε διάταξη υψηλής διαθεσιμότητας ή να γίνεται χρήση τεχνικών εξισορρόπησης φορτίου (load balancing) (Βεργή, 2009).

1.8.5. <u>Αντοχή σε κινδύνους φυσικής ασφάλειας</u>

Η ενδεχόμενη εκδήλωση κινδύνων όπως φυσικές καταστροφές, διακοπές ή διακυμάνσεις στην παροχή ηλεκτρικής ενέργειας κ.τ.λ. θα πρέπει να λαμβάνεται υπόψη από τους φορείς του δημοσίου έτσι ώστε να λαμβάνονται όλα τα απαραίτητα και κατάλληλα μέτρα. Επίσης, οι χώροι στους οποίους φιλοξενούνται όλα τα συστήματα τα οποία υποστηρίζουν την λειτουργία ενός ΔΔΤ πρέπει να είναι κατάλληλα διαμορφωμένοι και να πληρούν κατά ελάχιστο τις παρακάτω απαιτήσεις (Λιουδάκης, 2008):

- Να διαθέτουν επαρκή κλιματισμό και εξαερισμό πυρόσβεσης.

- Να κλειδώνουν ώστε να μην είναι προσβάσιμα σε όλους.

- Τα υπολογιστικά συστήματα να τοποθετούνται σε ικριώματα (racks), να υποστηρίζονται από συστήματα αδιάλειπτης παροχής ηλεκτρικής ενέργειας (UPS), με ικανή ισχύ, ώστε να μπορούν να καλύψουν τις ανάγκες των συστημάτων για 20 λεπτά τουλάχιστον.

- Να διαθέτουν υπερυψωμένο δάπεδο, ψευδοροφές και ηλεκτρονικό σύστημα ελεγχόμενης πρόσβασης (access control).

- Να υποστηρίζονται από γεννήτριες ηλεκτρικής ενέργειας.

1.8.6. Προσβασιμότητα

Προκειμένου να διασφαλιστεί η προσβασιμότητα του ΔΔΤ σε όσο το δυνατόν μεγαλύτερο κοινό θα πρέπει να ακολουθούνται κάποιες προδιαγραφές, οδηγίες και κατευθύνσεις όπως αυτές αναπτύχθηκαν από το World Wide Consortium (W3C). Οι οδηγίες αυτές ορίζουν τρεις προτεραιότητες (De Vivo, de Vivo, & Germinal, 1998):

- ***Προτεραιότητα επιπέδου 1 (Priority 1)***: Κάθε μία οδηγία του συγκεκριμένου επιπέδου προτεραιότητας πρέπει οπωσδήποτε να ακολουθείται, διαφορετικά η προσβασιμότητα του συγκεκριμένου διαδικτυακού τόπου για πολλές κατηγορίες χρηστών θα είναι αδύνατη.

- ***Προτεραιότητα επιπέδου 2 (Priority 2)***: Κάθε οδηγία του συγκεκριμένου επιπέδου προτεραιότητας καλό είναι να ακολουθείται, αλλιώς η προσβασιμότητα του διαδικτυακού τόπου ίσως είναι δύσκολη για κάποιες κατηγορίες χρηστών.

- ***Προτεραιότητα επιπέδου 3 (Priority 3)***: Η εφαρμογή των οδηγιών που αποδίδονται στο συγκεκριμένο επίπεδο προτεραιότητας αφήνονται στη διακριτική ευχέρεια αυτού που είναι υπεύθυνος για την ανάπτυξη του διαδικτυακού τόπου. Στην περίπτωση μη εφαρμογής τους είναι δυνατόν η προσβασιμότητα να παρουσιάσει μικρές δυσκολίες για κάποιες κατηγορίες χρηστών.

Ακόμη, υπάρχουν και τρία επίπεδα συμμόρφωσης (conformance level), τα εξής (Vivo et al, 1998; Λιουδάκης, 2008):

- Επίπεδο συμμόρφωσης Α: Στο επίπεδο αυτό ικανοποιούνται όλες οι οδηγίες του επιπέδου προτεραιότητας 1.

- Επίπεδο συμμόρφωσης AA: Στο επίπεδο αυτό ικανοποιούνται όλες οι οδηγίες των επιπέδων προτεραιότητας 1 και 2.

- Επίπεδο συμμόρφωσης AAA: Στο επίπεδο αυτό ικανοποιούνται όλες οι οδηγίες των επιπέδων προτεραιότητας 1, 2 και 3.

Σύμφωνα με τα παραπάνω και τους ορισμούς των προτεραιοτήτων των οδηγιών Web Content Accessibility Guidelines (WCAG), η συμμόρφωση με το επίπεδο Α είναι απαραίτητη, με το επίπεδο ΑΑ προαιρετική, ενώ με το επίπεδο ΑΑΑ υπό μελέτη (Βεργή, 2009).

1.9 Διαλειτουργικότητα

Ως διαλειτουργικότητα ορίζεται η δυνατότητα συνεργασίας μεταξύ διαφόρων οργανισμών με ένα ομοιογενή και αποτελεσματικό τρόπο με σκοπό την επίτευξη κοινών στόχων και η οποία περιλαμβάνει διαμοιρασμό της πληροφορίας που εμπλέκεται στις επιχειρησιακές τους διαδικασίες και πραγματοποιείται μέσω της σύνδεσης των πληροφοριακών συστημάτων και επικοινωνιών που τις υποστηρίζουν τα οποία υιοθετούν κοινά πρότυπα.

Η διαλειτουργικότητα αναγνωρίζεται διεθνώς σαν ένα από τα σημαντικότερα ζητήματα για την επίτευξη της αποτελεσματικής και αποδοτικής λειτουργίας πληροφοριακών συστημάτων σε επιχειρήσεις και οργανισμούς κάθε μεγέθους και κλάδου. Μέσω της διαλειτουργικότητας ενισχύεται η συνεργασία μεταξύ πολιτών - επιχειρήσεων και δημόσιων φορέων, ενώ παράλληλα μειώνονται οι απαιτούμενες επενδύσεις για συντήρηση και διασύνδεση πολύπλοκων συστημάτων. Η διαλειτουργικότητα εξετάζεται και αναλύεται ως εξής: (ΚτΠ, 2008)

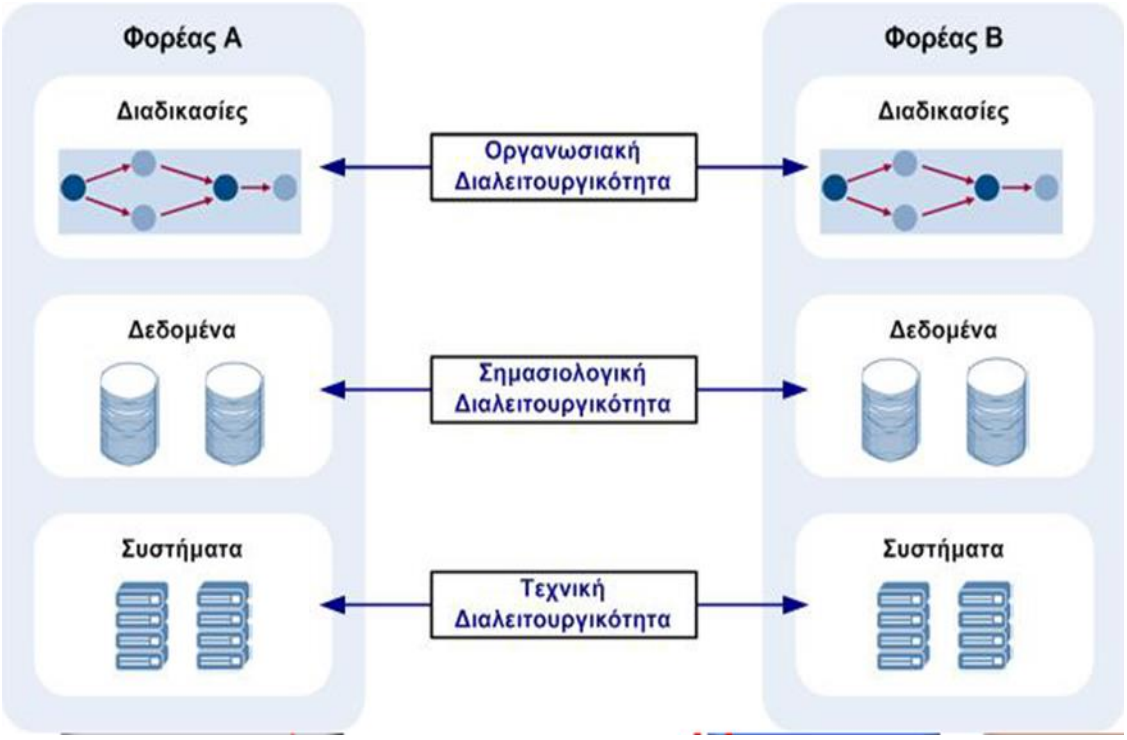
- την *Οργανωσιακή Διαλειτουργικότητα*, η οποία αναφέρεται στον καθορισμό στόχων, τη διαμόρφωση διαδικασιών και την επίτευξη συνεργασίας των φορέων που επιδιώκουν ανταλλαγή πληροφοριών και ίσως έχουν διαφορετικές εσωτερικές δομές και διαδικασίες. Επιπλέον στοχεύει στην ικανοποίηση των απαιτήσεων της κοινότητας των χρηστών προσφέροντας υπηρεσίες αναγνωρίσιμες, προσβάσιμες και επικεντρωμένες στις ανάγκες του

χρήστη. Η Οργανωσιακή Διαλειτουργικότητα διασφαλίζεται μέσω νομοθετικών ρυθμίσεων και διατάξεων και μέσω γενικών συμφωνιών μεταξύ των εμπλεκόμενων φορέων.

- τη *Σημασιολογική Διαλειτουργικότητα*, η οποία αφορά στη διασφάλιση ότι η ακριβής έννοια/σημασία των ανταλλασσόμενων πληροφοριών είναι κατανοητή από οποιαδήποτε εφαρμογή. Η επίτευξη διαλειτουργικότητας σε σημασιολογικό επίπεδο επιτρέπει στα συστήματα να συνδυάζουν τις πληροφορίες με εκείνες από άλλες πηγές και να τις επεξεργάζονται αποτελεσματικά. Η Σημασιολογική Διαλειτουργικότητα επιτυγχάνεται ορίζοντας και υιοθετώντας κοινό λεξιλόγιο και ορολογία σε όλα τα συστήματα και υπηρεσίες. Ο ορισμός και η συντήρηση ενός τέτοιου «λεξικού» γίνεται συνήθως από μια κεντρική υπηρεσία.

- την *Τεχνική Διαλειτουργικότητα*, η οποία αναφέρεται στην ικανότητα μεταφοράς και χρησιμοποίησης της πληροφορίας με ομοιογενή και αποτελεσματικό τρόπο μεταξύ συστημάτων πληροφορικής και οργανισμών. Το επίπεδο αυτό αφορά σε τεχνικές προδιαγραφές για την αποθήκευση, δόμηση, μεταφορά, παρουσίαση και ασφάλεια δεδομένων και υπηρεσιών. Η Τεχνική Διαλειτουργικότητα αντιπροσωπεύει τη διαλειτουργικότητα των υποδομών και του λογισμικού.

Στο σχήμα 2-3 παρουσιάζονται οι διαστάσεις και τα επίπεδα της διαλειτουργικότητας μεταξύ δύο φορέων.



ΣΧΗΜΑ 2-3.ΔΙΑΣΤΑΣΕΙΣ ΚΑΙ ΕΠΙΠΕΔΑ ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑΣ

(Πηγή: (ΚτΠ, 2008))

1.10 Διαλειτουργικότητα σε Πανευρωπαϊκό επίπεδο

Στον γενικότερο Ευρωπαϊκό χώρο, έχει θεσπιστεί το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας (European Interoperability Framework, EIF) το οποίο είναι μια από κοινού συμφωνημένη προσέγγιση για την παροχή ευρωπαϊκών δημόσιων υπηρεσιών με διαλειτουργικό τρόπο. Ορίζει τις βασικές κατευθυντήριες γραμμές για τη διαλειτουργικότητα με τη μορφή κοινών αρχών, μοντέλων και συστάσεων με κυριότερο σκοπό (EC, 2017):

- Να εμπνεύσει τις ευρωπαϊκές δημόσιες διοικήσεις στην προσπάθειά τους να σχεδιάσουν και να παρέχουν απρόσκοπτες ευρωπαϊκές δημόσιες υπηρεσίες προς άλλες δημόσιες διοικήσεις, πολίτες και επιχειρήσεις που, στο μέτρο του δυνατού, είναι εκ προεπιλογής ψηφιακές (δηλαδή παρέχουν υπηρεσίες και δεδομένα κατά προτίμηση μέσω ψηφιακών διαύλων), εκ προεπιλογής διασυνοριακές (δηλαδή προσβάσιμες για όλους τους πολίτες στην ΕΕ) και εκ προεπιλογής ανοικτές (δηλαδή επιτρέπουν την περαιτέρω χρήση, συμμετοχή/πρόσβαση και διαφάνεια).

- Να παρέχει κατευθύνσεις προς τις δημόσιες διοικήσεις όσον αφορά τον σχεδιασμό και την επικαιροποίηση των Εθνικών Πλαισίων Διαλειτουργικότητας (ΕΠΔ) (National Interoperability Framework, NIF) ή των εθνικών πολιτικών, στρατηγικών και κατευθυντήριων γραμμών που προωθούν τη διαλειτουργικότητα.

- Να συμβάλει στην καθιέρωση της ψηφιακής ενιαίας αγοράς, προωθώντας τη διασυνοριακή και διατομεακή διαλειτουργικότητα για την παροχή ευρωπαϊκών δημόσιων υπηρεσιών.

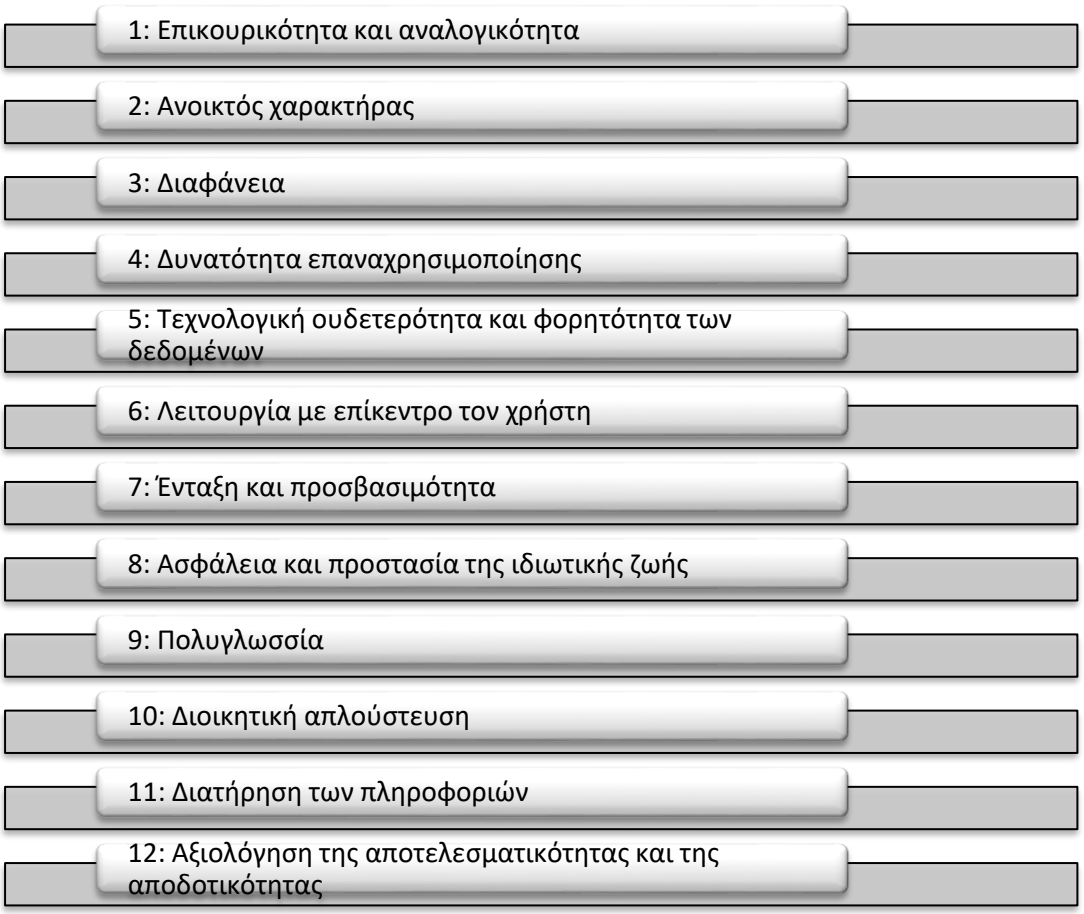
Όλες οι προτάσεις του Ευρωπαϊκού Πλαισίου Διαλειτουργικότητας (EIF) είναι βασισμένες σε δώδεκα βασικές αρχές οι οποίες ομαδοποιούνται σε τέσσερις κατηγορίες:

1. Αρχή που καθορίζει το πλαίσιο των δράσεων της ΕΕ για τη διαλειτουργικότητα (1).

2. Βασικές αρχές διαλειτουργικότητας (2 - 5).

3. Αρχές που αφορούν τις γενικές ανάγκες και προσδοκίες των χρηστών (6 - 9).

4. Θεμελιώδεις αρχές για τη συνεργασία μεταξύ δημόσιων διοικήσεων (10 - 12).



ΣΧΗΜΑ 2-4.ΑΡΧΕΣ ΕΥΡΩΠΑΪΚΗΣ ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑΣ

(Πηγή: (EC, 2017))

1.10.1. <u>Βασική αρχή 1: επικουρικότητα και αναλογικότητα:</u>

Η αρχή της επικουρικότητας προϋποθέτει τη λήψη των αποφάσεων της ΕΕ όσο το δυνατόν πιο κοντά στον πολίτη. Με άλλα λόγια, η ΕΕ δεν λαμβάνει μέτρα αν αυτό δεν είναι πιο αποτελεσματικό από τη λήψη των μέτρων σε εθνικό επίπεδο. Η αρχή της αναλογικότητας περιορίζει τις δράσεις της ΕΕ στις αναγκαίες για την επίτευξη των στόχων των Συνθηκών.

Όσον αφορά τη διαλειτουργικότητα, ένα ευρωπαϊκό πλαίσιο δικαιολογείται να υπερβεί διαφορές σε πολιτικές που καταλήγουν σε ανομοιογένεια και έλλειψη διαλειτουργικότητας και θέτουν σε κίνδυνο την ψηφιακή ενιαία αγορά.

Το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας (EIF) προβλέπεται να αποτελεί τον «κοινό παρονομαστή» των πολιτικών διαλειτουργικότητας στα κράτη

μέλη. Τα κράτη μέλη θα πρέπει να διαθέτουν επαρκή ελευθερία για την ανάπτυξη των οικείων Εθνικών Πλαισίων Διαλειτουργικότητας (NIF) όσον αφορά τις συστάσεις του EIF. Τα NIF αναμένεται να προσαρμοστούν και να επεκταθούν έτσι ώστε να λαμβάνονται δεόντως υπόψη οι εθνικές ιδιαιτερότητες.

1.10.2. Βασική αρχή 2: ανοικτός χαρακτήρας

Στο πλαίσιο διαλειτουργικών δημόσιων υπηρεσιών, η έννοια του ανοικτού χαρακτήρα αφορά κυρίως δεδομένα, προδιαγραφές και λογισμικό. Τα ανοικτά δημόσια δεδομένα αναφέρονται στην ιδέα ότι όλα τα δημόσια δεδομένα θα πρέπει να διατίθενται ελεύθερα για χρήση και περαιτέρω χρήση από άλλους, εφόσον δεν ισχύουν περιορισμοί π.χ. για την προστασία δεδομένων προσωπικού χαρακτήρα, για λόγους απορρήτου ή για δικαιώματα διανοητικής ιδιοκτησίας. Οι δημόσιες διοικήσεις συλλέγουν και παράγουν τεράστιο όγκο δεδομένων. Η οδηγία για την περαιτέρω χρήση πληροφοριών του δημόσιου τομέα ενθαρρύνει τα κράτη μέλη να καθιστούν τις δημόσιες πληροφορίες διαθέσιμες για πρόσβαση και περαιτέρω χρήση ως ανοικτά δεδομένα. Επίσης προβλέπεται η κοινοχρησία συνόλων και υπηρεσιών χωρικών δεδομένων μεταξύ δημόσιων αρχών χωρίς περιορισμούς ή πρακτικά εμπόδια στην περαιτέρω χρήση τους. Τα εν λόγω δεδομένα θα πρέπει να δημοσιεύονται με όσο το δυνατόν λιγότερους περιορισμούς και με σαφείς άδειες για τη χρήση τους, προκειμένου να επιτρέπεται ο αποτελεσματικότερος έλεγχος των διαδικασιών λήψης αποφάσεων από τις διοικήσεις και να εφαρμόζεται η διαφάνεια στην πράξη.

Η χρήση τεχνολογιών και προϊόντων λογισμικού ανοικτής πηγής μπορεί να συντελέσει στην εξοικονόμηση κόστους ανάπτυξης, στην αποφυγή φαινομένου εγκλωβισμού και να επιτρέψει την ταχεία προσαρμογή σε συγκεκριμένες επιχειρηματικές ανάγκες, επειδή οι κοινότητες ανάπτυξης που τις υποστηρίζουν τις αναπροσαρμόζουν διαρκώς. Οι δημόσιες διοικήσεις δεν θα πρέπει μόνο να χρησιμοποιούν λογισμικό ανοικτής πηγής, αλλά, όπου είναι εφικτό, θα πρέπει να συμβάλλουν στο έργο των συναφών κοινοτήτων ανάπτυξης. Η ανοικτή πηγή αποτελεί καταλύτη της βασικής αρχής του EIF για τη δυνατότητα επαναχρησιμοποίησης.

Το επίπεδο του ανοικτού χαρακτήρα μιας προδιαγραφής/ενός προτύπου είναι καθοριστικό για την περαιτέρω χρήση στοιχείων λογισμικού που υλοποιούν την εν λόγω προδιαγραφή. Αυτό ισχύει επίσης σε περίπτωση που αυτά τα στοιχεία χρησιμοποιούνται για τη δημιουργία νέων ευρωπαϊκών δημόσιων υπηρεσιών. Αν η αρχή του ανοικτού χαρακτήρα εφαρμόζεται στο ακέραιο:

- όλοι οι ενδιαφερόμενοι έχουν τη δυνατότητα να συμβάλλουν στην εκπόνηση των προδιαγραφών και η δημόσια επανεξέταση αποτελεί μέρος της διαδικασίας λήψης αποφάσεων·
- η προδιαγραφή είναι διαθέσιμη σε όλους προς μελέτη·
- τα δικαιώματα πνευματικής ιδιοκτησίας που αναφέρονται στην προδιαγραφή χορηγούνται υπό όρους με τρόπο που επιτρέπει την εφαρμογή τόσο σε ιδιόκτητο λογισμικό όσο και σε λογισμικό ανοικτής πηγής, και κατά προτίμηση ατελώς.

Λόγω του θετικού τους αντίκτυπου στη διαλειτουργικότητα, η χρήση ανοικτών προδιαγραφών έχει προωθηθεί σε πολλές δηλώσεις πολιτικής και ενθαρρύνεται όσον αφορά την παροχή ευρωπαϊκών δημόσιων υπηρεσιών. Τα θετικά αποτελέσματα των ανοικτών προδιαγραφών αποδεικνύονται επίσης από το οικοσύστημα του διαδικτύου. Ωστόσο, οι δημόσιες διοικήσεις μπορεί να αποφασίσουν να χρησιμοποιούν λιγότερο ανοικτές προδιαγραφές, εφόσον δεν υπάρχουν ανοικτές προδιαγραφές ή δεν καλύπτουν τις λειτουργικές ανάγκες. Σε κάθε περίπτωση, οι προδιαγραφές θα πρέπει να είναι ώριμες και να υποστηρίζονται επαρκώς από την αγορά, εκτός αν χρησιμοποιούνται στο πλαίσιο δημιουργίας καινοτόμων λύσεων.

Τέλος, ο ανοικτός χαρακτήρας συνεπάγεται επίσης την παροχή της δυνατότητας σε πολίτες και επιχειρήσεις να συμμετέχουν στον σχεδιασμό νέων υπηρεσιών, να συμβάλλουν στη βελτίωση των υπηρεσιών και να υποβάλλουν παρατηρήσεις σχετικά με την ποιότητα των υφιστάμενων δημόσιων υπηρεσιών.

1.10.3. Βασική αρχή 3: διαφάνεια

Η διαφάνεια στο πλαίσιο του ΕΠΔ αναφέρεται στα εξής:

- Στη δυνατότητα προβολής εντός του διοικητικού περιβάλλοντος μιας δημόσιας διοίκησης. Αυτή συνίσταται στο να έχουν οι άλλες δημόσιες διοικήσεις, πολίτες και επιχειρήσεις τη δυνατότητα να παρακολουθούν και να κατανοούν διοικητικούς κανόνες, διαδικασίες, δεδομένα, υπηρεσίες και τη διαδικασία λήψης αποφάσεων.

- Στη διασφάλιση της διαθεσιμότητας διεπαφών με εσωτερικά πληροφοριακά συστήματα. Οι δημόσιες διοικήσεις διαχειρίζονται μεγάλο αριθμό συχνά ανομοιογενών και διάσπαρτων πληροφοριακών συστημάτων που υποστηρίζουν τις εσωτερικές διαδικασίες τους. Η διαλειτουργικότητα εξαρτάται από τη διασφάλιση της ύπαρξης διεπαφών με αυτά τα συστήματα και με τα δεδομένα που χειρίζονται. Με τη σειρά της, η διαλειτουργικότητα διευκολύνει την περαιτέρω χρήση συστημάτων και δεδομένων, και επιτρέπει την ενσωμάτωσή τους σε μεγαλύτερα συστήματα.

Στη διασφάλιση του δικαιώματος προστασίας των δεδομένων προσωπικού χαρακτήρα, με τήρηση του ισχύοντος νομοθετικού πλαισίου για τους μεγάλους όγκους δεδομένων προσωπικού χαρακτήρα των πολιτών που τηρούν και διαχειρίζονται οι δημόσιες διοικήσεις

1.10.4. Βασική αρχή 4: δυνατότητα επαναχρησιμοποίησης

Η επαναχρησιμοποίηση σημαίνει ότι οι δημόσιες διοικήσεις που αντιμετωπίζουν συγκεκριμένο πρόβλημα επιδιώκουν να επωφεληθούν από την εργασία άλλων φορέων, αναζητώντας τι είναι διαθέσιμο, αξιολογώντας τη χρησιμότητα ή τη συνάφειά του με το υπό εξέταση πρόβλημα και, κατά περίπτωση, υιοθετώντας λύσεις που έχουν αποδειχτεί αποτελεσματικές σε άλλες περιστάσεις. Αυτό προϋποθέτει ότι η δημόσια διοίκηση είναι ανοικτή στην ανταλλαγή λύσεων, εννοιών, πλαισίων, προδιαγραφών, εργαλείων και στοιχείων διαλειτουργικότητας με άλλους φορείς.

Η δυνατότητα επαναχρησιμοποίησης λύσεων Τεχνολογιών Πληροφορικής (ΤΠ) (π.χ. στοιχείων λογισμικού, διεπαφών προγραμματισμού εφαρμογών, προτύπων), πληροφοριών και δεδομένων αποτελεί καταλύτη διαλειτουργικότητας και βελτιώνει την ποιότητα, διότι παρατείνει τη λειτουργική χρήση αλλά και συντελεί στην εξοικονόμηση κόστους και χρόνου. Η εν λόγω δυνατότητα συμβάλλει σημαντικά στην ανάπτυξη ψηφιακής ενιαίας αγοράς στην ΕΕ. Στα DIF υπάρχουν επίσης ορισμένα πρότυπα και προδιαγραφές της ΕΕ τα οποία θα πρέπει να εφαρμόζονται ευρύτερα.

Ορισμένες δημόσιες διοικήσεις και κυβερνήσεις στην ΕΕ ήδη προωθούν την ανταλλαγή και επαναχρησιμοποίηση λύσεων ΤΠ υιοθετώντας νέα επιχειρηματικά μοντέλα, προωθώντας τη χρήση λογισμικού ανοικτής πηγής για βασικές υπηρεσίες ΤΠΕ και κατά την ανάπτυξη υποδομών ψηφιακών υπηρεσιών.

Υπάρχουν ορισμένες βασικές προκλήσεις που περιορίζουν την ανταλλαγή και επαναχρησιμοποίηση λύσεων ΤΠ, σε τεχνικό, οργανωτικό, νομικό και επικοινωνιακό επίπεδο. Το πλαίσιο ανταλλαγής και επαναχρησιμοποίησης για λύσεις ΤΠ του ISA[2] (Λύσεις διαλειτουργικότητας για τις δημόσιες διοικήσεις, τις επιχειρήσεις και τους πολίτες - Interoperability solutions for public administrations, businesses and citizens) παρέχει συστάσεις που βοηθούν τις δημόσιες διοικήσεις να αντιμετωπίζουν αυτές τις προκλήσεις και να ανταλλάσσουν/επαναχρησιμοποιούν κοινές λύσεις ΤΠ. Η επαναχρησιμοποίηση και η ανταλλαγή μπορούν να υποστηριχτούν αποτελεσματικά από συνεργατικές πλατφόρμες.

1.10.5. Βασική αρχή 5: τεχνολογική ουδετερότητα και φορητότητα των δεδομένων

Κατά τη δημιουργία ευρωπαϊκών δημόσιων υπηρεσιών, οι δημόσιες διοικήσεις θα πρέπει να εστιάζουν σε λειτουργικές ανάγκες και να αναβάλλουν τις αποφάσεις σχετικά με την τεχνολογία όσο το δυνατόν περισσότερο, ώστε να ελαχιστοποιούνται οι τεχνολογικές εξαρτήσεις, να αποφεύγεται η επιβολή συγκεκριμένων τεχνικών εφαρμογών ή προϊόντων στα στελέχη τους και να μπορούν να προσαρμόζονται στο ταχέως εξελισσόμενο τεχνολογικό περιβάλλον.

Οι δημόσιες διοικήσεις θα πρέπει να παρέχουν τη δυνατότητα πρόσβασης και επαναχρησιμοποίησης των δημόσιων υπηρεσιών και δεδομένων τους ανεξάρτητα από συγκεκριμένες τεχνολογίες ή προϊόντα.

Η λειτουργία της ψηφιακής ενιαίας αγοράς προϋποθέτει τη δυνατότητα εύκολης μεταφοράς δεδομένων μεταξύ διαφορετικών συστημάτων, ώστε να αποφεύγεται ο εγκλωβισμός, καθώς και την υποστήριξη της ελεύθερης κυκλοφορίας των δεδομένων. Αυτή η απαίτηση αφορά τη φορητότητα δεδομένων - την ικανότητα μετακίνησης και επαναχρησιμοποίησης δεδομένων με εύκολο τρόπο μεταξύ διαφορετικών εφαρμογών και συστημάτων, η οποία θέτει ακόμα μεγαλύτερες προκλήσεις στο πλαίσιο διασυνοριακών σεναρίων.

1.10.6. <u>Βασική αρχή 6: λειτουργία με επίκεντρο τον χρήστη</u>

Ως χρήστες ευρωπαϊκών δημόσιων υπηρεσιών νοούνται δημόσιες διοικήσεις, πολίτες ή επιχειρήσεις που έχουν πρόσβαση σε αυτές τις υπηρεσίες και επωφελούνται από τη χρήση τους. Οι ανάγκες των χρηστών θα πρέπει να λαμβάνονται υπόψη κατά τον καθορισμό των δημόσιων υπηρεσιών που θα πρέπει να παρέχονται και του τρόπου παροχής τους.

Επομένως, στο μέτρο του δυνατού, οι ανάγκες και οι απαιτήσεις των χρηστών θα πρέπει να διέπουν τον σχεδιασμό και την ανάπτυξη δημόσιων υπηρεσιών, σύμφωνα με τις παρακάτω προσδοκίες:

- Μια προσέγγιση πολυκαναλικής παροχής υπηρεσιών, η οποία συνεπάγεται τη διαθεσιμότητα εναλλακτικών διαύλων, φυσικών και ψηφιακών, για την πρόσβαση σε μια υπηρεσία, αποτελεί σημαντικό μέρος του σχεδιασμού μιας δημόσιας υπηρεσίας, δεδομένου ότι οι χρήστες μπορεί να προτιμούν διαφορετικούς διαύλους αναλόγως με τις περιστάσεις και τις ανάγκες τους·

- Ένα ενιαίο σημείο επαφής θα πρέπει να καθίσταται διαθέσιμο σε χρήστες, προκειμένου να καλύπτει την εσωτερική διοικητική πολυπλοκότητα και να διευκολύνει την πρόσβαση σε δημόσιες υπηρεσίες, π.χ. όταν πρέπει να συνεργαστούν πολλοί φορείς για την παροχή μιας δημόσιας υπηρεσίας·

- Οι παρατηρήσεις που υποβάλλουν οι χρήστες θα πρέπει να συγκεντρώνονται, να αξιολογούνται και να χρησιμοποιούνται συστηματικά για τον σχεδιασμό νέων δημόσιων υπηρεσιών και την περαιτέρω βελτίωση των υφιστάμενων υπηρεσιών·

- Στο μέτρο του δυνατού, βάσει της ισχύουσας νομοθεσίας, οι χρήστες θα πρέπει να μπορούν να παρέχουν δεδομένα μόνο μία φορά, και οι διοικήσεις θα πρέπει να είναι σε θέση να ανακτούν και να ανταλλάσσουν αυτά τα δεδομένα για να εξυπηρετούν τον χρήστη, σύμφωνα με τους κανόνες για την προστασία των δεδομένων·

- Θα πρέπει να ζητείται από τους χρήστες να παρέχουν μόνο τις πληροφορίες που είναι απολύτως απαραίτητες προκειμένου να λάβουν μια συγκεκριμένη δημόσια υπηρεσία.

1.10.7. <u>Βασική αρχή 7: ένταξη και προσβασιμότητα</u>

Η ένταξη αφορά τη δυνατότητα που πρέπει να δοθεί στον καθένα να αξιοποιεί πλήρως τις ευκαιρίες που προσφέρουν οι νέες τεχνολογίες για πρόσβαση και χρήση ευρωπαϊκών δημόσιων υπηρεσιών, ώστε να αίρεται το κοινωνικό και οικονομικό χάσμα και ο αποκλεισμός.

Η προσβασιμότητα διασφαλίζει ότι άτομα με αναπηρίες, ηλικιωμένοι και λοιπές ομάδες να μην μειονεκτούν των ατόμων που μπορούν να χρησιμοποιούν δημόσιες υπηρεσίες σε επίπεδα συγκρίσιμα με τα επίπεδα υπηρεσιών που παρέχονται σε άλλους πολίτες.

Η ένταξη και η προσβασιμότητα πρέπει να αποτελούν μέρος του συνολικού κύκλου ζωής για την ανάπτυξη ευρωπαϊκών δημόσιων υπηρεσιών όσον αφορά τον σχεδιασμό, το περιεχόμενο των πληροφοριών και την παροχή της υπηρεσίας. Θα πρέπει να συμμορφώνονται με τις προδιαγραφές ηλεκτρονικής προσβασιμότητας που είναι ευρέως αποδεκτές σε ευρωπαϊκό ή διεθνές επίπεδο .

Η ένταξη και η προσβασιμότητα συνήθως συνεπάγονται πολυκαναλική παροχή υπηρεσιών. Η παραδοσιακή έντυπη ή κατ' ιδίαν παροχή υπηρεσίας μπορεί να χρειαστεί να συνυπάρξει με την ηλεκτρονική παροχή.

Η ένταξη και η προσβασιμότητα μπορούν επίσης να βελτιωθούν χάρη στην ικανότητα ενός πληροφοριακού συστήματος να επιτρέπει σε τρίτους να ενεργούν για λογαριασμό πολιτών οι οποίοι δεν είναι σε θέση, μόνιμα ή προσωρινά, να κάνουν άμεση χρήση των δημόσιων υπηρεσιών.

1.10.8. Βασική αρχή 8: ασφάλεια και προστασία της ιδιωτικής ζωής

Οι πολίτες και οι επιχειρήσεις πρέπει να αισθάνονται εμπιστοσύνη ότι όταν αλληλεπιδρούν με δημόσιες αρχές το πράττουν σε ασφαλές και αξιόπιστο περιβάλλον και σε πλήρη συμμόρφωση με τους συναφείς κανονισμούς, π.χ. τον κανονισμό και την οδηγία για την προστασία δεδομένων και τον κανονισμό σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης . Οι δημόσιες διοικήσεις πρέπει να εγγυώνται την ιδιωτική ζωή των πολιτών και την εμπιστευτικότητα, τη γνησιότητα, την ακεραιότητα και τη μη άρνηση αναγνώρισης των πληροφοριών που υποβλήθηκαν από πολίτες και επιχειρήσεις.

1.10.9. Βασική αρχή 9: πολυγλωσσία

Οι ευρωπαϊκές δημόσιες υπηρεσίες μπορούν δυνητικά να χρησιμοποιηθούν από οποιονδήποτε σε όλα τα κράτη μέλη. Επομένως, η πολυγλωσσία χρειάζεται προσεκτική εξέταση κατά τον σχεδιασμό. Οι πολίτες σε ολόκληρη την Ευρώπη συχνά αντιμετωπίζουν προβλήματα με την πρόσβαση και χρήση ψηφιακών δημόσιων υπηρεσιών, αν αυτές δεν είναι διαθέσιμες στις γλώσσες που μιλούν.

Χρειάζεται να βρεθεί μια ισορροπία μεταξύ των προσδοκιών των πολιτών και των επιχειρήσεων ώστε να εξυπηρετούνται στη γλώσσα τους ή την προτιμώμενη γλώσσα τους και της ικανότητας των δημόσιων διοικήσεων των κρατών μελών να προσφέρουν υπηρεσίες σε όλες τις επίσημες γλώσσες της ΕΕ. Μια κατάλληλη ισορροπία θα μπορούσε να επέλθει με τη διαθεσιμότητα των ευρωπαϊκών δημόσιων υπηρεσιών στις γλώσσες των αναμενόμενων τελικών χρηστών, δηλαδή ο αριθμός των γλωσσών αποφασίζεται με βάση τις ανάγκες των χρηστών, όπως το επίπεδο στο οποίο η υπηρεσία είναι καθοριστική για την υλοποίηση της ψηφιακής ενιαίας αγοράς ή εθνικών πολιτικών ή το μέγεθος του αντίστοιχου κοινού.

Η πολυγλωσσία έρχεται στο προσκήνιο όχι μόνο όσον αφορά τη διεπαφή χρήστη, αλλά σε όλα τα επίπεδα του σχεδιασμού των ευρωπαϊκών δημόσιων υπηρεσιών. Για παράδειγμα, οι επιλογές αναπαράστασης δεδομένων σε μια ηλεκτρονική βάση δεδομένων δεν θα πρέπει να περιορίζουν τη δυνατότητα υποστήριξης διαφορετικών γλωσσών.

Η πολυγλωσσική πτυχή της διαλειτουργικότητας επανέρχεται επίσης στο προσκήνιο όταν οι δημόσιες υπηρεσίες απαιτούν ανταλλαγή μεταξύ πληροφοριακών συστημάτων πέρα από γλωσσικά σύνορα, δεδομένου ότι πρέπει να διατηρηθεί το νόημα των ανταλλασσόμενων πληροφοριών.

1.10.10. <u>Βασική αρχή 10: διοικητική απλούστευση</u>

Όπου είναι εφικτό, οι δημόσιες διοικήσεις θα πρέπει να επιδιώκουν τον εξορθολογισμό και την απλούστευση των διοικητικών διαδικασιών τους βελτιώνοντας ή εξαλείφοντας τις διαδικασίες που δεν παρέχουν προστιθέμενη αξία στους πολίτες. Η διοικητική απλούστευση μπορεί να συμβάλει στη μείωση της διοικητικής επιβάρυνσης επιχειρήσεων και πολιτών όσον αφορά τη συμμόρφωση με τη νομοθεσία της ΕΕ ή με εθνικές υποχρεώσεις. Επίσης, οι δημόσιες διοικήσεις θα πρέπει να δημιουργήσουν ευρωπαϊκές δημόσιες υπηρεσίες που υποστηρίζονται από ηλεκτρονικά μέσα, περιλαμβανομένων των αλληλεπιδράσεών τους με άλλες δημόσιες διοικήσεις, πολίτες και επιχειρήσεις.

Η ψηφιοποίηση δημόσιων υπηρεσιών θα πρέπει να πραγματοποιηθεί σύμφωνα με τις εξής έννοιες:

- εκ προεπιλογής ψηφιακές, εφόσον κριθεί σκόπιμο, ώστε να υπάρχει τουλάχιστον ένας ψηφιακός δίαυλος διαθέσιμος για πρόσβαση και χρήση συγκεκριμένης ευρωπαϊκής δημόσιας υπηρεσίας·

- κατά προτεραιότητα ψηφιακές, που σημαίνει ότι δίνεται προτεραιότητα στη χρήση δημόσιων υπηρεσιών μέσω ψηφιακών διαύλων ενώ συνυπάρχει η εφαρμογή της έννοιας της πολυκαναλικής παροχής και της πολιτικής «καμία λάθος πόρτα» («no wrong door»), δηλαδή συνυπάρχουν οι φυσικοί και οι ψηφιακοί δίαυλοι.

1.10.11. Βασική αρχή 11: διατήρηση των πληροφοριών

Η νομοθεσία προβλέπει ότι οι αποφάσεις και τα δεδομένα αποθηκεύονται και η πρόσβαση σε αυτά είναι δυνατή για καθορισμένο χρονικό διάστημα. Αυτό σημαίνει ότι αρχεία και πληροφορίες σε ηλεκτρονική μορφή που τηρούνται από δημόσιες διοικήσεις για τον σκοπό της τεκμηρίωσης διαδικασιών και αποφάσεων πρέπει να διατηρούνται και να μετατρέπονται, όποτε είναι απαραίτητο, σε νέα μέσα, όταν τα παλαιά μέσα καθίστανται παρωχημένα. Ο στόχος είναι να διασφαλιστεί ότι τα αρχεία και οι λοιπές μορφές πληροφοριών παραμένουν αναγνώσιμα, αξιόπιστα και διατηρούν την ακεραιότητά τους, καθώς και ότι η πρόσβαση σε αυτά είναι δυνατή για όσο διάστημα χρειάζεται σύμφωνα με τις διατάξεις για την ασφάλεια και την προστασία της ιδιωτικής ζωής.

Για την εγγύηση της μακροπρόθεσμης διατήρησης ηλεκτρονικών αρχείων και λοιπών ειδών πληροφοριών, θα πρέπει να επιλέγονται μορφότυποι που διασφαλίζουν τη μακροπρόθεσμη προσβασιμότητα, περιλαμβανομένης της διαφύλαξης των αντίστοιχων ηλεκτρονικών υπογραφών ή σφραγίδων. Στο πλαίσιο αυτό, η χρήση εγκεκριμένων υπηρεσιών διαφύλαξης, σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014, μπορεί να διασφαλίσει τη μακροπρόθεσμη διατήρηση των πληροφοριών.

Για πηγές πληροφοριών που βρίσκονται υπό την κατοχή και τη διαχείριση εθνικών διοικήσεων, η διατήρηση αποτελεί αποκλειστικά εθνικό ζήτημα. Για πληροφορίες που δεν είναι αυστηρά εθνικές, η διατήρηση καθίσταται ευρωπαϊκό ζήτημα. Σε αυτή την περίπτωση, τα οικεία κράτη μέλη θα πρέπει να εφαρμόζουν κατάλληλη «πολιτική διατήρησης» προκειμένου να αντιμετωπίσουν τυχόν δυσκολίες που προκύπτουν αν οι συναφείς πληροφορίες χρησιμοποιούνται στο πλαίσιο διαφορετικής δικαιοδοσίας.

1.10.12. Βασική αρχή 12: αξιολόγηση αποτελεσματικότητας & αποδοτικότητας

Υπάρχουν πολλοί τρόποι να αποτιμηθεί η αξία των διαλειτουργικών ευρωπαϊκών δημόσιων υπηρεσιών, συμπεριλαμβανομένων πτυχών όπως η απόδοση της επένδυσης, το συνολικό κόστος κυριότητας, το επίπεδο ευελιξίας και προσαρμοστικότητας, η μειωμένη διοικητική επιβάρυνση, η αποδοτικότητα, ο μειωμένος κίνδυνος, η διαφάνεια, η απλούστευση, οι βελτιωμένες μέθοδοι

εργασίας και το επίπεδο ικανοποίησης των χρηστών.Στην προσπάθεια διασφάλισης της αποτελεσματικότητας και αποδοτικότητας των ευρωπαϊκών δημόσιων υπηρεσιών θα πρέπει να αξιολογούνται διάφορες τεχνολογικές λύσεις.

Το ευρωπαϊκό πλαίσιο διαλειτουργικότητας όπως φαίνεται παραπάνω έχει διαμορφωθεί σε στενή συνεργασία με τα κράτη μέλη και ύστερα από διαδικασία ευρείας διαβούλευσης με όλους τους άλλους συναφείς ενδιαφερόμενους φορείς. Για την επιτυχή εφαρμογή του προϋποτίθεται η ενεργή συμμετοχή όλων των παραγόντων, ιδίως των δημόσιων διοικήσεων. Οι σχεδιαζόμενες δράσεις θα διασφαλίσουν ότι το νέο ευρωπαϊκό πλαίσιο διαλειτουργικότητας μπορεί να επιτύχει τον απώτερο σκοπό του για παροχή διαλειτουργικών δημόσιων υπηρεσιών στην ΕΕ με επίκεντρο τον χρήστη (Ευρωπαϊκή Επιτροπή, 2017).

1.11 Εξέλιξη της Ηλεκτρονικής Διακυβέρνησης παγκοσμίως

Η έκθεση του 2016 των Ηνωμένων Εθνών, η οποία αναφέρεται στην ανάπτυξη της Ηλεκτρονικής Διακυβέρνησης παγκοσμίως (United Nations, 2016), εξετάζει πως μπορεί η Ηλεκτρονική Κυβέρνηση να υποστηρίξει την παροχή ολοκληρωμένων υπηρεσιών σε οικονομικό, κοινωνικό και περιβαλλοντικό επίπεδο στα πλαίσια της αειφόρου ανάπτυξης καθώς και τον τρόπο με τον οποίο μπορεί να επιτευχθεί γεφύρωση των διαφορών που υπάρχουν μεταξύ των οργανισμών με την υποστήριξη ενσωματωμένων πολιτικών και θεσμικού συντονισμού.

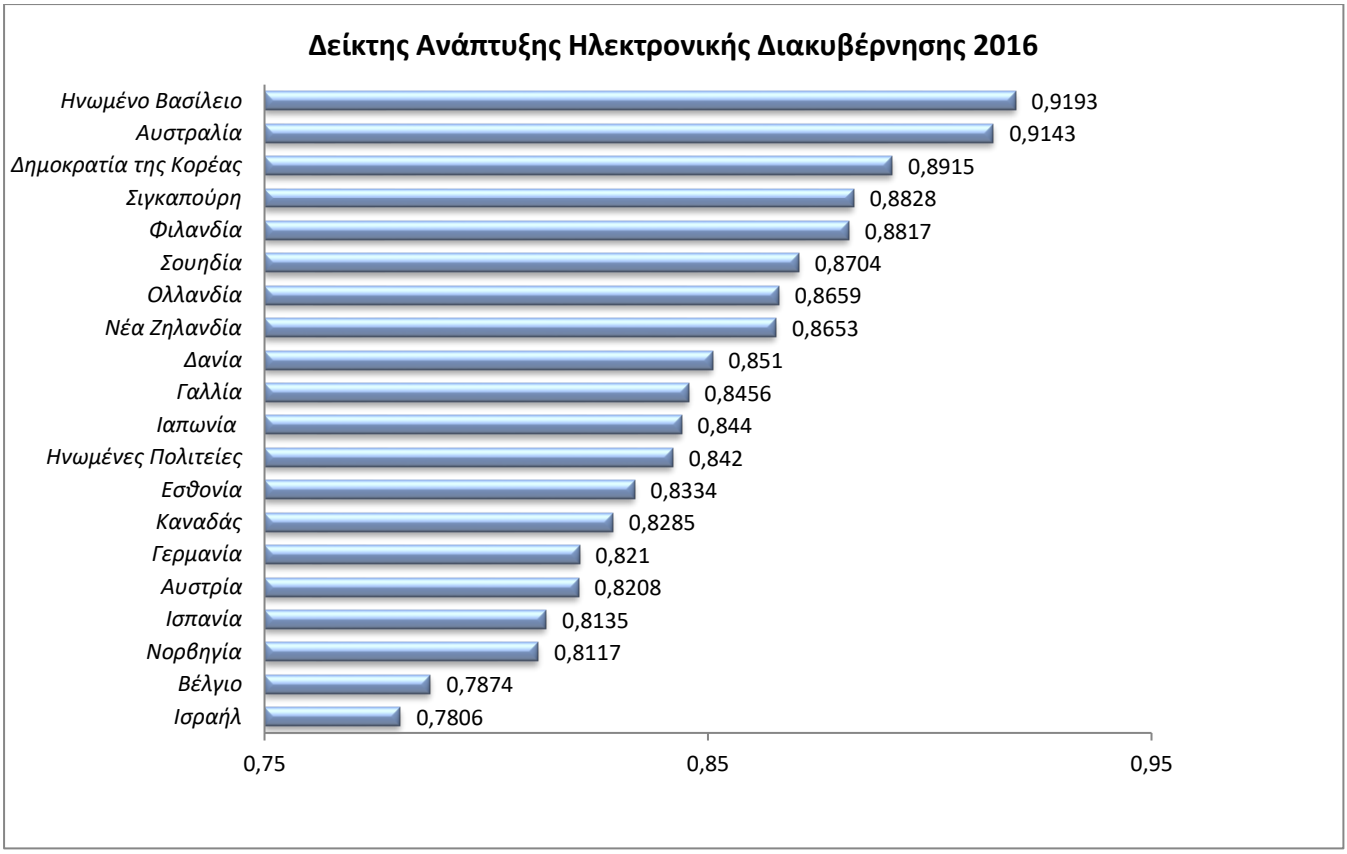
Παράλληλα, αναζητά τρόπους για την προώθηση προσεγγίσεων με γνώμονα τη ζήτηση προκειμένου να γεφυρωθεί το ψηφιακό χάσμα μεταξύ εκείνων που έχουν πρόσβαση και μπορούν να χρησιμοποιήσουν πλήρως τα κυβερνητικά δεδομένα και όσους έχουν μείνει πίσω σε μια κοινωνία η οποία παρέχει όλο και περισσότερα δεδομένα.

Επίσης, εξετάζει πως η ηλεκτρονική συμμετοχή μπορεί να συμβάλει στην προαγωγή κοινωνιών χωρίς αποκλεισμούς μέσω μιας παγκόσμιας και περιφερειακής ανάλυση των τάσεων ηλεκτρονικής συμμετοχής ενώ γίνεται μια επισκόπηση των υφιστάμενων μοντέλων ηλεκτρονικής συμμετοχής. Γίνεται μελέτη της αλληλεξάρτησης μεταξύ της ηλεκτρονικής πληροφόρησης, της ηλεκτρονικής

διαβούλευσης και της λήψης αποφάσεων μέσω ηλεκτρονικών υπολογιστών, τις προκλήσεις και τις ευκαιρίες που παρουσιάζονται μέσω της ηλεκτρονικής συμμετοχής ενώ παρέχονται επίσης καινοτόμοι τρόποι κινητοποίησης των ιδεών των ανθρώπων και των οικονομικών πόρων όπως είναι το crowdsourcing και το crowdfunding.

Διερευνώνται και αναλύονται οι παγκόσμιες τάσεις στην παροχή ηλεκτρονικών και κινητών δημόσιων υπηρεσιών ρίχνοντας φως στη διανομή επιγραμμικών υπηρεσιών ανά επίπεδο εισοδήματος και τομείς, η προσβασιμότητα και η διαθεσιμότητα της ευρυζωνικότητας η οποία αποτελεί ζωτικό παράγοντα οικονομικής, κοινωνικής και περιβαλλοντικής προόδου. Παρουσιάζεται μια ολοκληρωμένη προσέγγιση για την υπέρβαση των ψηφιακών διαχωρισμών και τις τάσεις των κυβερνητικών υπηρεσιών για απευθείας σύνδεση με τις ευάλωτες ομάδες. Τέλος, γίνεται αναφορά στην έννοια του Ίντερνετ των Πραγμάτων (IoT) και τη χρήση των Γεωγραφικών Πληροφοριακών Συστημάτων (GIS) και πως αυτές θα μπορούσαν να συμβάλλουν στην βελτίωση της παροχής υπηρεσιών.

Οι 20 χώρες που σημειώνουν τους υψηλότερους δείκτες ανάπτυξης, συμπεριλαμβάνονται στις υψηλά ανεπτυγμένες οικονομίες. Από αυτές, οι 12 είναι από την Ευρώπη, 2 στην Αμερική (Η.Π.Α. και Καναδάς), 3 στην Ανατολική Ασία (Δημοκρατία της Κορέας, Σιγκαπούρη και Ιαπωνία), 2 στην Ωκεανία (Αυστραλία και Νέα Ζηλανδία) και 1 στη Δυτική Ασία (Ισραήλ). Το σχήμα 2-5, παρουσιάζει τους δείκτες ανάπτυξης για καθεμία από αυτές τις 20 χώρες.

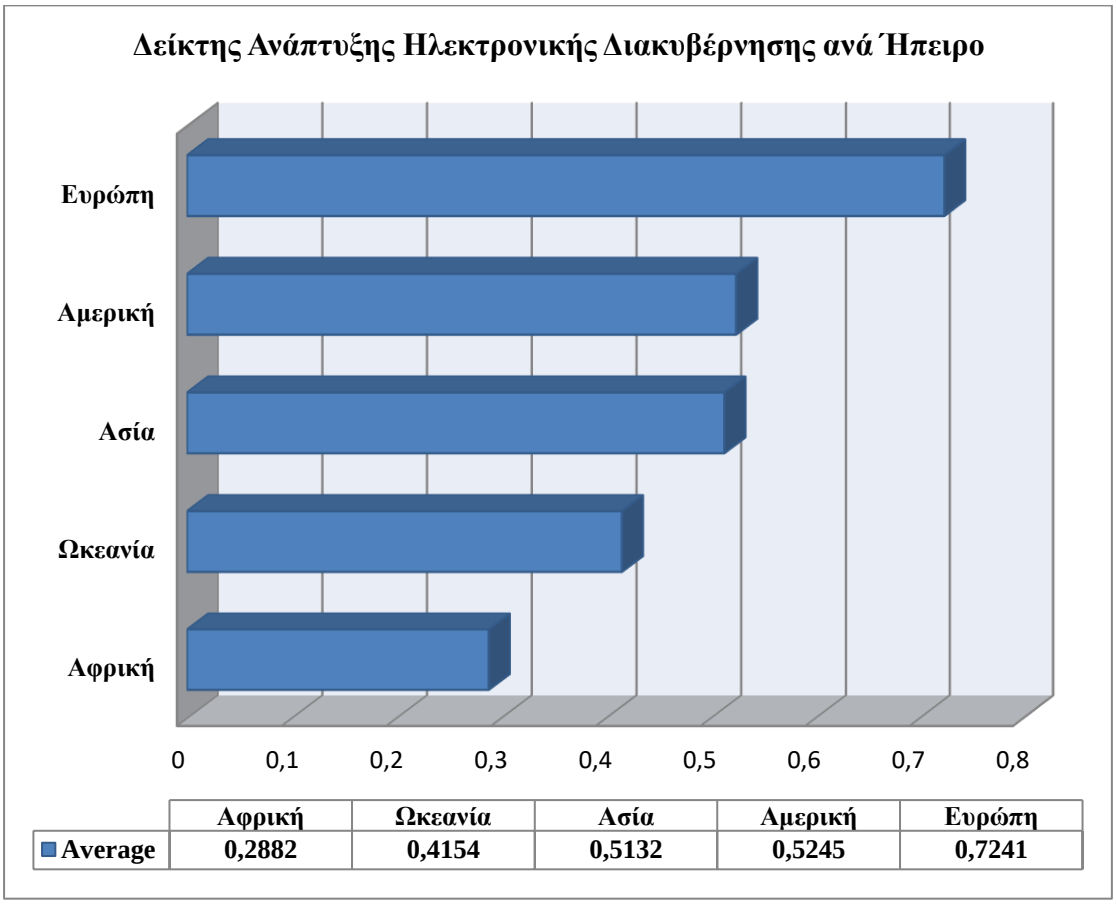


ΣΧΗΜΑ 2-5.ΔΕΙΚΤΗΣ ΑΝΑΠΤΥΞΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ 20 ΠΡΩΤΩΝ ΧΩΡΩΝ ΠΑΓΚΟΣΜΙΩΣ

(Πηγή: https://publicadministration.un.org/egovkb/en-us/Data/Compare-Countries)

Το Ηνωμένο Βασίλειο είναι ο παγκόσμιος ηγέτης στην ανάπτυξη (0,9193), ακολουθούμενο από την Αυστραλία (0,9143), τη Δημοκρατία της Κορέας (0,8915) και τη Σιγκαπούρη (0,8828), με την Φιλανδία, την Σουηδία, την Ολλανδία, την Νέα Ζηλανδία, την Δανία και την Γαλλία να βρίσκονται πιο πίσω. Σε σύγκριση με την αντίστοιχη έκθεση του 2014 (United Nations, 2014) παρατηρείται μια σταθερή βελτίωση των δεικτών ανάπτυξης σε παγκόσμιο επίπεδο, κάτι που οδήγησε σε αύξηση του μέσου όρου από 0,4712 σε 0,4922. Αυτή η αύξηση έρχεται να επιβεβαιώσει την αυξημένη προσπάθεια που παρατηρείται τα τελευταία χρόνια για παροχή υπηρεσιών Ηλεκτρονικής Διακυβέρνησης. Παρόλα αυτά όμως, παραμένει αρκετά μεγάλο το χάσμα που παρατηρείται μεταξύ των οικονομικά ανεπτυγμένων και μη κρατών, ιδιαίτερα στις χώρες της Αφρικής. Αυτή η διαφορά αποδίδεται κατά μεγάλο βαθμό στην έλλειψη τεχνολογικών υποδομών και διάδοσης της ευρυζωνικότητας καθώς και στο πολύ χαμηλό εισόδημα των πολιτών.

Σε επίπεδο ηπείρων τα σκήπτρα στην ανάπτυξη της Ηλεκτρονικής Διακυβέρνησης με μεγάλη διαφορά από την δεύτερη έχει η Ευρώπη (0,7241), γεγονός φυσιολογικό μιας και οι ευρωπαϊκές χώρες, συγκαταλέγονται μεταξύ των 50 κορυφαίων στην ανάπτυξη, ακολουθεί η Αμερική (0,5245), η Ασία (0,5132), την Ωκεανία (0,4154) και τελευταία η Αφρική (0,2882) όπως παρουσιάζεται στο σχήμα 2-6.



ΣΧΗΜΑ 2-6.ΔΕΙΚΤΗΣ ΑΝΑΠΤΥΞΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΑΝΑ ΉΠΕΙΡΟ

(Πηγή: https://publicadministration.un.org/egovkb/en-us/Data/Region-Information)

1.12 Η Ηλεκτρονική Διακυβέρνηση στην Ελλάδα

Κατά την διάρκεια των τελευταίων χρόνων η Ελληνική Δημόσια Διοίκηση βρίσκεται σε συνεχή αναδιάρθρωση και εκσυγχρονισμό προκειμένου να ανταπεξέλθει στις απαιτήσεις της ψηφιακής εποχής. Η αναδιοργάνωση αυτή στοχεύει στην εξυπηρέτηση του πολίτη και των επιχειρήσεων με καλύτερο και πιο αποτελεσματικό τρόπο.

Η προσπάθεια για την μετάβαση στην Ηλεκτρονική Διακυβέρνηση και την Κοινωνία της Πληροφορίας ξεκίνησε το 1994 με την υποστήριξη των Κοινοτικών Πλαισίων Στήριξης (ΚΠΣ) (Markellos, Markellou, Panayiotaki, & Stergianeli, 2007). Στην αρχή οι προσπάθειες επικεντρώθηκαν στην ανάπτυξη κυβερνητικών ιστοτόπων για την παροχή κυρίως πληροφοριακού υλικού. Το 1999 διαμορφώθηκε η Εθνική Στρατηγική που αφορούσε την προσέγγιση στην Ηλεκτρονική Διακυβέρνηση και την Κοινωνία της Πληροφορίας, δίνοντας έμφαση στην ποιότητα των παρεχόμενων υπηρεσιών και στο σχεδιασμό για το σύνολο της κοινωνίας, με στόχο τη διασφάλιση της κοινωνικής συνοχής και τη βελτίωση του βιοτικού επιπέδου (Gouscos, Georgiadis, & Sagris, 2000).

Η έναρξη της παροχής κάποιων υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, έγινε το 2002 (Hahamis, lles, & Healy, 2005). Όμως, η πολυπλοκότητα, η έλλειψη μηχανογράφησης και τεχνολογικών υποδομών, η χαμηλή απόδοση και το μικρό ποσοστό δαπανών για ΤΠΕ, που χαρακτηρίζουν τον Δημόσιο Τομέα στην Ελλάδα καθιστούν την εφαρμογή της Ηλεκτρονικής Διακυβέρνησης ιδιαίτερα δύσκολη (Κιοσσέ, 2011).

Το 2011 ψηφίστηκε στην Ελλάδα ο ν.3979/2011 για την ηλεκτρονική διακυβέρνηση, στον οποίο προβλέπονται, μεταξύ άλλων, η τήρηση ηλεκτρονικού πρωτοκόλλου από όλους τους φορείς του Δημοσίου, η νομική και αποδεικτική ισχύ των ηλεκτρονικών εγγράφων, ενώ θεσμοθετείται η ηλεκτρονική επικοινωνία μεταξύ φορέων της Δημόσιας Διοίκησης, φυσικών και νομικών προσώπων, αλλά και μεταξύ φορέων του Δημοσίου, και συστήνονται το Δίκτυο Δημόσιου Τομέα και η Ενιαία Αρχή Πληρωμής των Τηλεπικοινωνιακών Τελών του Δημοσίου.

Η Ελλάδα έχει μια διαμορφωμένη εθνική στρατηγική για την ηλεκτρονική διακυβέρνηση (Εθνική Στρατηγική για την Ηλεκτρονική Διακυβέρνηση), η οποία βασίζεται στις αρχές της ανταγωνιστικότητας, της παραγωγικότητας, της εξωστρέφειας, της ανάπτυξης και της απασχόλησης.

Οι κύριοι στόχοι της εθνικής στρατηγικής της Ελλάδας συνοψίζονται στα ακόλουθα σημεία (Παρασκευάς, Ασημακόπουλος, & Τριανταφύλλου, 2015):

- Παροχή του μέγιστου δυνατού αριθμού ψηφιακών υπηρεσιών προς τον πολίτη και την επιχείρηση, ειδικότερα «4ου ή 5ου επιπέδου», δηλαδή υπηρεσιών που

ολοκληρώνονται διαδικτυακά, χωρίς φυσική παρουσία του πολίτη στη Δημόσια Διοίκηση.

- Δημιουργία περιβάλλοντος πλήρους ψηφιακής συνεργασίας και επικοινωνίας μεταξύ των υπηρεσιών και των στελεχών της Δημόσιας Διοίκησης.
- Χρήση σύγχρονων υποδομών και διασφάλιση ποιοτικών και ασφαλών.

Το πλαίσιο ανάπτυξης της εθνικής στρατηγικής για την ηλεκτρονική διακυβέρνηση βασίζεται στις εξής τέσσερις προσεγγίσεις (Παρασκευάς και συν., 2015):

- **Προσέγγιση με επίκεντρο την πληροφορία** *(Data Oriented Approach)*: Η μετακίνηση από το σημερινό επίπεδο διαχείρισης εγγράφων προς μια νέα, πιο σύγχρονη πραγματικότητα είναι σημαντική για τη διαχείριση διακριτών τμημάτων πληροφορίας, ανοιχτών δεδομένων και περιεχομένου, τα οποία μπορούν εύκολα γίνουν αντικείμενο επεξεργασίας, να σημειωθούν, να χαρακτηριστούν, να διαμοιραστούν, να διασφαλιστούν και να παρουσιαστούν με τρόπο πολύ πιο χρήσιμο και κατανοητό για τον αποδέκτη αυτής της πληροφορίας.
- **Προσέγγιση κοινής πλατφόρμας** *(Shared Platform)*: Η κοινή πλατφόρμα συνεργασίας ανάμεσα στις διάφορες δομικές και λειτουργικές μονάδες του κράτους (υπουργεία, γενικές γραμματείες, διευθύνσεις, φορείς κτλ.) πρέπει να αποτελεί απαραίτητη προϋπόθεση, προκειμένου να μειωθούν οι δαπάνες, να προωθηθεί η ανάπτυξη, να εφαρμοστούν συνεκτικά πρότυπα και να διασφαλιστούν η δημιουργία και η παράδοση δεδομένων και πληροφοριών με συνοχή και αξιοπιστία.
- **Προσέγγιση με επίκεντρο τον τελικό χρήστη**: Από τις πληροφορίες που παρέχονται μέχρι το σύστημα διαχείρισης και τον τρόπο οργάνωσης, αλλά και την παρουσίαση, στο επίκεντρο πρέπει να βρίσκονται οι ανάγκες των πολιτών, των επιχειρήσεων και των στελεχών των δημόσιων φορέων, καθώς έτσι ποιοτικές πληροφορίες και υπηρεσίες θα είναι προσβάσιμες, ισχύουσες και ακριβείς οποιαδήποτε στιγμή τις χρειαστούν.

- **Προσέγγιση με επίκεντρο την ασφάλεια και την ιδιωτικότητα**: Ο σχεδιασμός της ψηφιακής ανάπτυξης δεν μπορεί να παραγνωρίσει τους κινδύνους που αφορούν εσκεμμένες επιθέσεις ή τυχαίες παραβιάσεις της ασφάλειας και της ιδιωτικότητας, είτε σε εφαρμογές είτε σε πληροφορία. Απέναντι σε αυτούς τους κινδύνους λαμβάνονται τα μέγιστα δυνατά μέτρα στη βάση των βέλτιστων διεθνών πρακτικών, τόσο από την πλευρά της τεχνολογίας, όσο και από την πλευρά της νομοθεσίας. Για να υποστηριχθούν η ανταλλαγή πληροφοριών και η συνεργασία, απαιτούνται σιγουριά και παράλληλα εγγύηση της ασφάλειας των δεδομένων σε ολόκληρο τον τεχνολογικό κύκλο ζωής (Δρογκάρης, 2013).

ΣΧΗΜΑ 2.7.ΠΥΛΩΝΕΣ ΑΝΑΠΤΥΞΗΣ ΤΗΣ ΕΘΝΙΚΗΣ ΣΤΡΑΤΗΓΙΚΗΣ ΓΙΑ ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

(Πηγή: (Παρασκευάς και συν., 2015))

1.13 Εξέλιξη 20 βασικών υπηρεσιών Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα

Τον Μάιο του 2013 δημοσιεύθηκαν από το Παρατηρητήριο για την Διοικητική Μεταρρύθμιση της Κοινωνίας της Πληροφορίας (ΚτΠ) τα αποτελέσματα της έρευνα που αποτύπωνε την εξέλιξη των 20 βασικών υπηρεσιών Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα. Πρόκειται για το σύνολο 20 υπηρεσιών που

αξιολογούνται σε ευρωπαϊκό επίπεδο βάσει κοινής μεθοδολογίας για λόγους συγκριτικής αξιολόγησης μεταξύ των κρατών – μελών, από τις οποίες οι 12 αφορούν τους πολίτες και οι 8 τις επιχειρήσεις. Στον Πίνακα 1-1 καταγράφονται αναλυτικά οι υπηρεσίες αυτές.

	Α/Α	**Δημόσια Υπηρεσία**	**Επίπεδο**	**Φορείς Δημοσίου που προσφέρουν τις υπηρεσίες**
ΥΠΗΡΕΣΙΕΣ ΠΡΟΣ ΠΟΛΙΤΕΣ	1	Φόρος εισοδήματος: δήλωση και ειδοποίηση εκκαθάρισης	5	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	2	Υπηρεσίες αναζήτησης εργασίας	4	Οργανισμός Απασχόλησης Εργατικού Δυναμικού (ΟΑΕΔ)
	3	Εισφορές κοινωνικής ασφάλισης	2,25[1]	Οργανισμός Απασχόλησης Εργατικού Δυναμικού (ΟΑΕΔ)
	4	Προσωπικά έγγραφα (διαβατήριο και άδεια οδήγησης)	3	Υπουργείο Δημοσίας Τάξης & Προστασίας του Πολίτη - Ελληνική Αστυνο-μία (διεύθυνση διαβατηρίων)/ Κέντρα Ενημέρωσης Πολιτών (ΚΕΠ)
	5	Καταχώρηση οχήματος (καινούρια, μεταχειρισμένα και εισαγόμενα αυτοκίνητα)	Δεν διατίθεται[2]	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	6	Έκδοση οικοδομικής άδειας	2	e- ΠΟΛΕΟΔΟΜΙΑ (Υπουργείο Περιβάλλοντος Ενέργειας & Κλιματικής Αλλα-γής (ΥΠΕΚΑ) & Υπουργείο Εσωτερικών (ΥΠΕΣ))
	7	Δήλωση προς την αστυνομία (π.χ., σε περίπτωση κλοπής)	1	Υπουργείο Δημοσίας Τάξης & Προστασίας του Πολίτη – Ελληνική Αστυνομία
	8	Δημόσιες βιβλιοθήκες (διαθεσιμότητα καταλόγων, εργαλεία αναζήτησης)	4	Υπουργείο Παιδείας & Θρη-σκευμάτων, Πολιτισμού & Αθλητισμού
	9	Πιστοποιητικά (γεννήσεως και γάμου): αίτηση και παραλαβή	3	Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ)
	10	Εισαγωγή στην ανώτατη εκπαίδευση	2	Υπουργείο Παιδείας & Θρη-σκευμάτων, Πολιτισμού & Αθλητισμού
	11	Ανακοίνωση μετακόμισης (αλλαγή διεύθυνσης)	4	Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ)
	12	Υπηρεσίες υγείας (διαθεσιμότητα υπηρεσιών και κλείσιμο ραντεβού)	2	Υπουργείο Υγείας

	Α/Α	Δημόσια Υπηρεσία	Επίπεδο	Φορείς Δημοσίου που προσφέρουν τις υπηρεσίες
ΥΠΗΡΕΣΙΕΣ ΠΡΟΣ ΕΠΙΧΕΙΡΗΣΕΙΣ	13	Εισφορές κοινωνικής ασφάλισης για τους εργαζομένους	4	Ίδρυμα Κοινωνικών Ασφαλίσεων (ΙΚΑ)
	14	Φόρος επιχειρήσεων: δήλωση και ειδοποίηση εκκαθάρισης	4	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	15	ΦΠΑ: δήλωση και ειδοποίηση εκκαθάρισης	4	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	16	Έναρξη επιχείρησης	2	Γενική Γραμματεία Εμπορίου (ΓΓΕ)
	17	Υποβολή στοιχείων σε Στατιστικές υπηρεσίες	4	Ελληνική Στατιστική Αρχή (ΕΛ.ΣΤΑΤ.)
	18	Τελωνειακές διασαφήσεις	4	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	19	Περιβαλλοντικές άδειες	2	Υπουργείο Περιβάλλοντος, Ενέργειας & Κλιματικής Αλλαγής/ Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ)
	20	Δημόσιες Προμήθειες	2	Γενική Γραμματεία Εμπορίου (ΓΓΕ)

ΠΙΝΑΚΑΣ 1-1.ΒΑΣΙΚΕΣ ΔΗΜΟΣΙΕΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΗΡΕΣΙΕΣ

(Πηγή: (Παρατηρητήριο για τη Διοικητική Μεταρρύθμιση, 2013)

[1] Στις Εισφορές κοινωνικής ασφάλισης περιλαμβάνονται 4 επιμέρους υπηρεσίες. Καθώς οι υπηρεσίες αυτές έχουν διαφορετικό επίπεδο ηλεκτρονικής διακυβέρνησης, σαν συνολική επίδοση υπολογίζεται ο μέσος όρος των επιμέρους επιδόσεων. Αντίστοιχα και για την υπηρεσία Προσωπικά Έγγραφα, όπου περιλαμβάνει υπηρεσίες, την έκδοση διαβατηρίου και την άδεια οδήγησης.

[2] Η υπηρεσία «Δήλωση Αυτοκινήτου», παρέχονταν μέσω της ιστοσελίδας της ΓΓΠΣ και ήταν πλήρως διαθέσιμη ηλεκτρονικά (υπηρεσία «e-Οχήματα»), πλέον είναι εκτός λειτουργίας. Ωστόσο τα στοιχεία χρησιμοποιούνται από τη ΓΓΠΣ για την έκδοση των τελών κυκλοφορίας..

ΚΕΦΑΛΑΙΟ 2

«ΘΕΜΑΤΑ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΙΣ ΥΠΗΡΕΣΙΕΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ»

2.1 Ιδιωτικότητα πληροφοριών σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης

Σύμφωνα με το Πλαίσιο Ψηφιακής Αυθεντικοποίησης (ΠΗΔ, 2012) η αξιοποίηση υπηρεσιών ηλεκτρονικής διακυβέρνησης απαιτεί συλλογή και επεξεργασία διαφορετικού είδους πληροφοριών, όπως προσωπικών δεδομένων, των οποίων η προστασία, επεξεργασία και μη αποκάλυψη και δημοσιοποίηση αποτελεί βασική κανονιστική απαίτηση, σύμφωνα με τις ειδικότερες προϋποθέσεις και εγγυήσεις της σχετικής νομοθεσίας (ν. 2472/97), που πρέπει να εκπληρώνεται από τις υπηρεσίες ηλεκτρονικής διακυβέρνησης (OECD, 2013).

Η συνταγματική και έννομη τάξη αναγνωρίζει την πληροφοριακή ιδιωτικότητα (informational privacy) ως το δικαίωμα και τη δυνατότητα του ατόμου να γνωρίζει, να ελέγχει και καταρχήν να προσδιορίζει τη χρήση των προσωπικών πληροφοριών του από άλλες οντότητες, ιδιώτες και κράτος. Ως ιδιωτικότητα ορίζεται η μη αποκάλυψη προσωπικών πληροφοριών σε μη εξουσιοδοτημένες οντότητες η οποία αποτελεί βασική παράμετρο της σχετικής νομοθεσίας που αναγνωρίζεται ρητά (άρθρο 10 ν.2472/97), ενώ η παραβίασή της τιμωρείται και με ποινικές κυρώσεις (άρθρο 22 § 4 ν. 2472/97). Το δικαίωμα στην ιδιωτικότητα αναφέρεται στη δυνατότητα ελέγχου της χρήσης των προσωπικών πληροφοριών.

Ως δεδομένα προσωπικού χαρακτήρα ή προσωπικά δεδομένα νοείται κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων, δηλαδή στο φυσικό πρόσωπο, στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική (άρθρο 2α σε συνδυασμό με άρθρο 2γ του ν. 2472/97). Δεν λογίζονται ως δεδομένα προσωπικού

χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων. Στον όρο "προσωπικά δεδομένα" περιλαμβάνονται και αυτά τα οποία χρησιμοποιούνται συνήθως για τον προσδιορισμό της ταυτότητας του προσώπου. Με το σύνηθες προσδιοριστικό της ταυτότητας ενός προσώπου, το όνομα, μπορούν να εξομοιωθούν ο αριθμός της κοινωνικής ασφάλισης, ο αριθμός του δελτίου ταυτότητας, ο αριθμός πελάτη και άλλα παρόμοια στοιχεία. Ως στοιχεία που δηλώνουν την ταυτότητα ενός προσώπου έχουν γίνει αποδεκτά και νομιμοποιητικά στοιχεία που αποδίδονται σε πρόσωπα ή επιλέγονται από αυτά (π.χ. κωδικός αναγνώρισης ή πρόσβασης, αριθμός PIN κ.α.).

Οι προσωπικές πληροφορίες μπορεί να αφορούν τις σχέσεις ενός προσώπου προς πρόσωπα ή τις σχέσεις προς πράγματα. Σε αυτές τις σχέσεις αντιστοιχούν πληροφορίες τόσο για τα εξωτερικά στοιχεία όσο και για ψυχικές καταστάσεις (απόψεις, κίνητρα, επιθυμίες), ενέργειες, αντιδράσεις, τρόπους συμπεριφοράς, ανεξάρτητα από το αν αφορούν το παρόν ή το παρελθόν και πόσο ανατρέχουν σε αυτό. Είναι αναμφισβήτητο ότι στις πληροφορίες προσωπικού χαρακτήρα εντάσσονται και οι σχέσεις προς το περιβάλλον. ως τέτοιες νοούνται, για παράδειγμα, στοιχεία για την περιουσιακή κατάσταση, για την επαγγελματική και οικονομική δραστηριότητα, την οικογενειακή κατάσταση, τις προσωπικές δραστηριότητες και σχέσεις (συνήθειες του ελεύθερου χρόνου, συμμετοχή και δραστηριοποίηση σε ενώσεις, καταναλωτική συμπεριφορά) καθώς και για τις σχέσεις και καταστάσεις ιδιωτικού και δημοσίου δικαίου (ιδιοκτησία, συμβατικές σχέσεις, διοικητικές άδειες κλπ.).

Ως ευαίσθητα προσδιορίζονται σαφώς στο νόμο (άρθρο 2β του ν. 2472/97, όπως ισχύει) τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων.

2.2 Απαιτήσεις ασφαλείας και ιδιωτικότητας δεδομένων

Οι απαιτήσεις ασφαλείας και ιδιωτικότητας των δεδομένων, οι οποίες αξιοποιούνται σε πληροφοριακά συστήματα και οι οποίες προκύπτουν από την ανάγκη προστασίας τους περιλαμβάνουν τα εξής (Γκρίτζαλης, Γκρίτζαλης, & Κάτσικας, 2004) (ISO/IEC 27001, 2013):

- ***Εμπιστευτικότητα (Confidentiality):*** που αφορά την προστασία από τη διάδοση και μεταφορά των δεδομένων σε οντότητες που είναι εξουσιοδοτημένες.

- ***Ακεραιότητα (Integrity):*** που αφορά την προστασία από εισαγωγή, τροποποίηση η διαγραφή δεδομένων, η οποία δεν είναι εξουσιοδοτημένη.

- ***Διαθεσιμότητα (Availability):*** που αφορά στην εξασφάλιση της ταυτότητας όλων των εμπλεκομένων οντοτήτων.

- ***Μη αποποίηση (Non Repudiation):*** που αφορά την προστασία από το να αρνηθεί μια οντότητα να πραγματοποίηση συγκεκριμένη δραστηριότητα.

Περισσότερα σχετικά με την ασφάλεια των πληροφοριών θα δούμε αναλυτικότερα στο επόμενο κεφάλαιο.

Η ιδιωτικότητα από γενική έννοια μετατρέπεται σε τεχνική απαίτηση με καθορισμό των επιμέρους απαιτήσεων ιδιωτικότητας, που είναι οι εξής (Cannon, 2004; Καλλονιάτης, 2011):

- ***Αυθεντικοποίηση (Authentication):*** η διαδικασία μέσω της οποίας επιβεβαιώνεται η ταυτότητα μιας οντότητας. Αποτελεί κυρίως απαίτηση ασφάλειας, παρά ιδιωτικότητας μιας υπηρεσίας Ηλεκτρονικής Διακυβέρνησης, ωστόσο έχει σημαντική συνεισφορά και στην ικανοποίηση απαιτήσεων ιδιωτικότητας.

- ***Εξουσιοδότηση (Authorization):*** η διαδικασία μέσω της οποίας μία οντότητα αποκτά δικαιώματα – πρόσβαση σε μια μεμονωμένη υπηρεσία ή σε συγκεκριμένες υπηρεσίες ενός πληροφοριακού συστήματος. που αφορά την

εξασφάλιση ότι κάθε οντότητα έχει πρόσβαση σε εκείνους τους πόρους του συστήματος που της έχει επιτραπεί η είσοδος.

- ***Αναγνώριση (Identification):*** η διαδικασία μέσω της οποίας ελέγχεται αν η υπηρεσία ή τα δεδομένα που ζητούνται απαιτούν αυθεντικοποίηση και στη συνέχεια εξουσιοδότησή της ή όχι.

- ***Προστασία Δεδομένων (Data Protection):*** η διαδικασία μέσω της οποίας διασφαλίζονται, σύμφωνα και με την Ευρωπαϊκή Οδηγία 1995/46/ΕΚ, οι κάτωθι αρχές:

  - Αρχή της νομιμότητας και της δικαιοσύνης.
  - Αρχή του καθορισμού του σκοπού της συλλογής των δεδομένων και της επεξεργασίας αυτών για το σκοπό που συλλέχθηκαν.
  - Αρχή της αναγκαιότητας της συλλογής και επεξεργασίας των δεδομένων.
  - Παροχή πληροφόρησης, ενημέρωσης και πρόσβασης στους κατόχους των δεδομένων.
  - Αρχή της ασφάλειας και της ακεραιότητας.
  - Εποπτεία και Επικύρωση.

- ***Ανωνυμία (Anonymity):*** η διαδικασία μέσω της οποίας διασφαλίζεται ότι μία οντότητα μπορεί να χρησιμοποιήσει μια υπηρεσία ή να επικοινωνήσει με μια άλλη οντότητα χωρίς να αποκαλύψει της ταυτότητά του.

- ***Ψευδωνυμία (Pseydonymity):*** η διαδικασία μέσω της οποίας προστατεύεται η αναγνώριση (Identification) μιας οντότητας από μη εξουσιοδοτημένες τρίτες οντότητες.

- ***Μη-συνδεσιμότητα (Unlinkability):*** η διαδικασία μέσω της οποίας προστατεύεται η ιδιωτικότητα μιας οντότητας από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να συνδέσουν τμήματα σχετικών

πληροφοριών μεταξύ τους, οδηγώντας έτσι στην αποκάλυψη της ταυτότητάς της.

- ***Μη-παρατηρησιμότητα (Unbservability):*** η διαδικασία μέσω της οποίας προστατεύεται η ιδιωτικότητα μιας οντότητας από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να παρατηρήσουν ή να εντοπίσουν ίχνη της πρώτης.

2.3 Αρχές προστασίας της ιδιωτικότητας

Το1980, ο ΟΟΣΑ ενέκρινε τις κατευθυντήριες γραμμές για την προστασία της ιδιωτικής ζωής και των διασυνοριακών ροών δεδομένων προσωπικού χαρακτήρα ("κατευθυντήριες γραμμές του 1980") προκειμένου να αντιμετωπίσει τις ανησυχίες που απορρέουν από την αυξημένη χρήση προσωπικών δεδομένων και τον κίνδυνο για τις παγκόσμιες οικονομίες που προκύπτει από περιορισμούς στη ροή πληροφοριών πέρα από τα σύνορα. Οι κατευθυντήριες γραμμές του 1980, που περιείχαν το πρώτο διεθνώς συμφωνημένο σύνολο αρχών προστασίας της ιδιωτικής ζωής, επηρέασαν τη νομοθεσία και την πολιτική στις χώρες μέλη του ΟΟΣΑ και πέραν αυτού ήταν οι εξής (OECD, 1980):

- ***Αρχή περιορισμού της συλλογής (Collection Limitation Principle):*** Θα πρέπει να υπάρχουν όρια στην συλλογή προσωπικών δεδομένων ενώ θα πρέπει να συλλέγονται με νόμιμα και θεμιτά μέσα και όπου ενδείκνυται, με τη γνώση ή τη συναίνεση του χρήστη.

- ***Αρχή ποιότητας των δεδομένων (Data Quality Principle):*** Τα προσωπικά δεδομένα θα πρέπει να είναι συναφή με τους σκοπούς για τους οποίους πρόκειται να χρησιμοποιηθούν και στο μέτρο που είναι απαραίτητο για τους σκοπούς αυτούς, να είναι ακριβή, πλήρη και ενημερωμένα.

- ***Αρχή προσδιορισμού του σκοπού (Purpose Specification Principle):*** Οι σκοποί για τους οποίους συλλέγονται δεδομένα προσωπικού χαρακτήρα πρέπει να προσδιορίζονται το αργότερο κατά τη στιγμή της συλλογής των δεδομένων και η επακόλουθη χρήση να περιορίζεται στην εκπλήρωση των

σκοπών αυτών ή σε άλλους που δεν είναι ασυμβίβαστοι με τους σκοπούς αυτούς και όπως προσδιορίζονται σε κάθε περίπτωση αλλαγής σκοπό.

- ***Αρχή περιορισμού της χρήσης (Use Limitation Principle):*** Τα προσωπικά δεδομένα δεν πρέπει να αποκαλύπτονται, να διατίθενται ή να χρησιμοποιούνται για άλλο σκοπό από τον προσδιορισμένο σύμφωνα με την αρχή προσδιορισμού του σκοπού, εκτός από αν υπάρχει: α) η συγκατάθεση του υποκειμένου των δεδομένων ή β) εξουσιοδότηση από τον νόμο.

- ***Αρχή προστασίας της ασφάλειας (Security Safeguards Principle):*** Τα προσωπικά δεδομένα θα πρέπει να προστατεύονται με κατάλληλους μηχανισμούς ασφαλείας έναντι κινδύνων όπως είναι: η απώλεια, η μη εξουσιοδοτημένη πρόσβαση, η καταστροφή, η χρήση, η τροποποίηση ή αποκάλυψη δεδομένων.

- ***Αρχή της διαφάνειας (Openness Principle):*** Θα πρέπει να υπάρχει μια γενική πολιτική διαφάνειας όσον αφορά τις πρακτικές και τις πολιτικές που σχετίζονται με την συλλογή των προσωπικών δεδομένων. Επίσης θα πρέπει να είναι διαθέσιμα άμεσα μέσα για τη διαπίστωση της ύπαρξης και της φύσης των προσωπικών δεδομένων και των κύριων σκοπών χρήσης τους, καθώς και της ταυτότητας και της έδρας του υπεύθυνου φορέα ο οποίος επεξεργάζεται τα δεδομένα.

- Αρχή της ατομικής συμμετοχής (Openness Principle): Το κάθε άτομο θα πρέπει να έχει το δικαίωμα:

    1. Να μπορεί να λάβει από τον ίδιο τον υπεύθυνο επεξεργασίας δεδομένων ή με άλλο τρόπο επιβεβαίωση αναφορικά με το αν ο υπεύθυνος επεξεργασίας διαθέτει δεδομένα σχετικά με αυτό.

    2. Να του κοινοποιούνται δεδομένα σχετικά με αυτό, εντός εύλογου χρονικού διαστήματος, με εύλογο τρόπο, σε μορφή που είναι ευκόλως κατανοητή ενώ σε περίπτωση επιβάρυνσης, εάν υπάρχει, αυτή δεν θα είναι υπερβολική.

3. Σε περίπτωση που η αίτηση που υποβλήθηκε δυνάμει των παραγράφων 1 και 2 απορρίπτεται θα πρέπει να αιτιολογείται και να δίνεται δυνατότητα περαιτέρω διεκδίκησης και αμφισβήτησης της απόρριψης.

4. Να έχει την δυνατότητα να αμφισβητήσει τα δεδομένα που σχετίζονται με αυτό και εάν η αμφισβήτηση είναι επιτυχής να μπορεί να διαγραφούν, διορθωθούν, συμπληρωθούν ή τροποποιηθούν.

- ***Αρχή της ευθύνης (Safeguards Principle):*** Ο υπεύθυνος επεξεργασίας προσωπικών δεδομένων θα πρέπει να είναι υπεύθυνος για τη συμμόρφωση με τα μέτρα που θέτουν σε εφαρμογή οι προαναφερόμενες αρχές.

Οι παραπάνω κατευθυντήριες γραμμές ήταν γραμμένες σε μια συνοπτική, τεχνολογικά ουδέτερη γλώσσα, ενώ έχουν αποδειχθεί εξαιρετικά προσαρμόσιμες στις τεχνολογικές και κοινωνικές αλλαγές. Ωστόσο, οι αλλαγές στη χρήση των προσωπικών δεδομένων καθώς και οι νέες προσεγγίσεις για την προστασία της ιδιωτικής ζωής, δημιούργησαν την ανάγκη ενημέρωσης τους το 2013 σε πολλά σημαντικά σημεία (OECD, 2013).

Οι νέες κατευθυντήριες γραμμές αποτελούν την πρώτη επικαιροποίηση της αρχικής έκδοσης του 1980 που αποτέλεσε το πρώτο διεθνώς συμφωνημένο σύνολο αρχών προστασίας της ιδιωτικής ζωής. Δύο θέματα εξετάζονται μέσω των ενημερωμένων οδηγιών (OECD, 2013):

- η εστίαση στην πρακτική εφαρμογή της προστασίας της ιδιωτικής ζωής μέσω μιας προσέγγισης που βασίζεται στη διαχείριση κινδύνων, και

- η ανάγκη αντιμετώπισης της παγκοσμιοποίησης της ιδιωτικότητας μέσω βελτιωμένης διαλειτουργικότητας.

Ενώ εισάγονται ορισμένες νέες έννοιες, όπως:

- ***Εθνικές στρατηγικές προστασίας της ιδιωτικής ζωής***. Ενώ οι νόμοι είναι απαραίτητοι, η στρατηγική σημασία της προστασίας της ιδιωτικής ζωής σήμερα απαιτεί επίσης μια πολύπλευρη εθνική στρατηγική συντονισμένη στα υψηλότερα επίπεδα διακυβέρνησης.

- ***Προγράμματα διαχείρισης απορρήτου***. Αυτά λειτουργούν ως ο βασικός λειτουργικός μηχανισμός μέσω του οποίου οι οργανισμοί εφαρμόζουν την προστασία της ιδιωτικής ζωής.

- ***Ειδοποίηση παραβίασης ασφάλειας δεδομένων***. Η διάταξη αυτή καλύπτει τόσο την ειδοποίηση προς μια αρχή όσο και την ειδοποίηση ενός ατόμου που έχει πληγεί από παραβίαση ασφαλείας που επηρεάζει τα προσωπικά δεδομένα.

2.4 Νομικό πλαίσιο προσωπικών δεδομένων

Παρακάτω παρατίθενται περιληπτικά σε πίνακες το νομικό πλαίσιο που ισχύει τόσο σε Ευρωπαϊκό όσο και Ελληνικό επίπεδο.

2.4.1. Ευρωπαϊκή Νομοθεσία

Συνοπτικά, η Ευρωπαϊκή Νομοθεσία σχετικά με την προστασία των προσωπικών δεδομένων, δίνεται στον Πίνακα 2-1, όπου καταγράφονται όλες οι εκδοθείσες οδηγίες καθώς επίσης και ο σκοπός έκδοσης τους. Η ανάπτυξη της πρώτης Ευρωπαϊκής Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Ευρωπαϊκό Κοινοβούλιο, 1995) στηρίχτηκε στις βασικές αρχές του 1980 και αποτέλεσε για πολλά χρόνια οδηγός για την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων όσον αφορά τις δραστηριότητες επεξεργασίας και τη διασφάλιση της ελεύθερης κυκλοφορίας δεδομένων προσωπικού χαρακτήρα μεταξύ κρατών μελών.

Νόμοι	Αντικείμενο έκδοσης
Ευρωπαϊκή Ένωση	Συνθήκη για την Ευρωπαϊκή Ένωση (Άρθρο 6) Ευρωπαϊκή Σύμβαση των δικαιωμάτων του Ανθρώπου (Άρθρο 8) Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (Άρθρο 8)

Οδηγία 95/46/ΕΚ	Για την προστασία των φυσικών προσώπων έναντι της επεξεργασία δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών
Οδηγία 2002/58/ΕΚ	Για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Βλ. κατωτέρω τροποποίηση της, δια της Οδηγίας 2009/136/ΕΚ
Οδηγία 2006/24/ΕΚ	Για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ
Οδηγία 2009/136/ΕΚ	Για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών
Κανονισμός (ΕΕ) 2016/679	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)
Οδηγία (ΕΕ) 2016/680	Για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου
Οδηγία (ΕΕ) 2016/681	Σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων

ΠΙΝΑΚΑΣ 2-1.ΕΥΡΩΠΑΪΚΗ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

(Πηγή: (ΑΠΔΠΧ, 2016))

2.4.2. Ο Νέος Κανονισμός Ε.Ε. 2016/679 για την προστασία των Προσωπικών Δεδομένων

Αν και η οδηγία 95/46/ΕΚ έπρεπε να εφαρμοστεί από κάθε κράτος μέλος για την προστασία των δεδομένων και είχε στόχο ένα εναρμονισμένο και σύγχρονο

καθεστώς προστασίας δεδομένων σε ολόκληρη την Ευρώπη ο στόχος δεν επιτεύχθηκε πλήρως λόγω των διαφορών στις διάφορες εθνικές εφαρμογές (Hansen, 2016).

Το 2016, περισσότερο από 20 χρόνια αργότερα, ο διάδοχος της οδηγίας για την προστασία των δεδομένων εγκρίθηκε μετά από αρκετά χρόνια συζήτησης και διαπραγμάτευσης ο οποίος ονομάστηκε Γενικός Κανονισμός Προστασίας Δεδομένων – General Data Protection Regulation (GDPR) (Regulation, 2016) με κύριους στόχους ξανά της εναρμόνισης και του εκσυγχρονισμού που επιδιωκόταν. Το GDPR θα τεθεί σε ισχύ στις 25 Μαΐου 2018. Η άμεση εφαρμογή του σε όλα τα κράτη μέλη θα συμβάλει στην ενοποίηση του επιπέδου προστασίας δεδομένων. Ωστόσο, οι περίπου 70 ρήτρες – άλλες υποχρεωτικές και άλλες προαιρετικές – παρέχουν τα μέσα για τις δικές τους εθνικές απαιτήσεις και ως εκ τούτου απόκλιση από μια κοινή στρατηγική σε όλα τα κράτη μέλη (Roßnagel & Nebel, 2016).

Το περιεχόμενο του κανονισμού οργανώνεται ως εξής: Στο 2ο τμήμα του σκιαγραφούνται οι σημαντικές ιδιότητες του Ευρωπαϊκού Κανονισμού για την Γενική Προστασία Δεδομένων που απορρέει από την ευρωπαϊκή πρωτοβουλία μεταρρύθμισης της προστασίας δεδομένων. Στο 3ο τμήμα παρουσιάζεται η έννοια της "προστασίας της ιδιωτικής ζωής από σχεδιασμό" και παρέχει σύντομες πληροφορίες για το ιστορικό και τους ορισμούς. Στο 4ο και 5ο τμήμα απαριθμούνται οι νομικές υποχρεώσεις σχετικά με την προστασία των δεδομένων από το σχεδιασμό και την προστασία των δεδομένων. Τέλος, στο 6ο και τελευταίο τμήμα συνοψίζονται τα συμπεράσματα και δίνεται ένας επίλογος (Hansen, 2016).

Θα πρέπει να σημειωθεί στο σημείο αυτό ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων δεν αποτελεί πανάκεια για την προστασία των δεδομένων, εξάλλου δεν είναι όλα καινούργια στον κανονισμό ενώ τα 99 άρθρα του αφήνουν περιθώρια για ερμηνεία. Η επιλεγμένη αφαίρεση νομικού κειμένου από τον κανονισμό είναι ένα επιδιωκόμενο χαρακτηριστικό και όχι ένα σφάλμα: Οι αφηρημένοι κανόνες πρέπει να τεκμηριώνονται με τέτοιο τρόπο έτσι ώστε να είναι κατάλληλοι σε σχέση με τους συνεχώς μεταβαλλόμενους κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και να είναι αποδεκτοί ως εποπτικές αρχές από τους Ευρωπαίους επιτρόπους προστασίας δεδομένων. Έτσι, ο Γενικός Κανονισμός Προστασίας Δεδομένων ορίζει μια διαδικασία για την

επίτευξη συνεκτικής ερμηνείας των νομικών υποχρεώσεων που αφορούν τις περιπτώσεις διασυνοριακών συναλλαγών. Με αυτό, ο κανονισμός μπορεί να καταφέρει να είναι ανθεκτικός στο μέλλον για πολλά χρόνια ή ακόμα και πολλές δεκαετίες - σε αντίθεση με τον προκάτοχό του. Ωστόσο, η συνεχής διαπραγμάτευση σχετικά με την τεκμηρίωση των αφηρημένων κανόνων είναι χρονοβόρα και ενδέχεται να επηρεαστούν από ομάδες πίεσης που δεν μοιράζονται τον ίδιο στόχο σχετικά με την βέλτιστη προστασία των δεδομένων (Hansen, 2016).

Πρέπει να σημειωθεί ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων δεν απευθύνεται μόνο σε ευρωπαίους υπευθύνους επεξεργασίας δεδομένων, αλλά αποσκοπεί στην εξασφάλιση της προστασίας των δεδομένων σε ολόκληρη την ευρωπαϊκή αγορά. Η αρχή της θέσης της αγοράς που ορίζεται στο άρθρο 3 του κανονισμού απευθύνεται σε οργανισμούς που προσφέρουν αγαθά ή υπηρεσίες σε άτομα στην ΕΕ ή παρακολουθούν τη συμπεριφορά τους, ακόμη και αν οι οργανώσεις δεν είναι εγκατεστημένες στην επικράτεια της Ευρωπαϊκής Ένωσης. Συγκεκριμένα, οι εταιρείες που δεν είναι μέλη της ΕΕ και κυριαρχούν στην ψηφιακή αγορά πρέπει να συμμορφώνονται με τις απαιτήσεις προστασίας των δεδομένων του κανονισμού (Hansen, 2016).

Εάν ο Γενικός Κανονισμός Προστασίας Δεδομένων θα παράσχει τα κατάλληλα μέσα για την επίτευξη της προστασίας δεδομένων δεν μπορεί να προβλεφθεί σε αυτό το πρώιμο στάδιο. Ωστόσο, σαφώς τα ευρωπαϊκά κράτη μέλη έχουν ένα κοινό σημείο εκκίνησης να το πάρουν από εκεί. Αυτό ισχύει για όλα τα όργανα που περιγράφονται στον κανονισμό π.χ. η προστασία δεδομένων από το σχεδιασμό, η προστασία των δεδομένων από προεπιλογή, η αξιολόγηση των επιπτώσεων στην προστασία δεδομένων, οι κώδικες δεοντολογίας, οι πιστοποιήσεις, οι κυρώσεις ή η εμπλοκή των δικαστηρίων (Hansen, 2016).

2.4.3. Ελληνική Νομοθεσία

Η Ελλάδα είναι μία από τις πρώτες χώρες που προσάρτησαν την κοινοτική Οδηγία 95/46/ΕΚ στο εσωτερικό δίκαιο. Από το 1985 είχαν εκπονηθεί προσχέδια νόμου και είχαν κατατεθεί στο κοινοβούλιο προτάσεις και σχέδια νόμου των οποίων όμως η ψήφιση δεν ολοκληρώθηκε (Μήτρου, 2010). Συνοπτικά η

Ελληνική Νομοθεσία σχετικά με την προστασία των προσωπικών δεδομένων, δίνεται στο Πίνακα 2-2, όπου καταγράφονται όλοι οι Νόμοι που έχουν εκδοθεί, καθώς επίσης και το αντικείμενο έκδοσης τους.

Νόμοι	Αντικείμενο έκδοσης
Νόμος 2472/1997	Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Αντικείμενο του Νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, έτσι ώστε να προστατεύονται τα δικαιώματα και οι θεμελιώδεις ελευθερίες των φυσικών προσώπων και κυρίως της ιδιωτικής ζωής (Άρθρο 1)
Νόμος 3051/2002	Συνταγματικά κατοχυρωμένες ανεξάρτητες Αρχές, τροποποίηση και συμπλήρωση του συστήματος προσλήψεων στο δημόσιο τομέα και συναφείς ρυθμίσεις
Νόμος 3471/2006	Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν.2472/97
Νόμος 3783/2009	Ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας και άλλες διατάξεις. Σκοπός του νόμου είναι η ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας προπληρωμένου χρόνου ομιλίας, συνδρομητών με συμβόλαιο, ή άλλης μορφής κινητής τηλεπικοινωνίας, για λόγους εθνικής ασφάλειας και για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. (Άρθρο 1).
Νόμος 3917/2011	Ενσωμάτωση της Οδηγίας 2006/24/ΕΚ του Ευρωπαϊκού κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου, για την διατήρηση δεδομένων που επεξεργάζονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών και για την τροποποίηση της Οδηγίας 2002/58/ΕΚ. Αντικείμενο και πεδίο εφαρμογής είναι η διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις. (Άρθρο 1)
Νόμος 4070/2012	Αφορά τις ρυθμίσεις ηλεκτρονικών επικοινωνιών, μεταφορών, δημοσίων έργων και άλλες διατάξεις

ΠΙΝΑΚΑΣ 2-2.ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

(Πηγή: (ΑΠΔΠΧ, 2016))

2.5 Βασικές υποχρεώσεις της Διοίκησης για την διασφάλιση της Ιδιωτικότητας

Οι βασικές υποχρεώσεις της Διοίκησης σχετικά με τη διασφάλιση της Ιδιωτικότητας όταν παρέχονται υπηρεσίες Ηλεκτρονικής Διακυβέρνησης με χρήση δεδομένων προσωπικού χαρακτήρα, είναι (ΠΗΔ, 2012):

1. Κατά τη συλλογή και επεξεργασία δεδομένων θα πρέπει να λαμβάνεται πρόνοια ώστε να υπάρχει σαφής προσδιορισμός και διαχωρισμός των δεδομένων προσωπικού και στατιστικού χαρακτήρα.

2. Θα πρέπει να διασφαλίζεται, με διαδικασίες ανωνυμοποίησης/ πολλαπλής κωδικοποίησης, ότι από τα δεδομένα στατιστικού χαρακτήρα δεν είναι δυνατός ο προσδιορισμός της ταυτότητας των φυσικών προσώπων.

3. Με εγκυκλίους και άλλα μέσα ενημέρωσης-εκπαίδευσης θα πρέπει να καταστούν γνωστές και σαφείς στους δημόσιους υπαλλήλους οι κατηγορίες των ευαίσθητων δεδομένων για να αποφευχθεί σχετική σύγχυση (π.χ. παρατηρείται σχετική σύγχυση μεταξύ των δεδομένων που αφορούν φυλετική ή εθνική προέλευση (φυλετική ή εθνική μειονότητα) που συνιστούν ευαίσθητα δεδομένα και αυτών που αφορούν την ιθαγένεια που συνιστούν απλά δεδομένα).

Σε περίπτωση προσφυγής σε εξωτερικούς ιδιωτικούς φορείς για την αποθήκευση και πρόσβαση σε προσωπικά δεδομένα χρήστη:

1. Θα πρέπει να περιλαμβάνονται στη σχετική σύμβαση όροι για τη συλλογή και επεξεργασία δεδομένων.

2. Θα ήταν χρήσιμο ένα ενιαίο πρότυπο συμβατικών όρων που θα προσδιορίζουν τις υποχρεώσεις των τρίτων ως προς τη συλλογή και χρήση προσωπικών δεδομένων. Οι πρότυποι όροι θα μπορούσαν να χρησιμοποιηθούν από τις υπηρεσίες με τις αναγκαίες κατά περίπτωση προσαρμογές.

3. Σε περίπτωση ανάθεσης της παροχής υπηρεσιών ηλεκτρονικής διακυβέρνησης σε τρίτους, εφόσον οι υπηρεσίες αυτές προϋποθέτουν ή/και συνεπάγονται συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα, η αναλυτική

περιγραφή και ποιότητα των πολιτικών εφαρμογής των κανόνων προστασίας και των πολιτικών/μέτρων ασφάλειας θα έπρεπε να αναχθεί σε κριτήριο επιλογής αναδόχου ή/και όρο ανάθεσης.

ΚΕΦΑΛΑΙΟ 3

«ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ & ΣΥΣΤΗΜΑΤΑ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ»

3.1 Εισαγωγή στην ασφάλεια των πληροφοριών

Το κεφάλαιο αυτό ξεκινάει με το εξής ερώτημα: Τι είναι η ασφάλεια των πληροφοριών; Η ασφάλεια των πληροφοριών είναι με απλά λόγια η διαδικασία κράτησης της πληροφορίας ασφαλούς προστατεύοντας την διαθεσιμότητα, την ακεραιότητα και την ιδιωτικότητα της (Demopoulos, n.d.).

Οι πληροφορίες ήταν πολύτιμες από την αυγή του ανθρώπινου είδους, π.χ. για το που θα βρει τροφή, πώς να φτιάξει ένα κατάλυμα κ.τ.λ. Στις παλαιότερες εποχές τα παραδοσιακά περιουσιακά στοιχεία ενός οργανισμού ή μιας επιχείρησης ήταν κατά κύριο λόγο απτά ή φυσικά με τη μορφή ιδιοκτησιακών τίτλων, εξοπλισμού, κτιρίων, γραφείων, χρημάτων ή άλλων μεταβιβάσιμων περιουσιακών στοιχείων, όπως ο χρυσός. Οι ανησυχίες σχετικά με την ασφάλεια ήταν κυρίως φυσικές, με τη ύπαρξη φρουρών, τοίχων, θυρίδων και χρηματοκιβωτίων. Σήμερα στα περιουσιακά στοιχεία των οργανισμών ή των επιχειρήσεων έχουν προστεθεί και τα εικονικά περιουσιακά στοιχεία όπως είναι η πνευματική ιδιοκτησία με τη μορφή ηλεκτρονικών μέσων (π.χ. αρχείων επεξεργασίας κειμένου, υπολογιστικών φύλλων και βάσεων δεδομένων). Επιπλέον, μεταβιβάσιμα περιουσιακά στοιχεία αποτελούν τα bits από έναν σκληρό δίσκο καθώς και οι συναλλαγές που εκτελούνται σε ένα δίκτυο, ενσύρματα ή ασύρματα. Ο πλούτος ενός οργανισμού αντιπροσωπεύεται σε μεγάλο βαθμό από τα ψηφιακά κομμάτια που διαθέτει (Arnason & Willett, 2007).

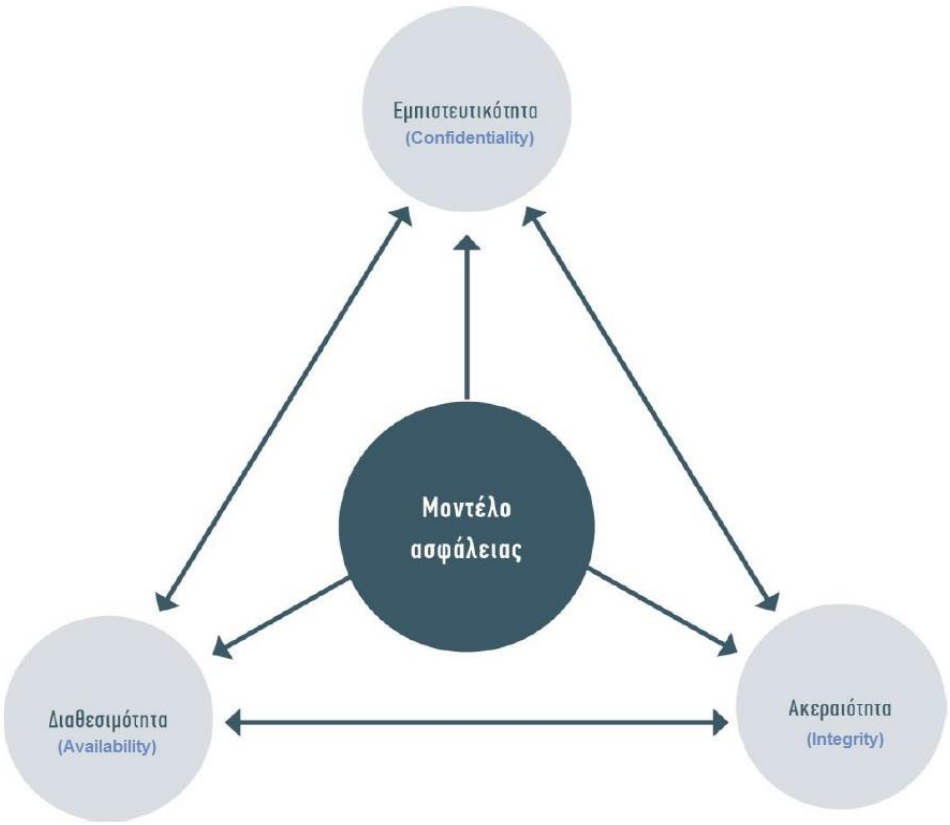
Έτσι δημιουργήθηκε η ανάγκη προστασίας αυτών των στοιχείων μέσω ελέγχων ασφαλείας της πληροφορίας. Η παραδοσιακή άποψη της ασφάλειας των πληροφοριών περιλαμβάνει τους τρεις ακρογωνιαίους λίθους της ασφάλειας των πληροφοριών: Εμπιστευτικότητα (Confidentiality), Ακεραιότητα (Integrity) και Διαθεσιμότητα (Availability), γνωστή και ως CIA της ασφάλειας των πληροφοριών και αποτελούν τους στόχους ασφαλείας της πληροφορίας ως εξής:

- *Εμπιστευτικότητα (Confidentiality):* Σκοπός της εμπιστευτικότητας είναι να διασφαλίζεται ότι μόνο εξουσιοδοτημένο προσωπικό μπορεί να έχει πρόσβαση σε πληροφορίες ή αντιθέτως ότι οι πληροφορίες δεν αποκαλύπτονται σε μη εξουσιοδοτημένα πρόσωπα ή διεργασίες (αυτοματοποιημένα συστήματα ή υπηρεσίες).

- *Ακεραιότητα (Integrity):* Για να διασφαλιστεί η ακεραιότητα πρέπει να προστατεύονται οι πληροφορίες από μη εξουσιοδοτημένη τροποποίηση ή καταστροφή ή ότι αυτές παραμένουν στην μορφή που ο δημιουργός τους τις προόριζε. Απώλεια ακεραιότητας σημαίνει μη εξουσιοδοτημένη τροποποίηση ή καταστροφή των πληροφοριών.

- *Διαθεσιμότητα (Availability)*: Η διασφάλιση της εξασφαλίζει ότι οι πληροφορίες είναι έτοιμες για χρήση. Απώλεια της διαθεσιμότητας σημαίνει διακοπή της πρόσβασης ή χρήσης των πληροφοριών ή της τεχνολογίας πληροφοριών.

Το Σχήμα 3-1 απεικονίζει τους τρεις ακρογωνιαίους λίθους της ασφάλειας δηλαδή της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας (CIA). (Arnason & Willett, 2007)



ΣΧΗΜΑ 3-1. ΟΙ 3 ΑΚΡΟΓΩΝΙΑΙΟΙ ΛΙΘΟΙ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Πηγή: (Παρασκευάς και συν., 2015)

3.2 Η ασφάλεια των πληροφοριών είναι μια διαδικασία

Η αποτελεσματική ασφάλεια των πληροφοριών ενσωματώνει προϊόντα ασφαλείας, τεχνολογίες, πολιτικές και διαδικασίες. Καμία συλλογή από τα παραπάνω προϊόντα από μόνο της δεν μπορεί να λύσει κάθε ζήτημα που θα προκύψει σένα οργανισμό σχετικά με την ασφάλεια των πληροφοριών. Προϊόντα όπως τοίχοι προστασίας (firewalls), συστήματα ανίχνευσης εισβολών (intrusion detection systems) και σαρωτές ευπαθειών (vulnerability scanners) από μόνα τους δεν επαρκούν για να παρέχουν αποτελεσματική ασφάλεια πληροφοριών (Demopoulos, n.d.).

Η ασφάλεια πληροφοριών είναι μια διαδικασία. Μια πολιτική ασφαλείας πληροφοριακών συστημάτων είναι ένα καλά καθορισμένο και τεκμηριωμένο σύνολο οδηγιών που περιγράφει πώς ένας οργανισμός διαχειρίζεται, προστατεύει τα πληροφοριακά του στοιχεία και λαμβάνει μελλοντικές αποφάσεις σχετικά με την

υποδομής ασφαλείας των συστημάτων πληροφορικής του. Οι διαδικασίες ασφαλείας τεκμηριώνουν με ακρίβεια τον τρόπο επίτευξης μια συγκεκριμένης εργασίας. Για παράδειγμα, μια πολιτική μπορεί να καθορίζει ότι το λογισμικό προστασίας από ιούς ενημερώνεται καθημερινά και μια διαδικασία θα αναφέρει επακριβώς τον τρόπο με τον οποίο θα γίνει αυτό – με μια λίστα βημάτων (Demopoulos, n.d.).

3.3 Η ασφάλεια είναι ευθύνη όλων

Αν και μερικά άτομα σένα οργανισμό μπορεί να έχουν τον όρο «Ασφάλεια» στον τίτλο τους ή μπορεί να ασχολούνται άμεσα με την ασφάλεια, η ασφάλεια σε καθημερινή βάση είναι ευθύνη όλων. Μια αλυσίδα είναι τόσο ισχυρή όσο η ασθενέστερη σύνδεση της. Ένας εργασιακός χώρος μπορεί να έχει άριστη ασφάλεια, αλλά αν ένας εργαζόμενος στο γραφείο υποστήριξης διανέμει άμεσα ή επαναφέρει τους χαμένους κωδικούς πρόσβασης ή οι εργαζόμενοι επιτρέπουν σε άλλους να εισέρχονται μαζί τους ανοίγοντας πόρτες ασφαλείας με την κάρτα τους, η ασφάλεια μπορεί να παραβιαστεί τρομερά. Παρά την ανθεκτικότητα ενός τείχους προστασίας (firewall), εάν ένας και μοναδικός χρήστης διαθέτει υλικό (π.χ. ένα μόντεμ) ή λογισμικό (π.χ. κάποιο λογισμικό κοινής χρήσης αρχείων) που επιτρέπει την παράκαμψη του τείχους προστασίας, ένας χάκερ μπορεί να αποκτήσει πρόσβαση με καταστροφικά αποτελέσματα (Demopoulos, n.d.).

Υπάρχουν παραδείγματα όπου μια κακή διαμόρφωση του τείχους προστασίας μόνο για λίγα λεπτά επέτρεψε σε έναν χάκερ να αποκτήσει πρόσβαση με καταστροφικά αποτελέσματα. Η ασφάλεια είναι ένα ζήτημα κατά τη διάρκεια ολόκληρου του κύκλου ζωής μιας εφαρμογής. Οι εφαρμογές πρέπει να σχεδιάζονται έτσι ώστε να είναι ασφαλείς, να αναπτύσσονται με γνώμονα τα θέματα ασφαλείας και με ασφάλεια. Η ασφάλεια δεν μπορεί να είναι μια σκέψη και πρέπει να είναι αποτελεσματική. Οι αναλυτές συστημάτων, οι αρχιτέκτονες και οι προγραμματιστές πρέπει όλοι να κατανοήσουν τα ζητήματα και τις τεχνικές ασφάλειας της πληροφορίας που είναι σχετικά με τη δουλειά τους (Demopoulos, n.d.).

Η συνειδητοποίηση των τελικών χρηστών είναι κρίσιμη, καθώς οι χάκερ συχνά τους στοχεύουν άμεσα. Οι χρήστες πρέπει να είναι εξοικειωμένοι με τις πολιτικές

ασφαλείας και πρέπει να γνωρίζουν πού μπορούν να ληφθούν τα πιο πρόσφατα αντίγραφα. Οι χρήστες πρέπει να γνωρίζουν τι αναμένεται και απαιτείται από αυτούς. Συνήθως αυτές οι πληροφορίες θα πρέπει να παρέχονται στους χρήστες αρχικά ως μέρος της νέας διαδικασίας πρόσληψης και να ανανεώνονται ανάλογα με τις ανάγκες (Demopoulos, n.d.).

3.4 Η ασφάλεια των πληροφοριών περιλαμβάνει μια ανταλλαγή μεταξύ της ασφάλειας και της χρηστικότητας

Δεν υπάρχει τίποτα καλύτερο από ένα απόλυτα ασφαλές σύστημα – εκτός ίσως από ένα, αυτό που να είναι εντελώς άχρηστο από τον οποιονδήποτε. Ο στόχος της εταιρικής ασφάλειας είναι να παρέχει το κατάλληλο επίπεδο ασφαλείας, με βάση την αξία των πληροφοριών ενός οργανισμού και τις επιχειρηματικές του ανάγκες. Όσο ποιο ασφαλές είναι το σύστημα, τόσο ποιο δύσκολή είναι πρόσβαση των νόμιμων χρηστών σε αυτό (Demopoulos, n.d.).

3.5 Η ασφάλεια των πληροφοριών σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης

Σύμφωνα λοιπόν με τα τεχνολογικά ζητήματα των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης που εξετάσαμε στο κεφάλαιο 2 και συνδυάζοντας όλα τα παραπάνω η ασφάλεια των πληροφοριών καθίσταται εξαιρετικά σημαντική στις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης, εξαιτίας τόσο του χαρακτήρα των πληροφοριών που αξιοποιούνται όσο και του σημαντικού όγκου που συλλέγεται, επεξεργάζεται και αποθηκεύεται (Vrakas, Kalloniatis, & Lambrinoudakis, 2010).

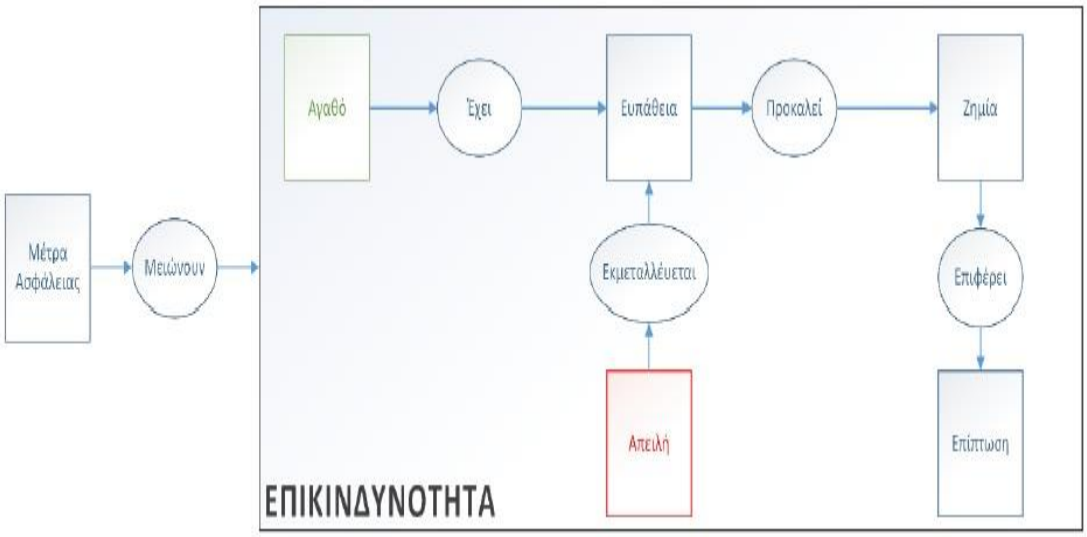
Παραδείγματα τέτοιων πληροφοριών – δεδομένων αποτελούν τα διάφορα αναγνωριστικά (τομεακά ή μη) που αξιοποιεί ο κάθε χρήστης: οικονομικά – φορολογικά στοιχεία, δημογραφικά στοιχεία, ποινικό μητρώο, ιατρικά αρχεία και δεδομένα που σχετίζονται με θρησκευτικές και πολιτικές πεποιθήσεις. Επιπρόσθετα, η ιδιαιτερότητα των υπηρεσιών που προσφέρονται από τη Δημόσια Διοίκηση έγκειται στην υποχρέωση παροχής όλων των απαιτούμενων πληροφοριών – δεδομένων, σε

αντίθεση με τις ηλεκτρονικές υπηρεσίες σε πληροφοριακά συστήματα ηλεκτρονικού εμπορίου ή ηλεκτρονικής μάθησης, όπου ο χρήστης μπορεί να μην παρέχει κάποιες πληροφορίες αλλά παρόλα αυτά να καταστεί δυνατή η παροχή της υπηρεσίας (Δρογκάρης, 2013).

3.6 Εννοιολογική Θεμελίωση.

Είναι αναγκαία η ύπαρξη ενός κοινού λεξιλογίου, αυστηρά καθορισμένου, έτσι ώστε να μπορέσουν δύο μέρη να επικοινωνήσουν αποτελεσματικά. Στο χώρο της ασφάλειας πληροφοριών, η ανάγκη αυτή είναι ακόμη επιτακτικότερη, καθώς τα μέρη τα οποία έρχονται σε επικοινωνία μπορεί να ανήκουν σε διαφορετικούς τομείς (π.χ. Πληροφορική, Οικονομικά, Διοίκηση κ.λπ.), ενώ λειτουργούν μέσα στον ίδιο οργανισμό για τον κοινό σκοπό. Έτσι, οι βασικές έννοιες που αφορούν στην ασφάλεια πληροφοριών (και κατ' επέκταση τη Διαχείριση της Ασφάλειας) θα πρέπει να είναι ξεκάθαρες για κάθε συμμετέχοντα στη διαδικασία λήψης αποφάσεων που αφορούν τον οργανισμό (Μαυρίδης, 2015).

Στο Σχήμα 3-2, εμφανίζονται οι συσχετίσεις μεταξύ των όρων ασφάλειας πληροφοριών, οι οποίοι θα μας απασχολήσουν στη συνέχεια.



ΣΧΗΜΑ 3-2. ΣΥΣΧΕΤΙΣΕΙΣ ΜΕΤΑΞΥ ΟΡΩΝ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Πηγή : (Μαυρίδης, 2015)

Ένα αγαθό, όπως εμφανίζεται στο παραπάνω Σχήμα 3-2, έχει αξία για ένα οργανισμό και πρέπει να προστατευτεί. Αυτό είναι ιδιαίτερα σημαντικό στο διαρκώς διασυνδεόμενο επιχειρηματικό περιβάλλον, όπου οι πληροφορίες εκτίθενται σε ένα ολοένα αυξανόμενο αριθμό και με μια διερευνώμενη ποικιλία απειλών (Μαυρίδης, 2015).

Η πληροφορία (ως αγαθό) μπορεί να εμφανιστεί υπό διάφορες μορφές. Μπορεί να γραφεί σε χαρτί, να αποθηκευτεί και να μεταδοθεί ηλεκτρονικά ή να αναφερθεί σε κάποια συζήτηση. Ασχέτως της μορφής ή του τρόπου αποθήκευσής της, η πληροφορία θα πρέπει πάντοτε να είναι επαρκώς προστατευμένη. Στο πλαίσιο της ασφάλειας πληροφοριών, επιδιώκεται η προστασία των πληροφοριών από μια ευρεία γκάμα απειλών, ώστε να διασφαλιστεί η επιχειρησιακή συνέχεια, να ελαχιστοποιηθεί η συνολική εναπομείνασα επικινδυνότητα και να μεγιστοποιηθούν οι αποδόσεις των επενδύσεων και οι επιχειρησιακές ευκαιρίες (Μαυρίδης, 2015).

Η μείωση της συνολικής επικινδυνότητας επιτυγχάνεται με την υλοποίηση ενός κατάλληλου συνόλου (αντι)μέτρων (controls), που περιλαμβάνουν πολιτικές, πρακτικές, διαδικασίες, τεχνικές και λειτουργίες λογισμικού και υλικού. Αυτά τα μέτρα είναι απαραίτητα προκειμένου να διασφαλιστεί ότι επιτυγχάνονται οι επιμέρους στόχοι του οργανισμού που αφορούν την ασφάλεια πληροφοριών, σε συνδυασμό με άλλες πρακτικές διαχείρισης (Μαυρίδης, 2015).

Η αξία ενός αγαθού αφορά τη σημαντικότητά του για την επίτευξη των στόχων του οργανισμού και εκφράζεται είτε με χρηματικούς ή άλλους όρους. Ένα υπολογιστικό σύστημα είναι δυνατό να παρουσιάζει ευπάθειες, δηλαδή αδυναμίες τις οποίες μπορεί να εκμεταλλευτεί μια απειλή (στο πλαίσιο μια επίθεσης) και να προκαλέσει ζημία. Η απειλή μπορεί να είναι φυσική, τεχνικής φύσης, ή ανθρώπινη, εκούσια ή ακούσια. Επίσης, μια απειλή μπορεί να είναι σκόπιμη ή τυχαία. Ως ζημία, θεωρούμε την επίπτωση που προκαλεί η μείωση της αξίας του αγαθού. Η επίπτωση αποτυπώνεται ως μια αλλαγή στο δυνητικό βαθμό επίτευξης των επιχειρησιακών στόχων του οργανισμού (Μαυρίδης, 2015).

Τα πέντε αυτά στοιχεία (αγαθό, ευπάθεια, ζημία, απειλή και επίπτωση) ορίζουν την έννοια της επικινδυνότητας (risk). Με βάση την κατάλληλη αποτίμηση της

επικινδυνότητας θα πρέπει να γίνεται επιλογή των κατάλληλων μέτρων προστασίας, που θα μετριάζουν την επικινδυνότητα.

Ο σχεδιασμός, η υλοποίηση, η συντήρηση και η βελτίωση της ασφάλειας πληροφοριών αποτελούν ουσιαστικούς παράγοντες για την επίτευξη ανταγωνιστικών χαρακτηριστικών, κερδοφορίας, επαρκούς συμμόρφωσης με τους νόμους και διαμόρφωσης κατάλληλης φήμης. Όμως, στον αρχικό σχεδιασμό των πληροφοριακών συστημάτων συνήθως δεν συμπεριλαμβάνονται εξ αρχής τα απαραίτητα χαρακτηριστικά ασφάλειας, με αποτέλεσμα το παρεχόμενο επίπεδο ασφάλειας να είναι ανεπαρκές και να χρειάζεται μια κατάλληλη διαχείριση και υλοποίηση επιμέρους διαδικασιών (Μαυρίδης, 2015).

Η επιλογή των κατάλληλων μέτρων ελέγχου, προϋποθέτει προσεκτικό και λεπτομερή σχεδιασμό, ενώ η ασφάλεια των πληροφοριών γενικότερα απαιτεί τη συμμετοχή όλων των εργαζομένων του οργανισμού. Επιπλέον, μπορεί να χρειάζεται και η συμμετοχή των προμηθευτών, των πελατών ή ακόμη και η συνδρομή εξωτερικών συνεργατών, εξειδικευμένων σε θέματα ασφάλειας. Συνολικά, η Διαχείριση Ασφάλειας αποσκοπεί στη διαμόρφωση ενός οργανωμένου πλαισίου εννοιών, αρχών, πολιτικών, διαδικασιών και τεχνικών μέτρων που απαιτούνται προκειμένου να προστατευθούν τα αγαθά από σκόπιμες ή τυχαίες απειλές (Μαυρίδης, 2015).

3.7 Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ)

Ορισμένοι βασικοί παράγοντες, στη βάση των οποίων ένας οργανισμός μπορεί να ορίζει το επιθυμητό επίπεδο ασφάλειας είναι οι εξής (Μαυρίδης, 2015):

- Αποδεκτό επίπεδο ασφάλειας.
- Λειτουργικότητα του Πληροφοριακού Συστήματος που διαθέτει.
- Κόστος που επιθυμεί να επωμισθεί.

Ο σχεδιασμός της ασφάλειας πληροφοριών ενός οργανισμού είναι μια επιχειρησιακή διεργασία, η οποία αποσκοπεί στο να παρέχονται τα κατάλληλα

εργαλεία λήψης αποφάσεων, προκειμένου να μπορεί η διοίκηση να ασκήσει αποτελεσματικά το ρόλο της. Υπό αυτή την έννοια, η ασφάλεια πληροφοριών δεν είναι ένα αμιγώς τεχνικό θέμα, αλλά συμπεριλαμβάνει ζητήματα και παραμέτρους από διάφορους χώρους (οικονομία, διοίκηση, κοινωνία κ.λπ.). Για να επιτευχθεί ένας αποδοτικός συντονισμός των ενεργειών προς αυτή τη κατεύθυνση, θα πρέπει να οριστούν οι στόχοι της ασφάλειας πληροφοριών, καθώς και οι διαδικασίες των οποίων η εξέλιξη αλλά και τα αποτελέσματα θα ελέγχονται διαρκώς, χρησιμοποιώντας ένα κατάλληλο σύστημα διαχείρισης της ασφάλειας. Επιπλέον, οι απαιτήσεις ασφάλειας θα πρέπει να προσδιορίζονται στη βάση μιας περιοδικά επαναλαμβανόμενης μελέτης για την ανάλυση και διαχείριση της επικινδυνότητας (Risk Management) (Μαυρίδης, 2015).

Ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών, ΣΔΑΠ (Information Security Management System – ISMS) επικεντρώνεται κυρίως στις διαδικασίες που λαμβάνουν χώρα στο πλαίσιο ενός οργανισμού. Για τη διαχείριση της Ασφάλειας Πληροφοριών υπάρχουν αρκετές διαφορετικές μεθοδολογίες οι οποίες χρησιμοποιούν ή στηρίζονται αποκλειστικά σε κάποιο από τα πολλά και διαφορετικά πρότυπα που έχουν αναπτυχθεί. Μερικές από τις γνωστότερες είναι οι παρακάτω (Μαυρίδης, 2015):

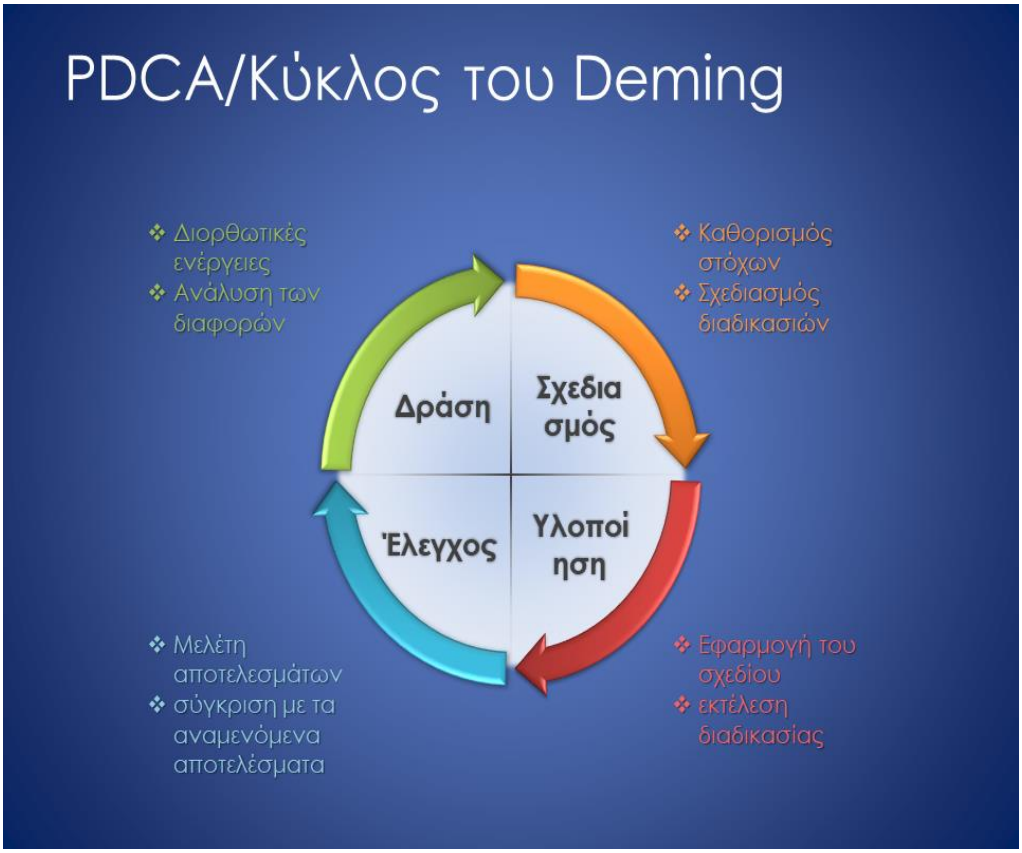
- OCTAVE από τον οργανισμό CERT (Carnegie Mellon University).
- COBIT από το Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής (Information Systems Audit and Control Association, ISACA). Βασίζεται στον κύκλο: Govern → Direct →Control → Implement → Measure → Evaluate Report.
- FIRM από το Information Security Forum
- Μεθοδολογία του οργανισμού NIST. Βασίζεται στον κύκλο: System Characterization Threat Identification → Vulnerability Identification → Control Analysis → Likelihood Determination → Impact Analysis → Risk Determination → Control Recommendations → Results Documentation

Μια ιδιαίτερα διαδεδομένη μέθοδος για τον έλεγχο και τη βελτίωση αυτών των διαδικασιών κατά την ανάπτυξη ενός Συστήματος Διαχείρισης της Ασφάλειας

Πληροφοριών (π.χ. σύμφωνα με το πρότυπο ISO/IEC 27001: 2005 αναθεωρήθηκε το 2013) είναι η μέθοδος Plan-Do-Check-Act (PDCA).

Η μέθοδος PDCA αποτελείται από τέσσερα επαναληπτικά βήματα ως εξής:

- **Σχεδιασμός (Plan):** Στο βήμα αυτό γίνεται ο καθορισμός των στόχων και ο σχεδιασμός των διαδικασιών που θα εφαρμοστούν με τους οποίους θα επιτευχθούν οι στόχοι.
- **Υλοποίηση (Do):** Εδώ υλοποιούνται τα μέτρα τα οποία ορίστηκαν κατά τη φάση του σχεδιασμού.
- **Έλεγχος (Check):** Πραγματοποιείται έλεγχος απόκλισης των αρχικών στόχων και των τελικών αποτελεσμάτων.
- **Δράση (Act):** Εφαρμόζονται ενέργειες διόρθωσης και βελτίωσης των μέτρων.



ΣΧΗΜΑ 3-3. Ο ΚΥΚΛΟΣ ΤΟΥ DEMING

Σύμφωνα με τον κύκλο του Deming λοιπόν μπορούμε να φανταστούμε το Σύστημα Διαχείρισης της Ασφάλειας Πληροφοριών (ΣΔΑΠ) ως μία ενιαία διεργασία η οποία δέχεται ως είσοδο τις απαιτήσεις ασφάλειας του οργανισμού και παρέχει ως έξοδο τη διαχείριση της ασφάλειας πληροφοριών. Κατά τη φάση του σχεδιασμού, πραγματοποιείται ανάλυση και εκτίμηση της επικινδυνότητας για την ασφάλεια των πληροφοριών. Πιο συγκεκριμένα, διαμορφώνονται και πραγματοποιούνται μεταξύ άλλων τα εξής (Μαυρίδης, 2015):

- Έγκριση από τη Διοίκηση του οργανισμού.
- Καθορισμός του πεδίου εφαρμογής (υπολογιστικά συστήματα, δεδομένα κλπ.).
- Μελέτη Ανάλυσης και Αποτίμησης Επικινδυνότητας.
- Καθορισμός απαιτήσεων ασφάλειας.
- Δημιουργία Πολιτικής Ασφάλειας.

Αξίζει εδώ να επισημανθεί ότι είναι πρωταρχικής σημασίας για έναν οργανισμό ο καθορισμός των απαιτήσεών του σε θέματα ασφάλειας. Μερικές βασικές πηγές άντλησης πληροφοριών για απαιτήσεις ασφάλειας είναι ο εξής (Μαυρίδης, 2015):

- Η αποτίμηση της επικινδυνότητας (risk assessment) που αντιμετωπίζει ο οργανισμός. Μέσω αυτής της διαδικασίας, αναγνωρίζονται οι πιθανές απειλές προς τους πόρους του οργανισμού. Επιπλέον, εκτιμάται η συνολική ευπάθεια (vulnerability) του οργανισμού στις συγκεκριμένες απειλές, η πιθανότητα υλοποιήσεών τους, καθώς και το κόστος που θα έχουν οι επιπτώσεις για τον οργανισμό από πιθανές επιθέσεις.
- Το νομικό και κανονιστικό πλαίσιο, καθώς και οι συμβατικές υποχρεώσεις του οργανισμού απέναντι στο κράτος, το προσωπικό και τους συνεργάτες του.
- Το σύνολο των αρχών, των απαιτήσεων και των στόχων που ορίζει ο ίδιος ο οργανισμός σχετικά με την επεξεργασία των πληροφοριών που είναι απαραίτητες για τη λειτουργία του.

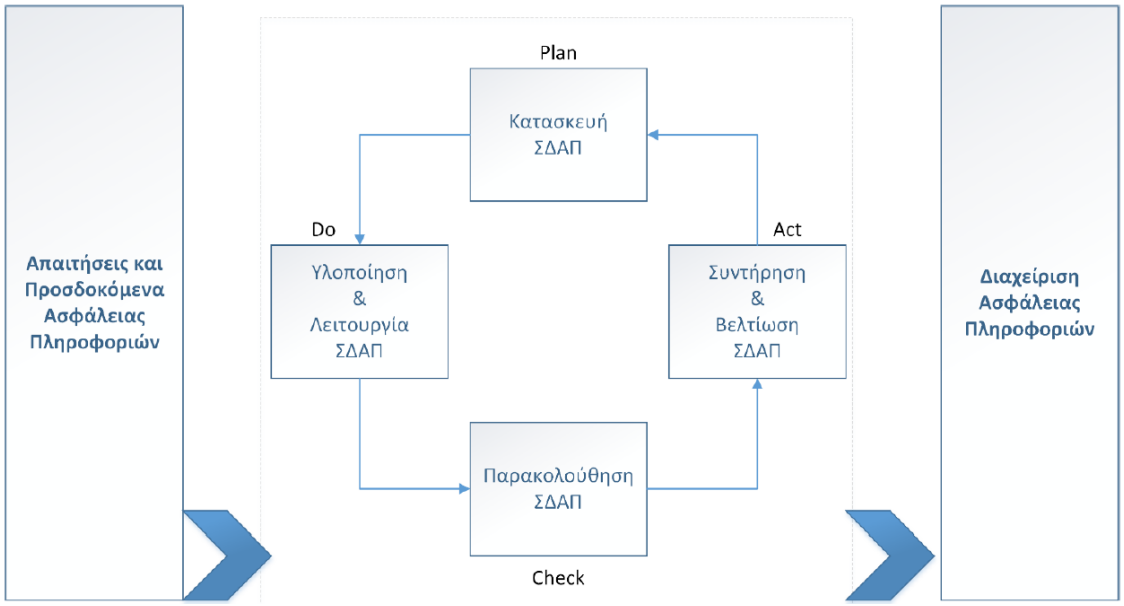
Στη φάση της υλοποίησης και με βάση τα αποτελέσματα της αποτίμησης, ακολουθεί νέα μελέτη που αποσκοπεί στη μείωση της επικινδυνότητας με την επιλογή και υλοποίηση των κατάλληλων μέτρων προστασίας. Αναλυτικότερα, διαμορφώνονται και υλοποιούνται μεταξύ άλλων τα εξής (Μαυρίδης, 2015):

- Σχέδιο Διαχείρισης Επικινδυνότητας.
- Κατανομή ρόλων και αρμοδιοτήτων.
- Υλοποίηση μέτρων ασφάλειας.
- Δράσεις ενημέρωσης και κατάρτισης του προσωπικού.

Κατά τον έλεγχο, πραγματοποιείται μια αξιολόγηση των αποτελεσμάτων σε σχέση με τους αρχικούς στόχους που είχαν τεθεί και διαμορφώνεται μια αναφορά αξιολόγησης προς τη διοίκηση του οργανισμού. Η διαδικασία του ελέγχου είναι επαναληπτική και πραγματοποιείται ανά τακτά χρονικά διαστήματα, συνήθως από το αρμόδιο τμήμα εσωτερικού ελέγχου του οργανισμού.

Τέλος, στο στάδιο της δράσης εκτελούνται όλες εκείνες οι απαραίτητες ενέργειες, οι οποίες κρίθηκε ότι απαιτούνται προκειμένου να βελτιωθεί η συνολική διεργασία της διαχείρισης της ασφάλειας πληροφοριών. Πραγματοποιείται ενημέρωση της διοίκησης και παράλληλα ελέγχεται και αξιολογείται και η ίδια η διαδικασία βελτίωσης των μέτρων προστασίας.

Το πρότυπο ISO/IEC 27001:2005, συνδυάζοντας τα τέσσερα (4) βήματα της μεθοδολογίας PDCA, όριζε το πλαίσιο της Διαχείρισης Ασφάλειας Πληροφοριών, όπως φαίνεται στο παρακάτω Σχήμα 3-4.



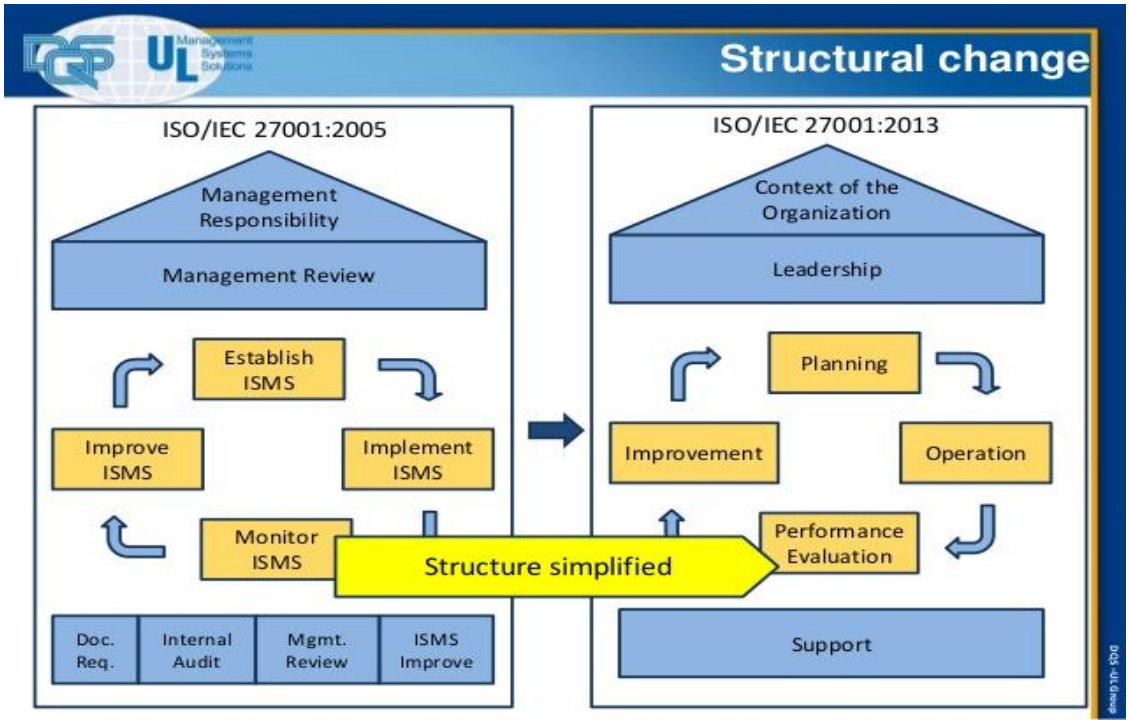
ΣΧΗΜΑ 3-4. ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΤΑ ISO/IEC 27001:2005

Πηγή : (Μαυρίδης, 2015)

Η παραπάνω μεθοδολογία χρησιμοποιήθηκε ως πυλώνας για τον σχεδιασμό ενός ΣΔΑΠ μέχρι την πλήρη αναθεωρημένη επανέκδοση του προτύπου ISO/IEC 27001 τον Σεπτέμβριο του 2013, η οποία περιείχε σημαντικές αλλαγές προκειμένου να ευθυγραμμιστεί με άλλα πρότυπα ISO συστημάτων διαχείρισης που καλύπτουν τη διασφάλιση της ποιότητας, την προστασία του περιβάλλοντος κλπ. Έτσι, έννοιες όπως η πιστοποίηση, η πολιτική, η μη συμμόρφωση, ο έλεγχος εγγράφων, οι εσωτερικοί έλεγχοι και οι ανασκοπήσεις διαχείρισης που είναι κοινές σε όλα τα πρότυπα ISO συστημάτων διαχείρισης και στην πραγματικότητα αποτελούν διαδικασίες μπορούν σε μεγάλο βαθμό να τυποποιηθούν μέσα σε έναν οργανισμό.

Το αναθεωρημένο πρότυπο δεν καθορίζει πλέον τη χρήση του κύκλου PDCA ως υποχρεωτική, αναγνωρίζοντας το γεγονός ότι υπάρχουν και άλλες μέθοδοι διασφάλισης της συνεχούς βελτίωσης μιας διεργασίας, όπως η μέθοδος DMAIC (Define-Measure-Analyze-Improve-Control) επιτρέποντας στους οργανισμούς να χρησιμοποιήσουν όποια άλλη μέθοδο επιθυμούν, αρκεί τα αποτελέσματα να συνάδουν με τις απαιτήσεις του προτύπου (Κάτσικας Σ. Κ., 2014). Στο σημείο αυτό θα πρέπει να επισημάνουμε ότι για τους περισσότερους οργανισμούς τα τέσσερα (4) βήματα της μεθοδολογίας PDCA θα εξακολουθούν να αποτελούν μια πρακτική μέθοδος για την ανάπτυξη ενός ΣΔΑΠ. Στο Σχήμα 3-6 φαίνονται οι κυριότερες

δομικές αλλαγές σε περίπτωση εφαρμογής της συγκεκριμένης μεθοδολογίας σε σχέση με την προηγουμένη έκδοση.



ΣΧΗΜΑ 3-5 ΣΥΓΚΡΙΣΗ ΚΥΚΛΩΝ PCDA ISO/IEC 27001:2005 & ISO/IEC 27001: 2013

(Πηγή: (Slidesharenet, 2015))

Αυτό που μπορεί να διαπιστώσει κάποιος παρατηρώντας το παραπάνω σχήμα είναι ότι η δομή του νέου προτύπου όπως διαμορφώνεται σε σχέση με τον κύκλο PCDA είναι ότι έχει απλοποιηθεί και έχει γίνει ποιο ευέλικτη σε σχέση με τον προκάτοχο του, στο σημείο αυτό θα πρέπει να επισημανθεί ότι υπάρχουν πολλές διαφοροποιήσεις σε αρκετά σημεία σε σχέση με τον προκάτοχο του οι οποίες δεν αποτελούν αντικείμενο αυτής της διπλωματικής. Το νέο πρότυπο ISO/IEC 27001:2013 αναλύεται σε βάθος στο επόμενο κεφάλαιο.

ΚΕΦΑΛΑΙΟ 4

«Η ΟΙΚΟΓΕΝΕΙΑ ΤΩΝ ΠΡΟΤΥΠΩΝ ΤΗΣ ΣΕΙΡΑΣ ISO/IEC 27000»

4.1 Εισαγωγή

Όπως είδαμε στο Κεφάλαιο 3 οι πληροφορίες και τα Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) αποτελούν σημαντικό θεμέλιο για τους οργανισμούς και τις επιχειρήσεις. Συγκεκριμένα, οι όλο περισσότερες εσωτερικές και ενδοεταιρικές μεταφορές δεδομένων καθώς και η χρήση ανοιχτών δικτύων αυξάνουν τους κινδύνους στους οποίους εκτίθενται οι πληροφορίες και τα συστήματα πληροφοριών. Προκειμένου να μειωθούν οι κίνδυνοι και να αποφευχθούν ζημίες στις επιχειρήσεις και τους οργανισμούς, πρέπει να ληφθεί μέριμνα για την εξασφάλιση επαρκούς ασφάλειας των πληροφοριών αυτών (BSI, 2005).

Για την προστασία των συστημάτων πληροφοριών και των πληροφοριών γενικά, αναπτύχθηκαν τα πρότυπα ISO 27000, ISO 27001 και ISO 27002 τα οποία παρέχουν στόχους ελέγχου, ειδικούς ελέγχους, απαιτήσεις και κατευθυντήριες γραμμές, με τις οποίες μια εταιρεία ή ένας οργανισμός μπορεί να επιτύχει επαρκή ασφάλεια πληροφοριών. Με τον τρόπο αυτό, το ISO 27001 καθιστά δυνατή την πιστοποίηση της εταιρείας ή του οργανισμού σύμφωνα με το πρότυπο, όπου η ασφάλεια των πληροφοριών μπορεί να τεκμηριωθεί ως αυστηρή εφαρμογή και διαχείριση σύμφωνα με ένα διεθνώς αναγνωρισμένο οργανωτικό πρότυπο.

Με την πιστοποίηση σύμφωνα με το πρότυπο ISO 27001, μια εταιρεία ή ένας οργανισμός επαληθεύει την εκπλήρωση γνωστών και αποδεκτών προτύπων ασφαλείας και επομένως προάγει την εμπιστοσύνη των πελατών ή των πολιτών αντίστοιχα. Επίσης, η πιστοποίηση συμμόρφωσης με ένα διεθνές πρότυπο μειώνει τον κίνδυνο επιβολής προστίμων ή αποζημιώσεων λόγω νομικών διαφορών, καθώς μπορεί να αντιμετωπιστούν ενδεχόμενες νομικές απαιτήσεις (Pelnekar, 2011). Παρακάτω παρουσιάζονται τα πρότυπα ISO 27000 έως ISO 27002, η εξέλιξη τους και γενικά η σειρά των προτύπων ISO 27K.

4.2 Γενικά περί προτύπων συστημάτων διαχείρισης ISO

Τα πρότυπα προκύπτουν από την ανάπτυξη λεπτομερών περιγραφών των ιδιαίτερων χαρακτηριστικών ενός προϊόντος ή υπηρεσίας από εμπειρογνώμονες, από εταιρείες και επιστημονικούς φορείς. Αντιπροσωπεύουν συναίνεση σχετικά με χαρακτηριστικά όπως η ποιότητα, η ασφάλεια και η αξιοπιστία που θα πρέπει να παραμείνουν σε ισχύ για μεγάλο χρονικό διάστημα και έτσι τεκμηριώνονται και δημοσιεύονται. Ο στόχος της ανάπτυξης προτύπων είναι να υποστηριχθούν τόσο τα άτομα όσο και οι εταιρείες κατά την προμήθεια προϊόντων και υπηρεσιών. Οι πάροχοι προϊόντων και υπηρεσιών μπορούν να ενισχύσουν τη φήμη τους πιστοποιώντας τη συμμόρφωσή τους με τα πρότυπα (Iso27001security.com, 2017).

Ο Διεθνής Οργανισμός Τυποποίησης - ISO (International Standardization Organization) είναι ένας οργανισμός που ιδρύθηκε το 1946, υποστηρίζεται από 159 χώρες και είναι ο κορυφαίος οργανισμός που εκδίδει διεθνή πρότυπα. Ο Διεθνής Οργανισμός Τυποποίησης - ISO και η Διεθνής Ηλεκτροτεχνική Επιτροπή - IEC (International Electrotechnical Commission), η οποία είναι ο κορυφαίος παγκόσμιος εκδότης διεθνών προτύπων στον κλάδο των ηλεκτρονικών και των ηλεκτρονικών τεχνολογιών εργάζονται από κοινού σε διεθνή πρότυπα και κατευθυντήριες γραμμές. Ένας από τους κοινούς στόχους αυτής της συνεργασίας είναι και η δημιουργία προτύπων ΣΔΑΠ που θα δούμε παρακάτω. (Iso27001security.com, 2017)

Η συλλογική προσπάθεια για την παραγωγή προτύπων περιλαμβάνει την Ομάδα Εργασίας 1 -WG1(Working Group 1), την Ομάδα Εργασίας 2 -WG2 (Working Group 2) και την Ομάδα Εργασίας 3 -WG3 (Working Group 3). Όλες αυτές οι ομάδες εργασίας αποτελούν μέρος της Υποεπιτροπής 27 - SC 27 (Subcommitee 27), η οποία αποτελεί με τη σειρά της κοινή τεχνική επιτροπή 1 - JTC 1 (Joint Technical Committee 1). Το πεδίο εφαρμογής της Ομάδας Εργασίας 1-WG1 είναι τα πρότυπα διαχείρισης ασφάλειας, συμπεριλαμβανομένων τομέων που αφορούν νέες εξελίξεις προτύπων στην ασφάλεια πληροφοριών και ανάπτυξη των ήδη υπαρχόντων προτύπων ΣΔΑΠ - ISMS (Information Security Management Systems) (Arnason & Willett, 2007).

Σκοπός της ομάδας εργασίας 1 - WG1 είναι ο καθορισμός ενός οδικού χάρτη που προσδιορίζει τις απαιτήσεις για ένα μελλοντικό σύνολο διεθνών προτύπων και κατευθυντήριων γραμμών για τη δημιουργία, εφαρμογή, λειτουργία, παρακολούθηση και συντήρηση των Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών ΣΔΑΠ - ISMS. Για να υποστηρίξουν αυτόν τον οδικό χάρτη, αποφασίστηκε μια νέα σειρά αριθμών (27000) για τα διεθνή πρότυπα ασφάλειας πληροφοριών. Το ISO / IEC 27001, συγκεκριμένα, είναι ένα από τα πακέτα προδιαγραφών ISO που τυπικά προσδιορίζουν τα «συστήματα διαχείρισης». Άλλα πρότυπα συστημάτων διαχείρισης ISO είναι τα παρακάτω (Iso27001security.com, 2017):

- ISO 9001 για τη διαχείριση της ποιότητας που απορρέει από το BS 5750 και πριν από αυτήν την προσέγγιση Deming για τη διασφάλιση της ποιότητας και τη συνεχή βελτίωση (αντιμετώπιση του εμπορικού, οικονομικού, φήμης και άλλων κινδύνων που συνδέονται με την αδυναμία παραγωγής αγαθών και υπηρεσιών σταθερής υψηλής ποιότητας).

- ISO 14001 για την περιβαλλοντική διαχείριση (ασχολείται με τους κινδύνους συμμόρφωσης, τους κοινωνικούς και υγειονομικούς κινδύνους που συνδέονται με την εκκένωση υγρών αποβλήτων, τη ρύπανση κ.λπ.).

- ISO 50001 για τη διαχείριση της ενέργειας (αντιμετώπιση του κόστους που συνδέεται με την αναποτελεσματική χρήση της ενέργειας).

- OHSAS 18001 για τη διαχείριση της υγείας και της ασφάλειας στην εργασία [που θα γίνει το ISO 45001 κατά το 2016] (αντιμετώπιση κινδύνων που σχετίζονται με ατυχήματα και θανάτους στην εργασία, ανθυγιεινές και μη ασφαλείς συνθήκες εργασίας ή πρακτικές κ.λπ.).

Όλα τα πρότυπα των συστημάτων διαχείρισης ISO καθορίζουν τις ρυθμίσεις ορθής πρακτικής και διαχείρισης σχετικά με τους αντίστοιχους τομείς θεμάτων.

Η διαχρονική κληρονομιά του W. Edward Deming (εκτός από τη βιομηχανική βάση της Ιαπωνίας και την εκπληκτική οικονομική της ανάκαμψη από τη δεκαετία του 1950!) είναι η θεμελιώδης ιδέα ότι η διοίκηση πρέπει πρώτα να πάρει τον έλεγχο για να αξιολογήσει και όπου χρειάζεται, να βελτιώσει συστηματικά τα πράγματα. Οι πληροφορίες και οι μετρήσεις διαχείρισης είναι ζωτικής σημασίας, μαζί με σαφείς

επιχειρησιακούς στόχους ή στόχους με τους οποίους πρέπει να μετρηθούν και να εκτιμηθούν οι πραγματικές επιδόσεις και οι δομές διακυβέρνησης (όπως πολιτικές και δραστηριότητες συμμόρφωσης) να θεσπίσουν ή να εφαρμόσουν τις απαραίτητες αλλαγές για την ωρίμανση του οργανισμού. Στον κόσμο του Deming, οι «γνώσεις» και «δεδομένα» είναι τα βασικά εργαλεία διαχείρισης, με αποχρώσεις του Taylorism και την προσέγγιση της «επιστημονικής διαχείρισης» που ήταν δημοφιλής καθώς η μαζική παραγωγή ήρθε στο προσκήνιο στις αρχές του 20ού αιώνα (Iso27001security.com, 2017).

Τα πρότυπα των συστημάτων διαχείρισης είναι σαφώς και τυπικά καθορισμένα, έτσι ώστε οι οργανισμοί να μπορούν να επιλέξουν να πιστοποιούνται σύμφωνα με αυτά από ανεξάρτητους φορείς και οργανισμούς πιστοποίησης οι οποίοι έχουν δεόντως διαπιστευτεί, δίνοντας έτσι αξιοπιστία, ακεραιότητα και νόημα στα πιστοποιητικά που χορηγούν. Μπορούν επίσης να επιλέξουν να υιοθετήσουν τα πρότυπα χωρίς να έχουν πιστοποιηθεί, αν και η πιστοποίηση απαιτείται μερικές φορές από τους ιδιοκτήτες, τις αρχές, τους επιχειρηματικούς εταίρους, τους νόμους ή τους κανονισμούς ως μέσο αύξησης της αξιοπιστίας (Iso27001security.com, 2017).

Από το 2012, όλα τα πρότυπα του συστήματος διαχείρισης ISO είναι σταδιακά ευθυγραμμισμένα γύρω από την ίδια βασική δομή και ιδέες, χρησιμοποιώντας συχνά άλλοτε περισσότερο και άλλοτε λιγότερο παρόμοιους όρους και λέξεις. Παρόλο που απαιτεί συμβιβασμούς και παραλείψεις σε διάφορα σημεία, το πλεονέκτημα της ευθυγράμμισης είναι ότι οι διευθυντές, το προσωπικό, οι ειδικοί και οι ελεγκτές που γνωρίζουν ένα σύστημα διαχείρισης μπορούν επίσης να είναι εξοικειωμένοι και με άλλα τουλάχιστον εννοιολογικά. Υπάρχουν και άλλα ποιο εξειδικευμένα πλεονεκτήματα όπως:

- Διαλειτουργικότητα μεταξύ συστημάτων διαχείρισης και αποτελεσματικότητα, όπως είναι η χρήση παρόμοιων φορμών και διαδικασιών, και συνδυασμένων ελέγχων.

- Συνέπεια στις προσεγγίσεις διαχείρισης και την ορολογία.

- Επιτρέπουν στην επιχείρηση ή τον οργανισμό να ελέγχει ο ίδιος ή ίδια τα συστήματα διαχείρισης, παρά τα πρότυπα ή οι ειδικοί.

4.3 Η ιστορία των προτύπων ασφάλειας πληροφοριών ISO27K

Το ISO27K ξεκίνησε τη δεκαετία του 1980 και συνεχίζει να αυξάνεται και να αλλάζει, αντικατοπτρίζοντας τη συνεχή εξέλιξη στον τομέα, τις νέες προκλήσεις (όπως το cloud computing) και την αναδυόμενη συναίνεση σχετικά με τις ορθές πρακτικές ασφάλειας των πληροφοριών. Τα βασικά στάδια στην ανάπτυξη των βασικών προτύπων περιγράφονται παρακάτω (Iso27001security.com, 2017):

4.3.1. Τέλη της δεκαετίας του '80: Ολλανδική Βασιλεία / Εγχειρίδιο Πολιτικής Ασφάλειας Πληροφοριών του ομίλου Shell

Το BS 7799 και ως εκ τούτου το ISO27K οφείλει την ύπαρξή του από τον όμιλο Shell και από ένα εσωτερικό έγγραφο που γενναιόδωρα έκανε δωρεά στην κοινότητα. Όταν δημοσιεύθηκε για πρώτη φορά το 1995, το BS 7799 έδινε έμφαση στις έννοιες της ασφάλειας κεντρικών υπολογιστικών συστημάτων και στην έλλειψη σαφών αναφορών για το Internet και την προέλευση του από την αρχή της προηγούμενης δεκαετίας: αυτή η έλλειψη γνώσης παραμένει ζήτημα ακόμα και σήμερα με το ISO27K, δεδομένου ότι οι διαδικασίες του ISO/IEC για τον καθορισμό, την σύνταξη, την συμφωνία και την αποδέσμευση διεθνών προτύπων έχουν κύκλους χρόνου πολλών ετών, ενώ σημαντικά νέα θέματα ασφάλειας πληροφοριών εμφανίζονται συνήθως κάθε χρόνο. Ακριβώς το ίδιο πρόβλημα επηρεάζει τους οργανισμούς που εφαρμόζουν τα πρότυπα, αλλά τουλάχιστον το σύστημα διαχείρισης τους δίνει τα εργαλεία για τον εντοπισμό και την ανταπόκριση στις αλλαγές των κινδύνων πληροφόρησης.

4.3.2. 1989: Κώδικας Πρακτικής Χρήσης του Υπουργείο Εμπορίου και Βιομηχανίας - Κέντρο Ασφάλειας Εμπορικών Υπολογιστών DTI CCSC (πρώτη δημοσίευση μετά την Shell).

Χρησιμοποιώντας το έγγραφο της Shell, το Υπουργείο Εμπορίου και Βιομηχανίας - Κέντρο Ασφάλειας Εμπορικών Υπολογιστών (Department of Trade and Industry’s Commercial Computer Security Centre, DTI-CCSC) του Ηνωμένου Βασιλείου ανέπτυξε και δημοσίευσε αυτόν τον οδηγό για την ασφάλεια των πληροφοριών για τα μέλη του. Το CCSC έγραψε επίσης τα «Πράσινα Βιβλία», τα οποία με τη βοήθεια της Κυβερνητικής Ομάδας Ασφάλειας Επικοινωνιών και

Ηλεκτρονικών του Ηνωμένου Βασιλείου (CESG) μετατράπηκαν στο Βρετανικό Σύστημα Αξιολόγησης Ασφαλείας και Πιστοποίησης Συστημάτων Πληροφορικής (IT Security Evaluation and Certification, ITSEC) και προσχέδιο για την πιστοποίηση προϊόντων ασφαλείας που ξεκίνησε το 1990/1991 στο Ηνωμένο Βασίλειο.

4.3.3. 1993: BSI-DISC PD003 - Κώδικας Πρακτικής DTI για τη διαχείριση της ασφάλειας πληροφοριών - πρώτη δημόσια κυκλοφορία.

Εν αναμονή της κυκλοφορίας του ως επίσημου βρετανικού προτύπου, τα κύρια μέρη του BS 7799 είχαν ήδη προεκδοθεί από το Υπουργείο Εμπορίου και Βιομηχανίας του Ηνωμένου Βασιλείου μέσω του Βρετανικού Ινστιτούτου Προτύπων (British Standards Institute, BSI) ως δωρεάν πληροφοριακό στοιχείο με την ονομασία BSI-DISC PD003 (BSI – Παροχή Πληροφοριακών Λύσεων Προς Πελάτες - Δημόσιο Έγγραφο 003). Ο καθηγητής Edward Humphreys, το Εθνικό Κέντρο Πληροφορικής του Ηνωμένου Βασιλείου (NCC) σε συνεργασία με επαγγελματίες πάνω στην ασφάλεια πληροφοριών από την Shell, την BOC, την British Telecom, τα Marks and Spencer, την Midland Bank, την Nationwide, συμμετείχαν στην ανάπτυξη του PD003. Η συγκεκριμένη έκδοση υποστηρίχθηκε από την BP, την Aerospace, την British Steel, την Bull, την Cadbury Schweppes, την Cameron Markby Hewitt, την Chelsea Building Society, την Ciba Geigy, την Digital Equipment Corporation, το Reuters και την TSB Bank. Η BSI-DISC κυκλοφόρησε επίσης σε μερικά πολύ κομψά συνοδευτικά φυλλάδια, σένα από τα οποία (PD005) είχε ένα τακτοποιημένο διάγραμμα ροής μιας σελίδας όπου συνοψιζόταν η διαδικασία υλοποίησης το οποίο, δυστυχώς, δεν επιβίωσε σε κανένα από τα μέχρι σήμερα αρχεία του ISO27K. Το Υπουργείο Εμπορίου και Βιομηχανίας (DTI) μετεξελίχθηκε σε Υπουργείο Εμπορικών Επιχειρήσεων και Ρυθμιστικών Μεταρρυθμίσεων (Department for Business Enterprise and Regulatory Reform, BERR), το οποίο εξακολουθεί να υποστηρίζει τα πρότυπα ISO27K έως σήμερα.

4.3.4. BS7799:1995 – Αρχική Έκδοση ως Βρετανικό Πρότυπο

Το Βρετανικό Ινστιτούτο Πιστοποίησης (British Standards Institute, BSI) το οποίο σήμερα ονομάζεται BSI (Βρετανικά Πρότυπα, μέρος του ομίλου BSI)

εξέδωσε τον «DTI-Κώδικα ορθής πρακτικής (DTI-User Code of Practice)» ως το πρώτο εθνικό Βρετανικό Πρότυπο (BS-British Standard) με την ονομασία BS7799:1995-«Κώδικας πρακτικής για διαχείριση ασφαλείας πληροφοριών (Code of Practice for Information Security Management)» (Καρδάρη, 2011).

4.3.5. BS 7799 Μέρος 1: 1998 – Μετονομασία

Το προηγούμενο BS 7799 συνδυάστηκε με ένα νέο πρότυπο πιστοποίησης το οποίο αποτέλεσε το «Μέρος 2» (αργότερα έγινε ISO / IEC 27001), οπότε το αρχικό πρότυπο μετονομάστηκε «Μέρος 1» το 1998.

4.3.6. BS 7799 Μέρος 1: 1999 – Αναθεώρηση

Μετά από μια διαδικασία αναθεώρησης του BSI, το πρότυπο αναθεωρήθηκε και επανεκδόθηκε το 1999.

4.3.7. ISO / IEC 17799: 2000 - πρώτη έκδοση ISO / IEC του BS7799-1

Μετά από μια δύσκολη περίοδο διεθνούς μελέτης και αναθεώρησης, το BS 7799 Μέρος 1: 1999 υιοθετήθηκε τελικά από το ISO / IEC με διαδικασία ταχείας ενσωμάτωσης και δημοσιεύθηκε ως ISO / IEC 17799 το Δεκέμβριο του 2000. Μέλη του Διεθνή Οργανισμού Τυποποίησης - ISO, της κοινής τεχνικής επιτροπής IEC JTC1 και της Υποεπιτροπής 27 - SC 27 δεν υποστήριζαν καθολικά αυτή την πρώτη έκδοση, αλλά έγινε δεκτή ως σημείο εκκίνησης εν αναμονή περαιτέρω ανάπτυξης.

4.3.8. ISO / IEC 17799:2005

Τον Ιούνιο του 2005, η έκδοση του 2000 επικαιροποιήθηκε σημαντικά με νέα τμήματα ενοποιώντας τις συμβουλές για τη διαχείριση κινδύνων και περιστατικών και πολλές άλλες αναθεωρήσεις που εκδόθηκαν σε ολόκληρο το διάστημα. Η μορφή του τροποποιήθηκε προκειμένου να παρέχει σημειώσεις "καθοδήγησης εφαρμογής" σε κάθε έλεγχο.

4.3.9. ISO/IEC 27002:2005

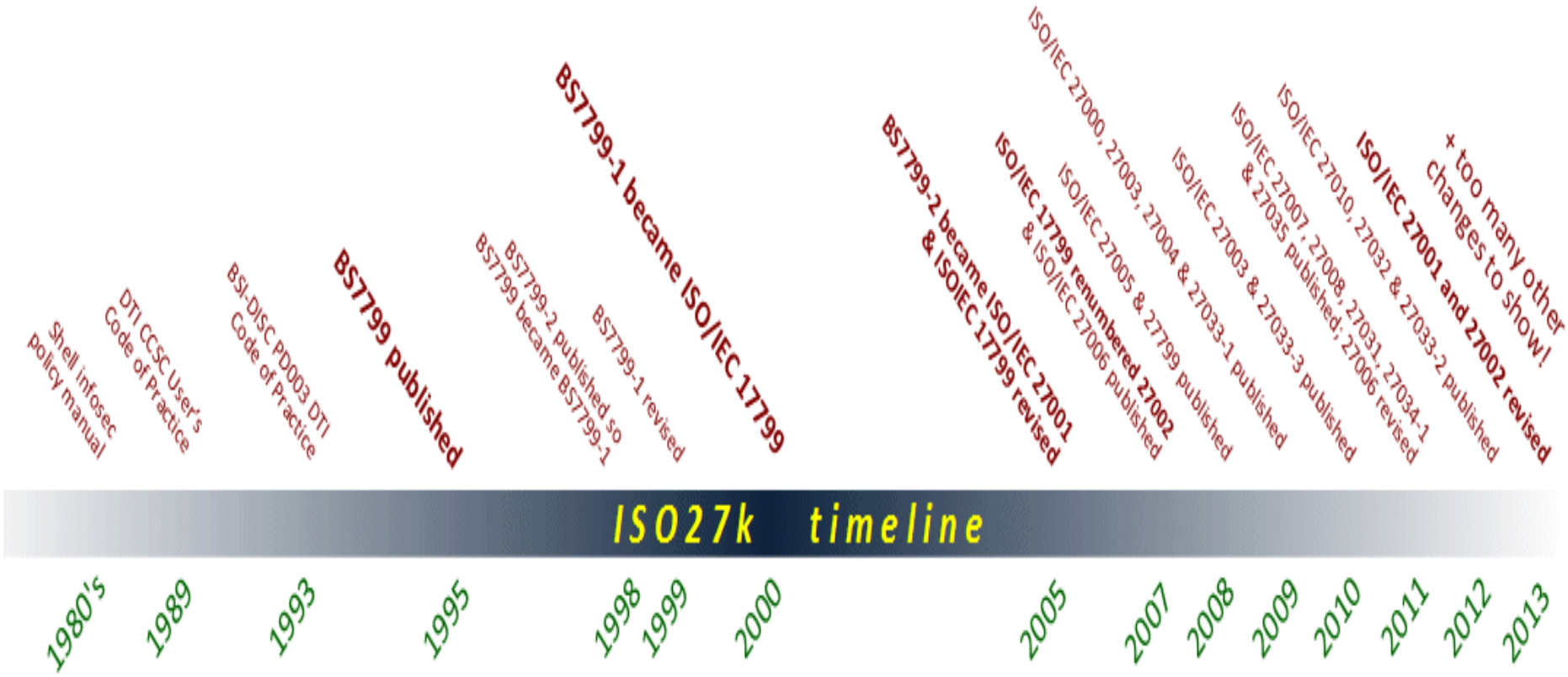
Το πρότυπο ISO / IEC 17799: 2005 αλλάζει αριθμό και γίνεται στα μέσα του 2007, ISO / IEC 27002: 2005 για να το φέρει πλέον στην οικογένεια των

προτύπων ISO / IEC 27000. Το κείμενο παραμένει κατά λέξη ταυτόσημο με το πρότυπο ISO / IEC 17799: 2005 - στην πραγματικότητα, για κάποιο διάστημα το πρότυπο ISO / IEC 17799 συνέχισε να παραδίδεται σε οποιονδήποτε ζητούσε το ISO / IEC 27002, συνοδευόμενο με ένα φύλλο επικύρωσης σημειώνοντας την αλλαγή του αριθμού.

4.3.10. ISO / IEC 27001:2013 και 27002:2013 - νέες εκδόσεις

Τα μέλη των ISO / IEC JTC1 / SC 27 αναδημοσίευσαν το αναθεωρημένο ISO / IEC 27001 και 27002 το 2013. Η διαδικασία αναθεώρησης ήταν επίπονη και αργή, ιδιαίτερα για το 27002, για το οποίο έχει καταστεί σχεδόν ανυπέρβλητη. Το 27001 αναθεωρήθηκε ουσιαστικά για να ευθυγραμμιστεί με άλλα πρότυπα συστημάτων διαχείρισης ISO. Διάφορα άλλα πρότυπα ISO27K δημοσιεύθηκαν ή ενημερώθηκαν από το 2013 έως σήμερα αλλά δεν αποτελεί σκοπό της παρούσας διπλωματικής να παρουσιαστούν.

Στο Σχήμα 4-1 παρουσιάζεται αναλυτικά η ιστορική εξέλιξη του προτύπου.



ΣΧΗΜΑ 4-1.ΙΣΤΟΡΙΚΗ ΕΞΕΛΙΞΗ ΤΟΥ ΠΡΟΤΥΠΟΥ ISO27K

(Πηγή: (ISO27K Forum, 2017))

4.4 Η σειρά των προτύπων ISO27K

Η σειρά των προτύπων ISO27K περιλαμβάνει περίπου σαράντα πρότυπα και ορισμένα τα οποία είναι υπό κατασκευή, τα περισσότερα εκ των οποίων έχουν δημοσιευθεί από τον Διεθνή Οργανισμό Τυποποίησης (ISO / IEC), όπως αυτά παρουσιάζονται αναλυτικά στον παρακάτω πίνακα:

Πρότυπο	***Εκδόθηκε***	***Τίτλος***	***Παρατηρήσεις***
ISO/IEC 27000	*2016*	*Συστήματα διαχείρισης ασφάλειας πληροφοριών - Επισκόπηση και λεξιλόγιο*	*Επισκόπηση / Εισαγωγή στα πρότυπα ISO27k συνολικά και ένα γενικότερο γλωσσάριο όρων*
ISO/IEC 27001	*2013*	*Συστήματα διαχείρισης ασφάλειας πληροφοριών - Απαιτήσεις*	*Ορίζει τυπικά ένα ISMS, σύμφωνα με το οποίο έχουν πιστοποιηθεί χιλιάδες οργανισμοί*
ISO/IEC 27002	*2013*	*Κώδικας πρακτικής για τους ελέγχους ασφάλειας πληροφοριών*	*Μια αρκετά ολοκληρωμένη σειρά στόχων ελέγχου ασφάλειας πληροφοριών και γενικά αποδεκτούς ελέγχους ορθής πρακτικής*
ISO/IEC 27003	*2017*	*Οδηγίες εφαρμογής συστήματος διαχείρισης ασφάλειας πληροφοριών*	*Συμβουλές σχετικά με την εφαρμογή του ISO27k, που επεκτείνονται από τομέα σε τομέα στο κύριο μέρος του ISO / IEC 27001*
ISO/IEC 27004	*2016*	*Διαχείριση της ασφάλειας πληροφοριών - Μετρήσεις*	*Απαιτείται η έκδοση μιας νεότερης βελτιωμένης έκδοσης*

Πρότυπο	***Εκδόθηκε***	***Τίτλος***	***Παρατηρήσεις***
ISO/IEC 27005	*2011*	*Διαχείριση κινδύνων ασφάλειας πληροφοριών*	*Συζητά τις αρχές διαχείρισης κινδύνου χωρίς να καθορίζει συγκεκριμένες μεθόδους. Δυστυχώς θεωρείται ξεπερασμένη και ατελής.*
ISO/IEC 27006	*2015*	*Απαιτήσεις για φορείς που παρέχουν έλεγχο και πιστοποίηση συστημάτων διαχείρισης της ασφάλειας των πληροφοριών*	*Τυπική καθοδήγηση για τους οργανισμούς πιστοποίησης*
ISO/IEC 27007	*2011*	*Κατευθυντήριες γραμμές για τον έλεγχο των συστημάτων διαχείρισης της ασφάλειας των πληροφοριών*	*Έλεγχος των στοιχείων συστήματος διαχείρισης του ISMS*
ISO/IEC TR 27008	*2011*	*Κατευθυντήριες γραμμές για τους ελεγκτές στους*	*Έλεγχος των στοιχείων ασφάλειας των πληροφοριών του ISMS*
		ελέγχους ασφάλειας πληροφοριών	
ISO/IEC 27009	*2016*	*Ειδική τομεακή εφαρμογή του ISO / IEC 27001 - απαιτήσεις*	*Καθοδήγηση για όσους αναπτύσσουν νέα πρότυπα ISO27k (δηλ. ISO / IEC JTC1 / SC27 – πρόκειται στην πραγματικότητα για ένα εσωτερικό έγγραφο)*

Πρότυπο	***Εκδόθηκε***	***Τίτλος***	***Παρατηρήσεις***
ISO/IEC 27010	*2015*	*Διαχείριση της ασφάλειας πληροφοριών για διατομεακές και δια-οργανωτικές επικοινωνίες*	*Η ανταλλαγή πληροφοριών για την ασφάλεια των πληροφοριών μεταξύ βιομηχανικών τομέων ή / και εθνών, ιδίως εκείνων που επηρεάζουν την "κρίσιμη υποδομή"*
ISO/IEC 27011	*2016*	*Οδηγίες διαχείρισης της ασφάλειας των πληροφοριών για οργανισμούς τηλεπικοινωνιών βάσει του ISO / IEC 27002*	*Έλεγχοι ασφάλειας πληροφοριών για τη βιομηχανία τηλεπικοινωνιών. Ονομάζεται επίσης "σύσταση ITU-T x.1051"*
ISO/IEC 27013	*2015*	*Οδηγίες για την ολοκληρωμένη εφαρμογή των προτύπων ISO / IEC 27001 και ISO / IEC 20000-1*	*Συνδυασμός ISO27k / ISMS με Διαχείριση Υπηρεσιών Πληροφορικής / ITIL*
ISO/IEC 27014	*2013*	*Διακυβέρνηση της ασφάλειας των πληροφοριών*	*Διακυβέρνηση στο πλαίσιο της ασφάλειας των πληροφοριών · Θα καλείται επίσης "σύσταση ITU-T X.1054"*
ISO/IEC TR 27015	*2012*	*Οδηγίες διαχείρισης της ασφάλειας των πληροφοριών για τις χρηματοπιστωτικές υπηρεσίες*	*Εφαρμογή του ISO27k στη χρηματοπιστωτική βιομηχανία*
ISO/IEC TR 27016	*2014*	*Διαχείριση της ασφάλειας πληροφοριών - οργανωτική οικονομία*	*Η οικονομική θεωρία εφαρμόζεται στην ασφάλεια των πληροφοριών*

Πρότυπο	***Εκδόθηκε***	***Τίτλος***	***Παρατηρήσεις***
ISO/IEC 27017	*2015*	*Κώδικας πρακτικής για ελέγχους ασφάλειας πληροφοριών για υπηρεσίες cloud computing βάσει του ISO / IEC 27002*	*Έλεγχοι ασφάλειας πληροφοριών για cloud computing*
ISO/IEC 27018	*2014*	*Κώδικας πρακτικής για τους ελέγχους για την προστασία προσωπικών πληροφοριών που υποβάλλονται σε επεξεργασία στις δημόσιες υπηρεσίες υπολογιστικού νέφους*	*Έλεγχοι απορρήτου για υπολογιστικά τύπου cloud*
ISO/IEC TR 27019	*2013*	*Κατευθυντήριες γραμμές διαχείρισης ασφάλειας πληροφοριών βασισμένες στο ISO / IEC 27002 για συστήματα ελέγχου της διαδικασίας ειδικά για την ενεργειακή βιομηχανία*	*Ασφάλεια πληροφοριών για ICS / SCADA / ενσωματωμένα συστήματα (και όχι μόνο που χρησιμοποιούνται στην ενεργειακή βιομηχανία!), Εξαιρουμένης της πυρηνικής βιομηχανίας*
ISO/IEC 27021	*ΠΡΟΣΧΕΔΙΟ*	*Απαιτήσεις ικανότητας για επαγγελματίες διαχείρισης της ασφάλειας πληροφοριών*	*Καθοδήγηση σχετικά με τις δεξιότητες και τις γνώσεις που απαιτούνται για να εργαστεί σε αυτόν τον τομέα*
ISO/IEC 27023	*2015*	*Χαρτογράφηση των αναθεωρημένων εκδόσεων ISO / IEC 27001 και ISO / IEC 2700*	*Συμβουλές για όσους επικαιροποιούν τα ISMS τους από τις εκδόσεις 2005 έως 2013*

Πρότυπο	***Εκδόθηκε***	***Τίτλος***	***Παρατηρήσεις***
ISO/IEC 27031	*2011*	*Κατευθυντήριες γραμμές για την ετοιμότητα της τεχνολογίας πληροφοριών και επικοινωνιών για τη συνέχιση της επιχειρηματικής δραστηριότητας*	*Συνέχεια (δηλαδή ανθεκτικότητα, διαχείριση συμβάντων και ανάκτηση καταστροφών) για τις ΤΠΕ, υποστηρίζοντας τη γενική επιχειρηματική συνέχεια*
ISO/IEC 27032	*2012*	*Κατευθυντήριες γραμμές για την ασφάλεια στον κυβερνοχώρο*	*Το πρότυπο αυτό φορά την ασφάλεια του Διαδικτύου*
ISO/IEC 27033	*-1 2015*	*Επισκόπηση και έννοιες ασφάλειας δικτύων*	*Διάφορες πτυχές της ασφάλειας του δικτύου, ενημέρωση και αντικατάσταση του ISO / IEC 18028*
	-2 2012	*Κατευθυντήριες γραμμές για το σχεδιασμό και την υλοποίηση της ασφάλειας του δικτύου*	
	-3 2010	*Σενάρια αναφοράς δικτύωσης - απειλές, τεχνικές σχεδιασμού και θέματα ελέγχου*	
	-4 2014	*Διασφάλιση επικοινωνιών μεταξύ δικτύων που χρησιμοποιούν πύλες ασφαλείας*	
	-5 2013	*Διασφάλιση επικοινωνιών μεταξύ δικτύων με τη χρήση εικονικών ιδιωτικών δικτύων (VPN)*	
	-6 2016	*Ασφάλεια πρόσβασης ασύρματου δικτύου IP*	

Πρότυπο	***Εκδόθηκε***	***Τίτλος***	***Παρατηρήσεις***
ISO/IEC 27034	*-1 2011*	*Ασφάλεια εφαρμογών - Επισκόπηση και έννοιες*	*Πρότυπο ασφαλείας πολλαπλών εφαρμογών*
	-2 2015	*Κανονιστικό πλαίσιο οργανισμού*	
	-3 ΠΡΟΣΧΕΔΙΟ	*Διαδικασία διαχείρισης ασφάλειας εφαρμογών*	*Προωθεί την έννοια μιας επαναχρησιμοποιήσιμης βιβλιοθήκης λειτουργιών ελέγχου ασφάλειας πληροφοριών, που καθορίζεται επισήμως, σχεδιάζεται και δοκιμάζεται*
	-4 ΠΡΟΣΧΕΔΙΟ	*Επικύρωση ασφάλειας εφαρμογών*	
	-5 ΠΡΟΣΧΕΔΙΟ	*Πρωτόκολλα και δομή δεδομένων για τον έλεγχο της ασφάλειας των εφαρμογών*	
	-6 2016	*Μελέτη υποθέσεων*	
	-7 ΠΡΟΣΧΕΔΙΟ	*Πλαίσιο πρόβλεψης διασφάλισης ασφάλειας εφαρμογών*	
ISO/IEC 27035	*-1 2016*	*Διαχείριση περιστατικών ασφάλειας πληροφοριών - Αρχές διαχείρισης περιστατικών*	*Replaced ISO TR 18044*
	-2 2016	*Κατευθυντήριες γραμμές για το σχεδιασμό και την προετοιμασία για την αντιμετώπιση περιστατικών*	

Πρότυπο	***Εκδόθηκε***	***Τίτλος***	***Παρατηρήσεις***
	-3 ΠΡΟΣΧΕΔΙΟ	*Κατευθυντήριες γραμμές για επιχειρήσεις αντιμετώπισης περιστατικών ΤΠΕ*	*Το σχέδιο σύνταξης του μέρους 3 ακυρώθηκε και ξαναξεκίνησε*
ISO/IEC 27036	*-1 2014*	*Ασφάλεια πληροφοριών για τις σχέσεις προμηθευτών - Επισκόπηση και έννοιες*	*Θέματα της ασφάλειας των πληροφοριών των ΤΠΕ από εξωτερικές πηγές και υπηρεσίες*
	-2 2014	*Κοινές απαιτήσεις*	
	-3 2013	*Κατευθυντήριες γραμμές για την τροφοδότηση της αλυσίδας ασφαλείας σε ΤΠΕ*	
	-4 2016	*Κατευθυντήριες γραμμές για την ασφάλεια υπηρεσιών cloud*	
ISO/IEC 27037	*2012*	*Κατευθυντήριες γραμμές για τον προσδιορισμό, τη συλλογή, την απόκτηση και τη διατήρηση ψηφιακών αποδεικτικών στοιχείων*	*Πρώτο από πολλά πρότυπα εγκληματολογικής πληροφορικής - δείτε επίσης 27042 και άλλα*
ISO/IEC 27038	*2014*	*Προδιαγραφές για ψηφιακή επεξεργασία*	*Σύνταξη ψηφιακών εγγράφων*

Πρότυπο	***Εκδόθηκε***	***Τίτλος***	***Παρατηρήσεις***
ISO/IEC 27039	*2015*	*Επιλογή, εγκατάσταση και λειτουργία συστημάτων ανίχνευσης και πρόληψης εισβολής (Intrusion Detection and Prevention Systems, IDPS)*	*IDS/IPS*
ISO/IEC 27040	*2015*	*Ασφάλεια αποθήκευσης*	*Ασφάλεια πληροφοριακών συστημάτων για αποθηκευμένα δεδομένα*
ISO/IEC 27041	*2015*	*Κατευθυντήριες γραμμές για τη διασφάλιση της καταλληλότητας και της επάρκειας των μεθόδων διερεύνησης περιστατικών*	*Η διασφάλιση της ακεραιότητας των εγκληματολογικών στοιχείων είναι απολύτως ζωτική*
ISO/IEC 27042	*2015*	*Κατευθυντήριες γραμμές για την ανάλυση και ερμηνεία των ψηφιακών αποδείξεων*	*Αναλυτικές μεθόδους Πληροφοριακών Συστημάτων εγκληματολογίας*
ISO/IEC 27043	*2015*	*Αρχές και διαδικασίες διερεύνησης περιστατικών*	*Οι βασικές αρχές της ηλεκτρονικής εγκληματολογίας*
ISO/IEC 27050	*-1 2016*	*Ηλεκτρονική ανακάλυψη - επισκόπηση και έννοιες*	*Περισσότερες πληροφορίες για την ηλεκτρονική εγκληματολογίας στα μέρη 3+(ένα 4^{ο} είναι πιθανό)*

Πρότυπο	*Εκδόθηκε*	*Τίτλος*	*Παρατηρήσεις*
	-2 ΠΡΟΣΧΕΔΙΟ	*-Καθοδήγηση για τη διακυβέρνηση και τη διαχείριση της ηλεκτρονικής ανακάλυψης*	*Συμβουλές για την αντιμετώπιση των κινδύνων που σχετίζονται με την εγκληματολογία*
	-3 ΠΡΟΣΧΕΔΙΟ	*Κώδικας πρακτικής για την ηλεκτρονική ανακάλυψη*	*Ένας οδηγός πώς να το κάνεις*
ISO/IEC PDTR 27103	*ΠΡΟΣΧΕΔΙΟ*	*Κυβερνοασφάλεια*	*Θα παρέχει συμβουλές για την ασφάλεια των πληροφοριών σε επαγγελματίες*
ISO 27799	*2016*	*Υγειονομική πληροφορική - Διαχείριση της ασφάλειας των πληροφοριών στην υγεία με τη χρήση του ISO / IEC 27002*	*Συμβουλές ασφάλειας πληροφοριών για τον κλάδο της υγείας*

ΠΙΝΑΚΑΣ 4.1. ΤΑ ΠΡΟΤΥΠΑ ΚΑΙ ΤΑ ΠΡΟΣΧΕΔΙΑ ΤΗΣ ΣΕΙΡΑΣ ISO27K

(Πηγή: (ISO27K Forum, 2017))

Παρατηρούμε ότι η σειρά έχει σκόπιμα ένα ευρύ πεδίο εφαρμογής προκειμένου να είναι εφαρμόσιμη σε οργανισμούς όλων των σχημάτων και μεγεθών. Όλοι οι οργανισμοί καλούνται να αξιολογήσουν τους κινδύνους ασφάλειας των πληροφοριών τους, στην συνέχεια, να εφαρμόσουν κατάλληλους ελέγχους ασφάλειας των πληροφοριών σύμφωνα με τις ανάγκες τους χρησιμοποιώντας τις κατευθύνσεις και τις προτάσεις των προτύπων κατά περίπτωση.

4.5 ISO / IEC 27000: 2016

Το ISO/IEC 27000:2016 είναι ένα πολύ πρόσφατο πρότυπο η δομή του οποίου παρουσιάζεται παρακάτω (ISO/IEC 27000, 2016):

4.5.1. Εισαγωγή και πεδίο εφαρμογής

Το ISO / IEC 27000 παρέχει μια επισκόπηση των Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών – ΣΔΑΠ (ISMS) (και ως εκ τούτου και των προτύπων ISO27K) και "καθορίζει συναφείς όρους" δηλαδή είναι ένα γλωσσάριο που ορίζει τυπικά και ρητά πολλούς ειδικούς όρους όπως χρησιμοποιούνται στα πρότυπα ISO27K.

4.5.2. ISMS / ISO27K τμήμα λεξιλογίου

Το λεξιλόγιο ή το γλωσσάριο των προσεκτικά διατυπωμένων τυπικών ορισμών καλύπτει τους περισσότερους από τους εξειδικευμένους όρους της ασφάλειας πληροφοριών που χρησιμοποιούνται στα πρότυπα ISO27K. Η ασφάλεια των πληροφοριών, όπως και στα περισσότερα τεχνικά θέματα, χρησιμοποιεί ένα πολύπλοκο δίκτυο ορολογίας που εξελίσσεται συνεχώς. Αρκετοί βασικοί όροι στην ασφάλεια πληροφοριών (όπως π.χ. "ο κίνδυνος") έχουν διαφορετικές έννοιες ή ερμηνείες ανάλογα με το πλαίσιο, την πρόθεση του δημιουργού και τις προκαταλήψεις του αναγνώστη. Λίγοι συγγραφείς καθορίζουν με ακρίβεια τι εννοούν, αλλά αυτή η ασάφεια οδηγεί σε σύγχυση. Εκτός από οτιδήποτε άλλο, θα ήταν δύσκολο να εκτιμηθεί και να πιστοποιηθεί η συμμόρφωση με το πρότυπο ISO / IEC 27001 εάν οι ειδικοί όροι σήμαιναν διαφορετικά πράγματα στους αξιολογητές και τους αξιολογούμενους.

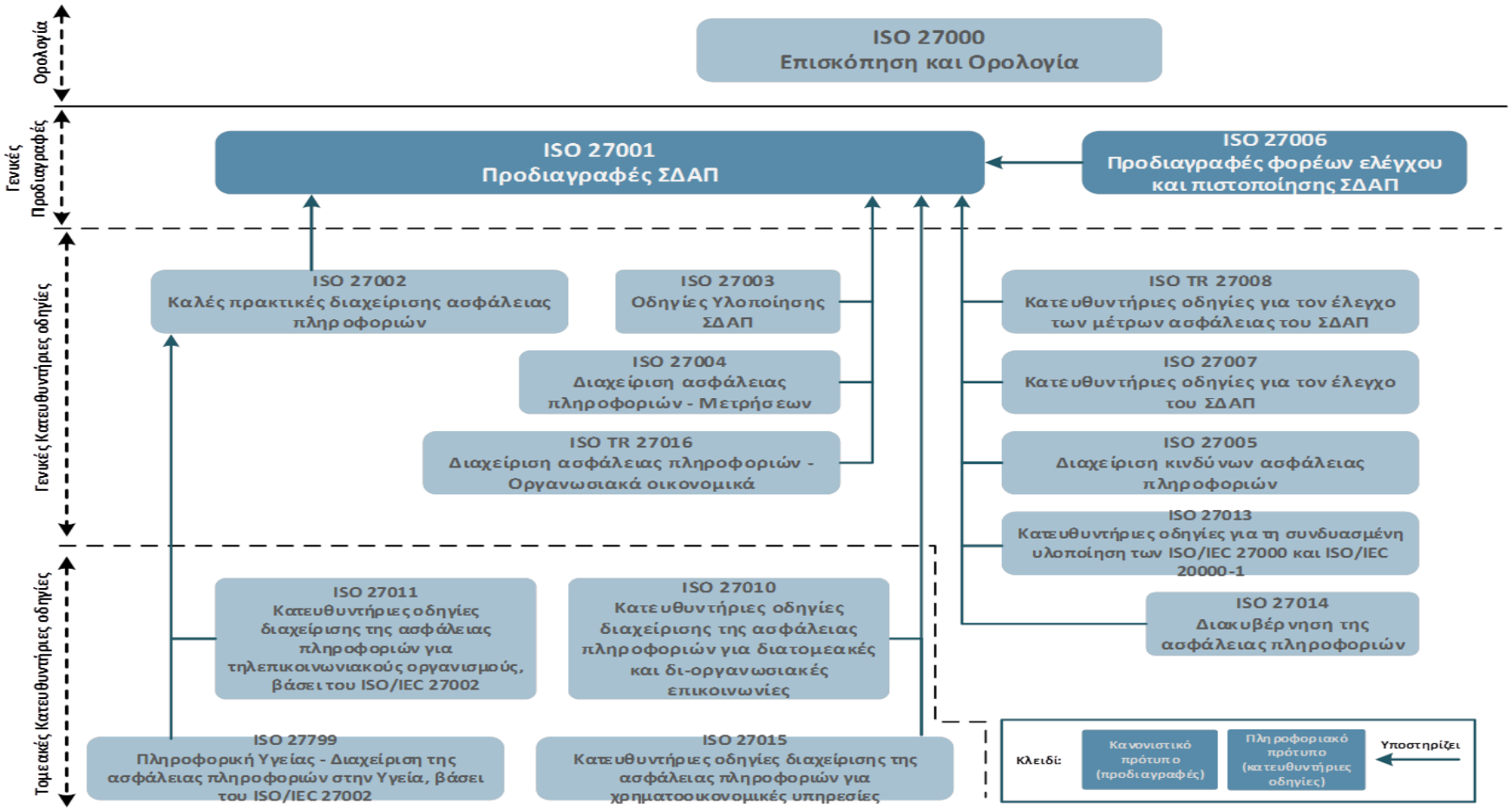
Το λεξιλόγιο στο ISO / IEC 27000 εξαπλώνεται σταδιακά σε ολόκληρο τον κλάδο της παγκόσμιας ασφάλειας πληροφοριών, αν και ορισμένα άτομα και ομάδες διαφέρουν, μερικές φορές με βάσιμους λόγους, δημιουργώντας περιστασιακές παρεξηγήσεις, συγκρούσεις και εννοιολογικά χάσματα. Ακόμα και αν υπάρχουν διαφωνίες με τους ορισμούς, αξίζει να εξοικειωθεί κάποιος με αυτούς καθώς όλο και περισσότεροι επαγγελματίες δέχονται σιωπηρά τις εκδόσεις ISO / IEC.

Το ISO / IEC 27000 αντικαθιστά σε μεγάλο βαθμό τον ISO / IEC Οδηγός 2: 1996 «Τυποποίηση και συναφείς δραστηριότητες - Γενικό λεξιλόγιο», ISO Οδηγός 73: 2009 «Διαχείριση κινδύνων - Λεξιλόγιο - Κατευθυντήριες γραμμές για χρήση στα πρότυπα» και ISO / IEC 2382-8: Τεχνολογία πληροφοριών - λεξιλόγιο Μέρος 8: Ασφάλεια». Περιλαμβάνει επίσης ορισμούς που λαμβάνονται από μερικά άλλα

πρότυπα ISO εκτός των προτύπων ISO27K. Οι όροι που αναπαράγονται αυτούσιοι από άλλα πρότυπα ISO όπως το ISO 9000 δεν είναι πάντοτε εξ' ολοκλήρου κατάλληλοι στο πλαίσιο εφαρμογής της ασφάλειας των πληροφοριών για τον λόγο αυτό δεν χρησιμοποιούνται απαραίτητα στα πρότυπα ISO27K σε πλήρη συμφωνία με τους αρχικούς ορισμούς ή τις προτεινόμενες έννοιες. Ωστόσο, καθώς οι ορισμοί ενημερώνονται ή αντικαθίστανται σταδιακά, το λεξικό εξελίσσεται σε μια λογική συνεκτική και σταθερή κατάσταση σε ολόκληρη την οικογένεια των προτύπων ISO27K - ένα αξιοσημείωτο επίτευγμα από μόνο του, δεδομένου των πρακτικών δυσκολιών συντονισμού στην προσπάθεια συλλογής πληροφοριών από ξεχωριστές επιτροπές, την επεξεργασία των έργων, των εκδοτών και των διαχειριστών στην ανάπτυξη της γλώσσας και των εννοιών.

4.5.3. ISMS / ISO27K τμήμα επισκόπησης

Η επισκόπηση των ΣΔΑΠ - ISMS μας εισάγει στην ασφάλεια πληροφοριών, διαχείριση κινδύνων και ασφάλειας και συστήματα διαχείρισης. Πρόκειται για μια αρκετά σαφή περιγραφή και προσέγγιση των προτύπων ISO27K. Επίσης, υπάρχει ένα διάγραμμα (Σχήμα 4-2), στο οποίο φαίνεται η ομαδοποίηση και η σχέση των προτύπων ISO27K.



ΣΧΗΜΑ 4-2.Η ΟΙΚΟΓΕΝΕΙΑ ΤΩΝ ΠΡΟΤΥΠΩΝ ΣΔΑΠ ΚΑΙ ΟΙ ΣΧΕΣΕΙΣ ΜΕΤΑΞΥ ΤΟΥΣ.

Πηγή: (Κάτσικας Σ. , 2016)

4.6 ISO / IEC 27001:2013

Το ISO/IEC 27001:2013 έχει πολύ πρόσφατα αναθεωρηθεί και αυτό, η δομή του οποίου παρουσιάζεται παρακάτω (ISO/IEC 27001, 2013); (Iso27001security.com, 2017):

4.6.1. Εισαγωγή

Η αναθεωρημένη έκδοση του προτύπου ISO 27001 δημοσιεύθηκε το 2013 υπό τον τίτλο "Τεχνολογία πληροφοριών - Τεχνικές ασφαλείας - Συστήματα διαχείρισης ασφάλειας πληροφοριών - Απαιτήσεις ". Η βασική του δομή έχει αναθεωρηθεί προκειμένου να ευθυγραμμιστεί με το Παράρτημα SL μέρος 1 των οδηγιών ISO / IEC. Στόχος είναι όλα τα πρότυπα συστημάτων διαχείρισης να υιοθετήσουν αυτόν τον τύπο κατά την επόμενη αναθεώρησή τους. Οι κύριοι αριθμοί και τίτλοι όλων των προτύπων διαχείρισης συστημάτων ISO θα παραμείνουν οι ίδιοι ενώ η εισαγωγή, το πεδίο εφαρμογής και κανονιστικές παραπομπές θα περιλαμβάνουν συγκεκριμένες λεπτομέρειες για την πειθαρχία. Αυτό θα δημιουργήσει μεγαλύτερη συνοχή για οργανισμούς που έχουν ολοκληρωμένα συστήματα διαχείρισης που καλύπτουν πολλαπλά πρότυπα, όπως είναι το ISO 9001, Ποιότητα Συστημάτων Διαχείρισης και το ISO 14001, Περιβαλλοντικά Συστήματα Διαχείρισης

Το πρότυπο ISO / IEC 27001 καθορίζει επισήμως ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών ΣΔΑΠ – ISMS (Information Security Management System), ένα σύνολο δραστηριοτήτων σχετικά με τη διαχείριση των κινδύνων πληροφόρησης (που ονομάζεται «κίνδυνοι ασφάλειας πληροφοριών» στο πρότυπο). Το ΣΔΑΠ – ISMS είναι ένα γενικό πλαίσιο διαχείρισης μέσω του οποίου ο οργανισμός ή επιχείρηση εντοπίζει, αναλύει και αντιμετωπίζει τους κινδύνους πληροφόρησης και να διασφαλίζει ότι οι ρυθμίσεις ασφαλείας προσαρμόζονται με τέτοιο τρόπο ώστε να συμβαδίζουν με τις αλλαγές στις απειλές για την ασφάλεια, τις ευπάθειες και τις επιπτώσεις στον οργανισμό ή την επιχείρηση - σημαντική πτυχή σε ένα τόσο δυναμικό τομέα και βασικό πλεονέκτημα της ευέλικτης προσέγγισης στην διαχείριση του κινδύνου της σειράς προτύπων ISO27K , σε αντίθεση με άλλα πρότυπα όπως είναι π.χ.το Payment Card Industry Data Security Standard (PCI-DSS).

Το πρότυπο καλύπτει όλους τους τύπους οργανισμών (π.χ. εμπορικές επιχειρήσεις, κυβερνητικούς οργανισμούς, μη κερδοσκοπικούς οργανισμούς), όλων των μεγεθών (από τις πολύ μικρές επιχειρήσεις έως τις τεράστιες πολυεθνικές) και όλους τους κλάδους ή αγορές (λιανικό εμπόριο).

Το ISO / IEC 27001 δεν επιβάλλει επίσημα συγκεκριμένους ελέγχους ασφάλειας πληροφοριών, καθώς οι έλεγχοι που απαιτούνται ποικίλλουν σημαντικά σε όλο το εύρος των οργανισμών που υιοθετούν το πρότυπο. Οι έλεγχοι ασφάλειας πληροφοριών από το ISO / IEC 27002 σημειώνονται στο παράρτημα A του ISO / IEC 27001, μάλλον σαν ένα μενού. Οι οργανισμοί που υιοθετούν το ISO / IEC 27001 είναι ελεύθεροι να επιλέξουν ποιοι συγκεκριμένοι έλεγχοι ασφάλειας πληροφοριών εφαρμόζονται στους ιδιαίτερους κινδύνους πληροφόρησης τους, βασιζόμενοι σε εκείνους που παρατίθενται στο μενού και ενδεχομένως συμπληρώνοντάς τους με άλλες επιλογές a la carte (ορισμένες φορές γνωστές ως εκτεταμένες ομάδες ελέγχου). Όπως και με το πρότυπο ISO / IEC 27002, το κλειδί για την επιλογή των εφαρμοστέων ελέγχων είναι η διεξοδική αξιολόγηση των κινδύνων πληροφόρησης του οργανισμού, που είναι ένα ζωτικό μέρος του ISMS.

Επιπλέον, η διοίκηση μπορεί να επιλέξει να αποφεύγει, να μεταφέρει ή να δέχεται κινδύνους πληροφόρησης αντί να τις μετριάζει μέσω ελέγχων - μια απόφαση αντιμετώπισης κινδύνου στο πλαίσιο της διαδικασίας διαχείρισης κινδύνου.

4.6.2. <u>Δομή του Προτύπου</u>

Το ISO / IEC 27001: 2013 έχει τις ακόλουθες ενότητες:

1. ***Εισαγωγή*** – γίνεται μια προσέγγιση της διαδικασίας.
2. ***Πεδίο εφαρμογής*** - καθορίζει γενικές απαιτήσεις ISMS κατάλληλες για οργανισμούς οποιουδήποτε τύπου, μεγέθους ή φύσης.
3. ***Κανονιστικές αναφορές*** - μόνο το ISO / IEC 27000 θεωρείται απολύτως απαραίτητο για τους χρήστες του 27001: τα υπόλοιπα πρότυπα ISO27K είναι προαιρετικά.

4. ***Όροι και ορισμοί*** - ένα σύντομο, επίσημο γλωσσάριο, το οποίο αντικαταστάθηκε στην πορεία από το ISO / IEC 27000:2016.

5. ***Πλαίσιο του οργανισμού*** - κατανόηση του οργανωτικού πλαισίου, των αναγκών και των προσδοκιών των «ενδιαφερομένων» και ο καθορισμός του πεδίου εφαρμογής του ΣΔΑΠ - ISMS. Η ενότητα 4.4 δηλώνει πολύ ξεκάθαρα ότι "Ο οργανισμός δημιουργεί, εφαρμόζει, διατηρεί και συνεχώς βελτιώνει" ένα συμμορφούμενο ΣΔΑΠ - ISMS.

6. ***Ηγεσία*** - η ανώτατη διοίκηση πρέπει να επιδεικνύει ηγετική θέση και δέσμευση στο ΣΔΑΠ - ISMS, να δίνει πολιτικές εντολές και να αναθέτει ρόλους, αρμοδιότητες και αρχές επί της ασφάλειας πληροφοριών.

7. ***Σχεδιασμός*** - περιγράφει τη διαδικασία για την αναγνώριση, την ανάλυση και τον σχεδιασμό αντιμετώπισης των κινδύνων πληροφόρησης και την αποσαφήνιση των στόχων της ασφάλειας των πληροφοριών.

8. ***Υποστήριξη*** - πρέπει να διατεθούν επαρκείς πόρους, αυξημένη επαγρύπνηση, να ετοιμασθούν και να ελεγχθούν τα έγγραφα.

9. ***Λειτουργία*** - λίγο πιο λεπτομερές σχετικά με την αξιολόγηση και την αντιμετώπιση των κινδύνων πληροφόρησης, τη διαχείριση των αλλαγών και την τεκμηρίωση των εγγράφων (εν μέρει έτσι ώστε να μπορούν να ελεγχθούν από τους ελεγκτές πιστοποίησης).

10. ***Αξιολόγηση της απόδοσης*** - παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση / έλεγχος / επανεξέταση των ελέγχων, διαδικασιών και συστήματος διαχείρισης της ασφάλειας των πληροφοριών, προκειμένου να γίνονται συστηματικές βελτιώσεις, όπου ενδείκνυται.

11. ***Βελτίωση*** - να αξιολογηθούν τα ευρήματα των ελέγχων και των αναθεωρήσεων (π.χ. μη συμμορφώσεις και διορθωτικές ενέργειες), να γίνουν συνεχείς βελτιώσεις στο ΣΔΑΠ – ISMS.

12. ***Παράρτημα Α*** **Έλεγχοι και στόχοι αναφοράς** - κάτι παραπάνω από έναν κατάλογο τίτλων των τμημάτων ελέγχου του ISO / IEC 27002. Το παράρτημα είναι «κανονιστικό», υποδηλώνοντας ότι οι πιστοποιημένοι οργανισμοί

αναμένεται να το χρησιμοποιήσουν, αλλά είναι ελεύθεροι να αποκλίνουν από αυτό ή να το συμπληρώσουν, προκειμένου να αντιμετωπίσουν ιδιαίτερους κινδύνους στην ασφάλεια πληροφοριών.

13. ***Βιβλιογραφία*** - υποδεικνύει στους αναγνώστες τα πέντε σχετικά πρότυπα, καθώς και το μέρος 1 των οδηγιών ISO / IEC, για περισσότερες πληροφορίες. Επιπλέον, το ISO / IEC 27000 αναγνωρίζεται στο σώμα του προτύπου ως κανονιστικό (δηλαδή βασικό) πρότυπο και υπάρχουν πολλές αναφορές στο ISO 31000 για τη διαχείριση κινδύνου.

4.6.3. <u>Υποχρεωτικές απαιτήσεις πιστοποίησης</u>

Το ISO / IEC 27001 είναι μια τυποποιημένη προδιαγραφή για ένα ΣΔΑΠ - ISMS με δύο διακριτούς σκοπούς:

- ✓ Καθορίζει, σε αρκετά υψηλό επίπεδο, τι μπορεί να κάνει ένας οργανισμός για την εφαρμογή ενός ΣΔΑΠ - ISMS.
- ✓ Μπορεί (προαιρετικά) να χρησιμοποιηθεί ως βάση για την επίσημη αξιολόγηση συμμόρφωσης από διαπιστευμένους ελεγκτές πιστοποίησης, προκειμένου να πιστοποιηθεί ένας οργανισμός.

Η ακόλουθη υποχρεωτική τεκμηρίωση (ή μάλλον «τεκμηριωμένη πληροφορία» στην γλώσσα του προτύπου) απαιτείται ρητώς για την πιστοποίηση:

1) Το πεδίο εφαρμογής του ΣΔΑΠ - ISMS (σύμφωνα με το άρθρο 4.3)
2) Πολιτική ασφάλειας πληροφοριών (ρήτρα 5.2)
3) Διαδικασία αξιολόγησης του κινδύνου πληροφοριών (ρήτρα 6.1.2)
4) Διαδικασία επεξεργασίας κινδύνου πληροφοριών (ρήτρα 6.1.3)
5) Στόχοι ασφάλειας πληροφοριών (άρθρο 6.2)
6) Απόδειξη της ικανότητας των ατόμων που εργάζονται στην ασφάλεια των πληροφοριών (ρήτρα 7.2)

7) Άλλα έγγραφα που σχετίζονται με το ISMS και θεωρούνται απαραίτητα από τον οργανισμό (ρήτρα 7.5.1β)

8) Έγγραφα επιχειρησιακού προγραμματισμού και ελέγχου (ρήτρα 8.1)

9) Τα αποτελέσματα των αξιολογήσεων κινδύνου (ρήτρα 8.2)

10) Οι αποφάσεις σχετικά με την αντιμετώπιση κινδύνων (ρήτρα 8.3)

11) Στοιχεία παρακολούθησης και μέτρησης της ασφάλειας των πληροφοριών (ρήτρα 9.1)

12) Το πρόγραμμα εσωτερικού ελέγχου του ISMS και τα αποτελέσματα των ελέγχων που πραγματοποιήθηκαν (ρήτρα 9.2)

13) Στοιχεία των επισκοπήσεων κορυφαίας διαχείρισης του ISMS (ρήτρα 9.3)

14) Αποδεικτικά στοιχεία διαπιστωθέντων μη συμμορφώσεων και διορθωτικών ενεργειών (ρήτρα 10.1)

15) Διάφορα άλλα: Το Παράρτημα Α, το οποίο είναι κανονιστικό, αναφέρει αλλά δεν καθορίζει πλήρως περαιτέρω έγγραφα, συμπεριλαμβανομένων των κανόνων για την αποδεκτή χρήση περιουσιακών στοιχείων, την πολιτική ελέγχου πρόσβασης, τις διαδικασίες λειτουργίας, τις συμφωνίες εμπιστευτικότητας ή μη αποκάλυψης, σχέσεις προμηθευτών, διαδικασίες αντιμετώπισης περιστατικών ασφάλειας πληροφοριών, συναφείς νόμους, κανονισμούς και συμβατικές υποχρεώσεις καθώς και τις σχετικές διαδικασίες συμμόρφωσης και διαδικασίες συνέχειας της ασφάλειας των πληροφοριών.

Οι ελεγκτές πιστοποίησης θα ελέγξουν σίγουρα ότι αυτοί οι δεκαπέντε τύποι τεκμηρίωσης είναι (α) παρόντες και (β) είναι κατάλληλοι για το σκοπό. Το πρότυπο δεν διευκρινίζει επακριβώς τη μορφή της τεκμηρίωσης, αλλά το τμήμα 7.5.2 μιλά για λεπτομέρειες όπως τίτλους, συγγραφείς, μορφότυπα, μέσα, αναθεωρήσεις και εγκρίσεις, ενώ το 7.5.3 αφορά τον έλεγχο των εγγράφων προσεγγίζοντας στο στυλ ένα αρκετά τυπικό ISO 9000. Η ηλεκτρονική τεκμηρίωση (όπως οι σελίδες intranet) είναι εξίσου καλή με τα έγγραφα σε χαρτί, στην πραγματικότητα καλύτερη με την έννοια ότι είναι πιο εύκολο να ελέγχονται.

4.6.4. Το πεδίο εφαρμογής ΣΔΑΠ - ISMS και Δήλωση Εφαρμοσιμότητας – SoA (Statement of Applicability)

Ενώ το πρότυπο προορίζεται να οδηγήσει στην υλοποίηση ενός ΣΔΑΠ - ISMS σε επίπεδο επιχείρησης, εξασφαλίζοντας ότι όλα τα μέρη του οργανισμού επωφελούνται αντιμετωπίζοντας τους κινδύνους πληροφόρησης με κατάλληλο και συστηματικό διαχειριζόμενο τρόπο, οι οργανισμοί μπορούν να εμβαθύνουν το ΣΔΑΠ - ISMS τους σε γενικές γραμμές ή όσο πιο στενά επιθυμούν - πράγματι, το πεδίο εφαρμογής είναι μια κρίσιμη απόφαση για ανώτερα στελέχη (άρθρο 4.3). Ένα τεκμηριωμένο έγγραφο του πεδίου εφαρμογής ενός ΣΔΑΠ - ISMS είναι μία από τις υποχρεωτικές απαιτήσεις για την πιστοποίηση.

Παρόλο που η "Δήλωση της Εφαρμοσιμότητας" (Statement of Applicability, SoA) δεν ορίζεται ρητά, αποτελεί υποχρεωτική απαίτηση του Κεφαλαίου 6.1.3. Αυτός ο συνήθης όρος αναφέρεται στην παραγωγή από τις αξιολογήσεις κινδύνου πληροφοριών και ειδικότερα, στις αποφάσεις σχετικά με την αντιμετώπιση αυτών των κινδύνων. Η Δήλωση της Εφαρμοσιμότητας - SoA μπορεί, για παράδειγμα, να λάβει τη μορφή ενός πίνακα που προσδιορίζει διάφορους τύπους κινδύνων πληροφόρησης στον έναν άξονα του και εναλλακτικές επιλογές αντιμετώπισης κινδύνου από τον άλλο, δείχνοντας πώς πρέπει να αντιμετωπίζονται οι κίνδυνοι στον οργανισμό και ποιος είναι υπεύθυνος γι 'αυτούς. Συνήθως αναφέρει τους σχετικούς ελέγχους από το ISO / IEC 27002, αλλά ο οργανισμός μπορεί να χρησιμοποιεί διαφορετικό πλαίσιο όπως το NIST SP800-55, το πρότυπο ISF, το BMIS ή / και το COBIT ή μια προσαρμοσμένη προσέγγιση. Οι στόχοι και οι έλεγχοι της ασφάλειας της πληροφόρησης από το ISO / IEC 27002 παρέχονται ως κατάλογος ελέγχου στο παράρτημα Α προκειμένου να αποφευχθεί η «παραβίαση των απαραίτητων ελέγχων».

Το πεδίο εφαρμογής του ΣΔΑΠ - ISMS και της Δήλωσης της Εφαρμογής - SoA είναι κρίσιμης σημασίας εάν ένας τρίτος σκοπεύει να αποδώσει οποιαδήποτε εξάρτηση από το πιστοποιητικό συμμόρφωσης ISO / IEC 27001 ενός οργανισμού. Εάν το πεδίο εφαρμογής του ISO / IEC 27001 ενός οργανισμού σημειώνει μόνο το "Επιχείρηση Α.Ε. Τμήμα Χ", για παράδειγμα, το σχετικό πιστοποιητικό δεν λέει απολύτως τίποτα για την κατάσταση της ασφάλειας των πληροφοριών στην

"Επιχείρηση Α.Ε. Τμήμα Υ" ή γενικά σε ολόκληρη την "Επιχείρηση Α.Ε." (Iso27001security.com, 2017).

Ομοίως, εάν για κάποιο λόγο η διοίκηση ενός οργανισμού αποφασίσει να δεχθεί κινδύνους κακόβουλου λογισμικού χωρίς να εφαρμόσει συμβατικούς ελέγχους προστασίας από ιούς, οι ελεγκτές πιστοποίησης μπορούν να αμφισβητήσουν έναν τόσο τολμηρό ισχυρισμό, αλλά εφόσον οι σχετικές αναλύσεις και αποφάσεις ήταν σωστές, αυτό από μόνο του δεν θα ήταν δικαιολογία να αρνηθούν να τον πιστοποιήσουν δεδομένου ότι οι έλεγχοι προστασίας από ιούς δεν είναι στην πραγματικότητα υποχρεωτικοί.

4.6.5. Μετρήσεις

Στην πραγματικότητα χωρίς να χρησιμοποιείται ο όρος "μετρήσεις", η έκδοση του προτύπου 2013 απαιτεί τη χρήση μετρήσεων σχετικά με την απόδοση και την αποτελεσματικότητα των ΣΔΑΠ - ISMS και των στοιχείων ελέγχου ασφαλείας των οργανισμών. Το τμήμα 9, "Αξιολόγηση απόδοσης", απαιτεί από τον οργανισμό να καθορίζει και να εφαρμόζει τις κατάλληλες μετρήσεις ασφάλειας αλλά δίνει μόνο απαιτήσεις υψηλού επιπέδου.

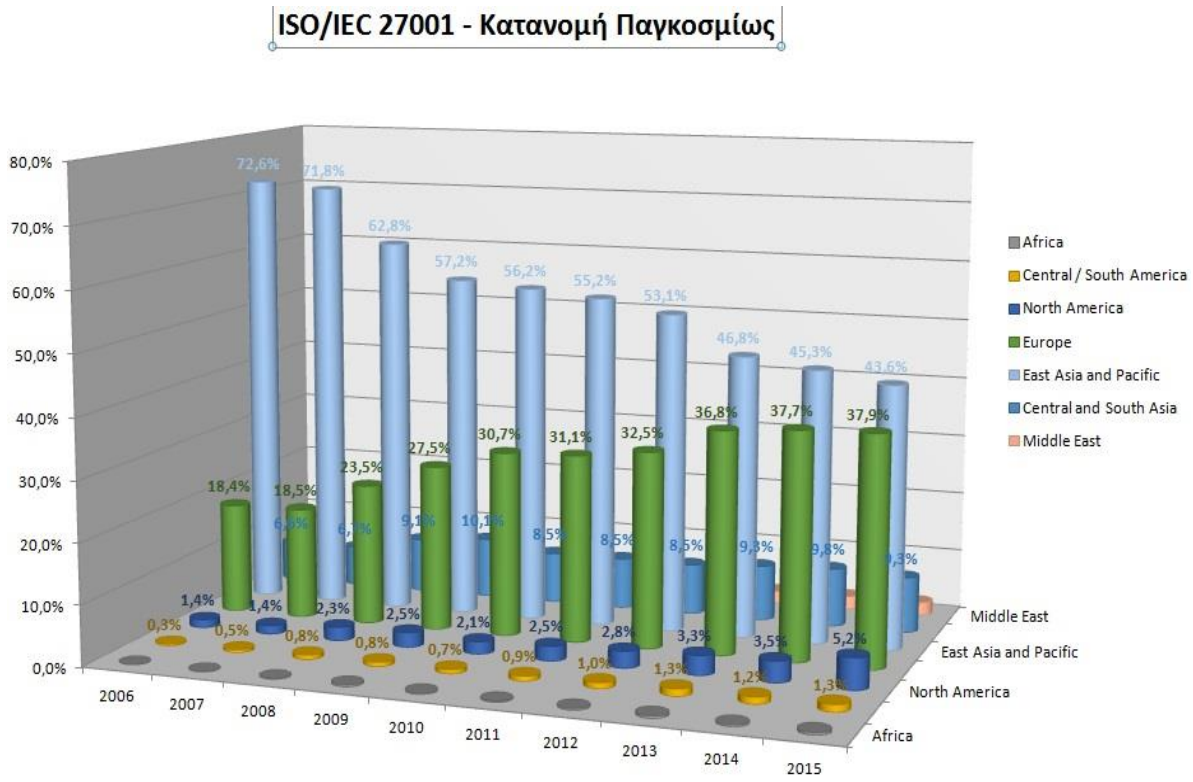
Όταν εκδοθεί η αναθεωρημένη έκδοση, το ISO / IEC 27004 θα παρέχει συμβουλές σχετικά με το τι και πώς θα μετρηθεί προκειμένου να ικανοποιηθεί η απαίτηση.

4.6.6. Γενικά επί της πιστοποίησης

Η πιστοποίηση της συμμόρφωσης κατά ISO / IEC 27001 από διαπιστευμένο και σεβαστό οργανισμό πιστοποίησης είναι εξ' ολοκλήρου προαιρετική, αλλά απαιτείται όλο και περισσότερο από τους προμηθευτές και τους επιχειρηματικούς συνεργάτες οργανισμών που ανησυχούν γενικά για την ασφάλεια των πληροφοριών τους καθώς και για την ασφάλεια πληροφοριών στην αλυσίδα τροφοδοσίας ή το δίκτυο τους.

Σύμφωνα με την έρευνα του οργανισμού ISO για το 2015, είχαν εκδοθεί πάνω από 27.000 πιστοποιητικά ISO / IEC 27001 παγκοσμίως παρουσιάζοντας μια

αύξηση της τάξης του 20% σε σχέση με το 2014 και με τάσεις συνεχούς αύξησης χρόνο με τον χρόνο.



ΣΧΗΜΑ 4-3.ΚΑΤΑΝΟΜΗ ΠΡΟΤΥΠΟΥ ISO27001 ΑΝΑ ΤΗΝ ΥΦΗΛΙΟ 2006 -2015

(Πηγή (ISO/IEC, 2017))

Η πιστοποίηση φέρνει πολλά πλεονεκτήματα πέρα από την απλή συμμόρφωση, με τον ίδιο τρόπο που ένα πιστοποιητικό της σειράς ISO 9000 λέει κάτι περισσότερο από το "είμαστε ένας ποιοτικός οργανισμός". Η ανεξάρτητη αξιολόγηση συνεπάγεται αναγκαστικά κάποια αυστηρότητα και διατύπωση στη διαδικασία υλοποίησης (που συνεπάγεται βελτιώσεις στην ασφάλεια των πληροφοριών και όλα τα οφέλη που συνεπάγεται η μείωση του κινδύνου) και απαιτεί πάντοτε έγκριση από ανώτατα στελέχη (που αποτελεί τουλάχιστον ένα πλεονέκτημα στους όρους της ευαισθητοποίησης σχετικά με την ασφάλεια).

Το πιστοποιητικό έχει δυνατότητες μάρκετινγκ και αποδεικνύει ότι ο οργανισμός λαμβάνει σοβαρά υπόψη τη διαχείριση της ασφάλειας των πληροφοριών. Ωστόσο, όπως αναφέρθηκε παραπάνω, η αξία διασφάλισης του

πιστοποιητικού εξαρτάται σε μεγάλο βαθμό από το πεδίο εφαρμογής του ΣΔΑΠ - ISMS και της Δήλωσης Εφαρμογής – SoA, με λίγα λόγια δεν θα πρέπει να εμπιστευόμαστε υπερβολικά το πιστοποιητικό συμμόρφωσης ISO / IEC 27001 ενός οργανισμού εάν αυτός εξαρτάται σε μεγάλο βαθμό από την ασφάλεια των πληροφοριών. Με τον ίδιο ακριβώς τρόπο που η συμβατή συμμόρφωση π.χ. με το PCI-DSS δεν σημαίνει ότι εγγυόμαστε την ασφάλεια των δεδομένων των πιστωτικών καρτών και άλλων προσωπικών πληροφοριών, η πιστοποίηση της συμμόρφωσης με το πρότυπο ISO / IEC 27001 αποτελεί θετικό σημάδι αλλά όχι απόλυτη εγγύηση για την ασφάλεια πληροφοριών ενός οργανισμού. Υπάρχει ειδοποιός διαφορά μεταξύ του "Έχουμε στη διάθεσή μας ένα συμβατό ΣΔΑΠ - ISMS" που είναι το ορθό από το "Είμαστε ασφαλείς".

4.7 ISO / IEC 27002:2013

Το ISO / IEC 27002: 2013 έχει τις ακόλουθες ενότητες (ISO/IEC 27002, 2013):

4.7.1. Εισαγωγή

Η αναθεωρημένη έκδοση του προτύπου ISO 27002 δημοσιεύθηκε το 2013 υπό τον τίτλο "Τεχνολογία πληροφοριών - Τεχνικές ασφαλείας - Κώδικας πρακτικής για τον έλεγχο της ασφάλειας των πληροφοριών" και αποτελεί ένα δημοφιλές, διεθνώς αναγνωρισμένο πρότυπο καλής πρακτικής για την ασφάλεια των πληροφοριών.

4.7.2. Σκοπός του προτύπου

Όπως η διακυβέρνηση και η διαχείριση κινδύνων έτσι και η διαχείριση της ασφάλειας των πληροφοριών είναι ένα ευρύ θέμα με διακλαδώσεις σε όλους τους οργανισμούς. Η ασφάλεια των πληροφοριών και κατά συνέπεια το ISO / IEC 27002, αφορά όλους τους τύπους οργανισμών, συμπεριλαμβανομένων των εμπορικών επιχειρήσεων όλων των μεγεθών (από ατομικές μέχρι πολυεθνικούς γίγαντες), μη κερδοσκοπικούς, φιλανθρωπικούς, κυβερνητικά τμήματα και σχεδόν αυτόνομα όργανα - στην ουσία αφορά κάθε οργανισμό που χειρίζεται και

εξαρτάται από τις πληροφορίες. Οι συγκεκριμένες απαιτήσεις κινδύνου και ελέγχου των πληροφοριών ενδέχεται να διαφέρουν λεπτομερώς, αλλά υπάρχουν πολλά κοινά σημεία, για παράδειγμα οι περισσότερες οργανώσεις πρέπει να αντιμετωπίσουν τους κινδύνους πληροφόρησης που αφορούν τους υπαλλήλους τους, καθώς και τους αναδόχους, τους συμβούλους και τους εξωτερικούς προμηθευτές υπηρεσιών πληροφόρησης.

Το πρότυπο ασχολείται ρητά με την ασφάλεια των πληροφοριών, δηλαδή την ασφάλεια όλων των μορφών πληροφοριών (π.χ. δεδομένα υπολογιστών, τεκμηρίωση, γνώση και πνευματική ιδιοκτησία) και όχι μόνο την ασφάλεια των Πληροφορικών Συστημάτων ή την Κυβερνοασφάλεια "Cybersecurity" που ακούγεται ολοένα και περισσότερο σήμερα.

4.7.3. Σχέση μεταξύ του ISO27001 και του ISO27002

Το ISO / IEC 27001 ορίζει τυπικά τις υποχρεωτικές απαιτήσεις για ένα ΣΔΑΠ – ISMS και χρησιμοποιεί το πρότυπο ISO / IEC 27002 για να υποδείξει τους κατάλληλους ελέγχους ασφαλείας πληροφοριών στο ΣΔΑΠ – ISMS. Δεδομένου ότι το ISO / IEC 27002 αποτελεί απλώς κώδικα πρακτικής / κατευθυντήριας γραμμής και όχι πρότυπο πιστοποίησης, οι οργανισμοί είναι ελεύθεροι να επιλέγουν και να εφαρμόζουν άλλους ελέγχους ή εναλλακτικές πλήρεις σουίτες ελέγχου ασφάλειας πληροφοριών που αυτοί κρίνουν κατάλληλες. Το ISO / IEC 27001 ενσωματώνει στο παράρτημα Α μια σύνοψη (λίγο περισσότερο από τους τίτλους των τμημάτων στην πραγματικότητα) των ελέγχων από το ISO / IEC 27002. Στην πράξη, οι περισσότεροι οργανισμοί που υιοθετούν το ISO / IEC 27001 υιοθετούν επίσης ISO / IEC 27002.

4.7.4. Δομή και μορφή του προτύπου ISO/IEC 27002:2013

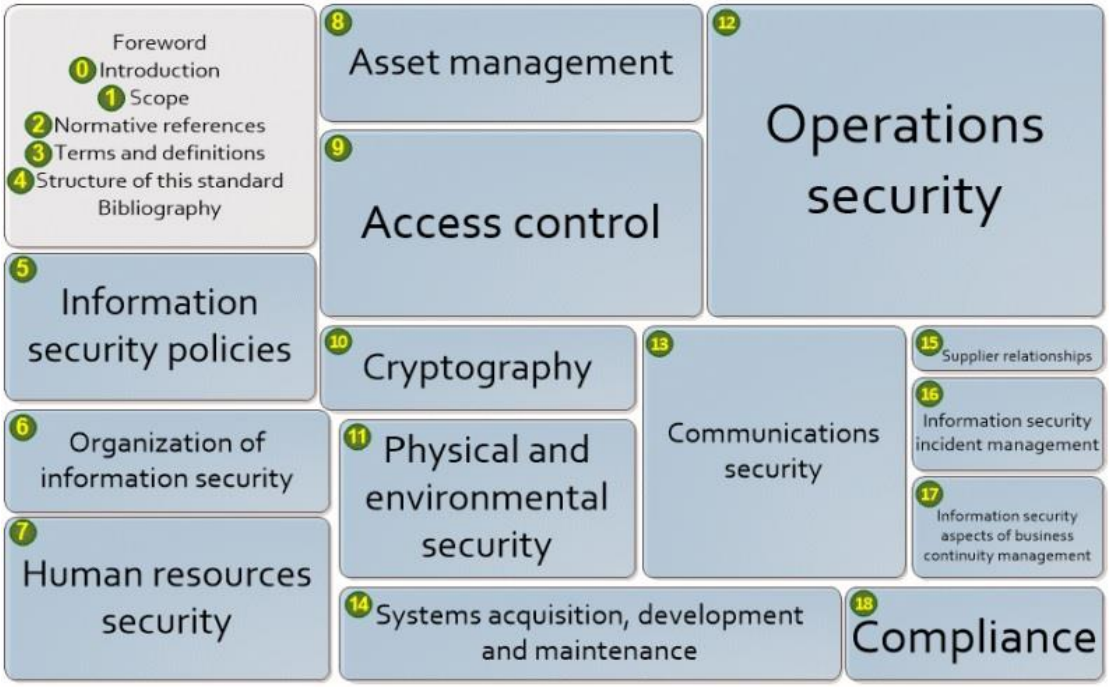
Όπως είδαμε και στην προηγούμενη παράγραφο το ISO / IEC 27002 είναι ένας κώδικας πρακτικής - ένα γενικό συμβουλευτικό έγγραφο, όχι μια τυπική προδιαγραφή όπως το ISO / IEC 27001 το οποίο συνιστά τους ελέγχους ασφάλειας των πληροφοριών που αφορούν τους στόχους ελέγχου της ασφάλειας των πληροφοριών που προκύπτουν από τους κινδύνους για την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα πληροφοριών. Οι οργανισμοί που υιοθετούν το πρότυπο ISO / IEC 27002 πρέπει να αξιολογούν τους δικούς τους κινδύνους

πληροφόρησης, να αποσαφηνίζουν τους στόχους ελέγχου τους και να εφαρμόζουν κατάλληλους ελέγχους (ή και άλλες μορφές αντιμετώπισης κινδύνου) χρησιμοποιώντας το πρότυπο για καθοδήγηση.

Το πρότυπο είναι δομημένο λογικά γύρω από ομάδες συναφών ελέγχων ασφαλείας. Πολλοί έλεγχοι θα μπορούσαν να έχουν μπει σε πολλούς τομείς, αλλά για να αποφευχθούν οι αλληλοεπικαλύψεις και οι συγκρούσεις, αυτοί αυθαίρετα ανατέθηκαν σε ένα και σε ορισμένες περιπτώσεις, διασταυρώθηκαν από κάπου αλλού. Για παράδειγμα, ένα σύστημα ελέγχου πρόσβασης με κάρτα (card access control system) για μια αίθουσα υπολογιστών ή ένα αρχειοφυλάκιο είναι ταυτόχρονα ένας έλεγχος πρόσβασης και ένας φυσικός έλεγχος ο οποίος περιλαμβάνει τεχνολογία μαζί με συσχετισμένες διευθύνσεις/διαχειριστές, διαδικασίες χρήσης και πολιτικές. Αυτό έχει ως αποτέλεσμα μερικές ιδιαιτερότητες (όπως στο τμήμα 6.2 για τις κινητές συσκευές και την τηλεεργασία που αποτελούν μέρος του τμήματος 6 σχετικά με την οργάνωση της ασφάλειας των πληροφοριών), αλλά είναι τουλάχιστον μια λογικά εκτεταμένη δομή. Μπορεί να μην είναι τέλεια, αλλά είναι αρκετά καλή στο σύνολο της.

4.7.5. Περιεχόμενο του ISO/IEC 27002:2013

Το πρότυπο περιέχει 19 τμήματα ή κεφάλαια (21 αν συμπεριλάβουμε την αρίθμηση του προλόγου και την βιβλιογραφία). Στο Σχήμα 4-4 μπορούμε να δούμε ποια είναι αυτά.



ΣΧΗΜΑ 4-4.ΤΟΜΕΙΣ ΤΟΥ ISO27002:2013

(Πηγή: (ISO27K Forum, 2017)

Αναλυτικότερα έχουμε:

- ***Πρόλογος:*** Αναφέρεται εν συντομία στην επιτροπή ISO / IEC JTC1 / SC 27 που έγραψε το πρότυπο και σημειώνει ότι αυτή η "δεύτερη έκδοση ακυρώνει και αντικαθιστά την πρώτη έκδοση (ISO / IEC 27002: 2005), η οποία αναθεωρήθηκε τεχνικά και δομικά".

- ***Τμήμα 0: Εισαγωγή*** Στη εισαγωγή καθορίζεται το ιστορικό και γίνεται αναφορά στις τρεις πηγές προέλευσης των απαιτήσεων ασφάλειας πληροφοριών, σημειώνει ότι το πρότυπο προσφέρει γενικές και δυνητικά ατελείς οδηγίες που πρέπει να ερμηνεύονται στο πλαίσιο του οργανισμού, αναφέρει τους κύκλους ζωής των πληροφοριών και του συστήματος πληροφοριών και υποδεικνύει την συνολική δομή του ISO / IEC 27000 και την ορολογία για το ISO27K.

- ***Τμήμα 1: Πεδίο εφαρμογής*** Το πρότυπο δίνει συστάσεις για όσους είναι υπεύθυνοι για την επιλογή, την εφαρμογή και τη διαχείριση της ασφάλειας των πληροφοριών. Μπορεί ή όχι να χρησιμοποιηθεί για την υποστήριξη ενός ΣΔΑΠ - ISMS που καθορίζεται στο ISO / IEC 27001.

- ***Τμήμα 2: Κανονιστικές αναφορές*** Το ISO / IEC 27000 είναι το μοναδικό πρότυπο που θεωρείται απολύτως απαραίτητο για τη χρήση του ISO / IEC 27002. Ωστόσο, στο πρότυπο αναφέρονται διάφορα άλλα πρότυπα και υπάρχει βιβλιογραφία.

- ***Τμήμα 3: Όροι και ορισμοί*** Όλοι οι ειδικοί όροι και ορισμοί ορίζονται τώρα στο ISO / IEC 27000 και οι περισσότεροι εφαρμόζονται σε ολόκληρη την οικογένεια προτύπων ISO27K.

- ***Τμήμα 4: Δομή του προτύπου***

1. *Ρήτρες ελέγχου ασφάλειας:* Από τα 21 τμήματα ή κεφάλαια του προτύπου, στα 14 προσδιορίζονται οι στόχοι και οι έλεγχοι. Αυτά τα 14 τμήματα είναι οι «ρήτρες ελέγχου ασφάλειας». Υπάρχει μια τυποποιημένη δομή μέσα σε κάθε ρήτρα ελέγχου: μία ή περισσότερες υποενότητες, καθεμία από τις οποίες ορίζει ένα στόχο ελέγχου και κάθε στόχος ελέγχου υποστηρίζεται διαδοχικά από έναν ή περισσότερους δηλωμένους ελέγχους, κάθε έλεγχος ακολουθείτε από τις σχετικές οδηγίες εφαρμογής του ενώ σε ορισμένες περιπτώσεις περιλαμβάνονται και πρόσθετες επεξηγηματικές σημειώσεις. Για να αντιληφθεί κάποιος σε ποσότητα την λεπτομέρεια που εμπεριέχεται στο πρότυπο αρκεί να δει το μέγεθος του το οποίο αγγίζει περίπου τις 90 σελίδες Α4.

2. *35 στόχοι ελέγχου:* Το ISO / IEC 27002 καθορίζει περίπου 35 στόχους ελέγχου (ένας ανά κατηγορία ελέγχου ασφαλείας) σχετικά με την ανάγκη προστασίας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών. Οι στόχοι ελέγχου είναι σε αρκετά υψηλό επίπεδο και στην πραγματικότητα περιλαμβάνουν μια γενική προδιαγραφή λειτουργικών απαιτήσεων για την αρχιτεκτονική διαχείρισης της ασφάλειας ενός οργανισμού.

3. Λίγοι επαγγελματίες θα αμφισβητούσαν σοβαρά την εγκυρότητα των στόχων ελέγχου ή για να το θέσουμε διαφορετικά θα ήταν δύσκολο να υποστηριχθεί ότι ένας οργανισμός δεν χρειάζεται να ικανοποιήσει τους αναφερόμενους στόχους ελέγχου γενικά. Ωστόσο, ορισμένοι στόχοι ελέγχου δεν ισχύουν σε όλες τις περιπτώσεις και η γενική τους διατύπωση είναι

απίθανο να αντικατοπτρίζει τις ακριβείς απαιτήσεις κάθε οργανισμού δεδομένου του πολύ ευρέος φάσματος των οργανισμών και των βιομηχανιών στις οποίες εφαρμόζεται το πρότυπο. Αυτός είναι ο λόγος για τον οποίο το ISO / IEC 27001 απαιτεί την Δήλωση Εφαρμογής (Statement of Applicability, SoA), η οποία καθορίζει με σαφήνεια τους ελέγχους ασφάλειας πληροφοριών που απαιτούνται ή δεν απαιτούνται από τον οργανισμό, καθώς και την κατάσταση εφαρμογής τους.

4. *114+++ ελέγχους:* Κάθε ένας από τους στόχους ελέγχου υποστηρίζεται από τουλάχιστον έναν έλεγχο, ο οποίος δίνει ένα σύνολο 114. Ωστόσο, ο τίτλος είναι κάπως παραπλανητικός δεδομένου του γεγονότος ότι οι κατευθυντήριες γραμμές εφαρμογής συνιστούν πολυάριθμους πραγματικούς ελέγχους στις λεπτομέρειες.

Έτσι για παράδειγμα, ο στόχος ελέγχου που σχετίζεται με τη σχετικά απλή υποπαράγραφο 9.4.2 "Ασφαλείς διαδικασίες σύνδεσης", υποστηρίζεται από την επιλογή, την εφαρμογή και τη χρήση των κατάλληλων τεχνικών επαλήθευσης ταυτότητας, την μη γνωστοποίηση ευαίσθητων πληροφοριών κατά τον χρόνο σύνδεσης, την προστασία από κυβερνοεπιθέσεις, την καταγραφή, την μη διαβίβαση κωδικών πρόσβασης ανοικτά στο δίκτυο, τα χρονικά όρια αδράνειας κατά την λειτουργία και περιορισμούς στους χρόνους πρόσβασης.

Θα μπορούσε να υποστηριχθεί ότι το ISO / IEC 27002 συνιστά κυριολεκτικά εκατοντάδες διακριτούς ελέγχους ασφάλειας πληροφοριών, αν και ορισμένοι υποστηρίζουν πολλαπλούς στόχους ελέγχου, με άλλα λόγια ορισμένοι έλεγχοι έχουν διάφορους σκοπούς. Επιπλέον, η διατύπωση σε όλο το πρότυπο δηλώνει σαφώς ή υπονοεί ότι αυτό δεν είναι ένα εντελώς ολοκληρωμένο σύνολο. Ένας οργανισμός μπορεί να έχει ελαφρώς διαφορετικούς ή τελείως νέους στόχους ελέγχου στην ασφάλεια των πληροφοριών, που απαιτούν άλλους ελέγχους (μερικές φορές γνωστούς ως «εκτεταμένα σύνολα ελέγχου») στη θέση τους ή επιπλέον αυτών που αναφέρονται στο πρότυπο.

- ***Τμήμα 5: Πολιτικές ασφάλειας πληροφοριών***

5.1 Κατεύθυνση διαχείρισης για την ασφάλεια των πληροφοριών

Η διοίκηση πρέπει να καθορίσει ένα σύνολο πολιτικών για να διευκρινίσει την κατεύθυνση και την υποστήριξή της στην ασφάλεια των πληροφοριών. Σε ανώτατο επίπεδο, θα πρέπει να υπάρχει μια συνολική "Πολιτική ασφάλειας πληροφοριών" όπως αυτή ορίζεται στο ISO / IEC 27001, τμήμα 5.2.

- ***Τμήμα 6: Οργάνωση της ασφάλειας των πληροφοριών***

6.1 Εσωτερική οργάνωση

Ο οργανισμός πρέπει να καθορίσει τους ρόλους και τις ευθύνες για την ασφάλεια των πληροφοριών και να τις κατανείμει ατομικά στο προσωπικό. Όπου είναι σκόπιμο, τα καθήκοντα θα πρέπει να διαχωρίζονται μεταξύ των ρόλων και των ατόμων, ώστε να αποφεύγονται οι συγκρούσεις συμφερόντων και να προλαμβάνονται οι ακατάλληλες δραστηριότητες. Η ασφάλεια πληροφοριών θα πρέπει να είναι αναπόσπαστο μέρος στην διαχείριση όλων των τύπων έργων.

6.2 Κινητές συσκευές και τηλεργασία

Πρέπει να υπάρχουν πολιτικές ασφάλειας και έλεγχοι για τις κινητές συσκευές (όπως φορητοί υπολογιστές, tablet PCs, φορητές συσκευές πληροφοριών και επικοινωνίας, smartphones, USB gadgets) και την τηλεργασία από απόσταση (όπως τηλεργασία από το σπίτι, τον δρόμο και απομακρυσμένους / εικονικούς χώρους εργασίας).

- ***Τμήμα 7: Ασφάλεια των ανθρώπινων πόρων***

7.1 Πριν από την απασχόληση

Οι ευθύνες για την ασφάλεια των πληροφοριών θα πρέπει να λαμβάνονται υπόψη κατά την πρόσληψη μόνιμων εργαζομένων, εργολάβων και έκτακτων υπαλλήλων (π.χ. μέσω κατάλληλων περιγραφών θέσεων εργασίας, προκαταρκτική εξέταση προσλήψεων) και να περιλαμβάνονται στις συμβάσεις (π.χ. όρους και συνθήκες εργασίας καθώς και άλλες υπογεγραμμένες συμφωνίες που ορίζουν ρόλους και ευθύνες ασφάλειας, υποχρεώσεις συμμόρφωσης κ.λ.π.).

7.2 Κατά τη διάρκεια της απασχόλησης

Οι διαχειριστές ασφαλείας θα πρέπει να διασφαλίζουν ότι οι εργαζόμενοι και οι εργολάβοι ενημερώνονται και παρακινούνται να συμμορφωθούν με τις υποχρεώσεις τους όσον αφορά την ασφάλεια των πληροφοριών. Μια επίσημη πειθαρχική διαδικασία είναι απαραίτητη για την αντιμετώπιση περιστατικών στην ασφάλεια των πληροφοριών που φέρεται ότι προκαλούν οι εργαζόμενοι.

7.3 Τερματισμός και αλλαγή της απασχόλησης

Οι πτυχές ασφάλειας που δημιουργούνται από την αποχώρηση ενός ατόμου από τον οργανισμό ή όταν γίνονται σημαντικές αλλαγές ρόλων μέσα σε αυτόν πρέπει να αντιμετωπιστούν, όπως η επιστροφή των εταιρικών πληροφοριών και του εξοπλισμού που βρίσκεται στην κατοχή του, η επικαιροποίηση των δικαιωμάτων πρόσβασης και η υπενθύμιση των συνεχιζόμενων υποχρεώσεών του βάσει της νομοθεσίας περί ιδιωτικότητας και πνευματικής ιδιοκτησίας, των συμβατικών όρων κ.λ.π. συν τις δεοντολογικές προσδοκίες του ιδίου του ατόμου.

- ***Τμήμα 8: Διαχείριση περιουσιακών στοιχείων***

8.1 Ευθύνη περιουσιακών στοιχείων

Όλα τα πληροφοριακά στοιχεία θα πρέπει να αποτιμώνται και οι ιδιοκτήτες θα πρέπει να προσδιορίζονται για να λογοδοτούν για την ασφάλειά τους. Πρέπει να οριστούν πολιτικές "Αποδεκτής χρήσης" και τα περιουσιακά στοιχεία θα πρέπει να επιστραφούν όταν οι άνθρωποι εγκαταλείψουν τον οργανισμό.

8.2 Κατάταξη πληροφοριών

Οι πληροφορίες πρέπει να ταξινομούνται και να επισημαίνονται από τους ιδιοκτήτες τους σύμφωνα με την απαιτούμενη προστασία ασφαλείας και να διαχειρίζονται κατάλληλα.

8.3 Διαχείριση μέσων

Τα μέσα αποθήκευσης πληροφοριών πρέπει να διαχειρίζονται, να ελέγχονται, να μετακινούνται και να διατίθενται με τέτοιο τρόπο ώστε να μην τίθεται σε κίνδυνο το περιεχόμενο των πληροφοριών.

- ***Τμήμα 9: Έλεγχος πρόσβασης***

9.1 Επιχειρηματικές απαιτήσεις ελέγχου πρόσβασης

Οι απαιτήσεις του οργανισμού για τον έλεγχο της πρόσβασης σε πληροφοριακά στοιχεία πρέπει να τεκμηριώνονται σαφώς σε μια πολιτική και διαδικασίες ελέγχου πρόσβασης. Η πρόσβαση στο δίκτυο και οι συνδέσεις θα πρέπει να περιοριστούν.

9.2 Διαχείριση πρόσβασης χρηστών

Η κατανομή των δικαιωμάτων πρόσβασης στους χρήστες θα πρέπει να ελέγχεται από την αρχική εγγραφή του χρήστη έως την κατάργηση των δικαιωμάτων πρόσβασης όταν δεν απαιτούνται πλέον, συμπεριλαμβανομένων των ειδικών περιορισμών για τα προνομιακά δικαιώματα πρόσβασης και τη διαχείριση των κωδικών πρόσβασης καθώς και της τακτικής ενημέρωσης και ανανέωσης των δικαιωμάτων πρόσβασης.

9.3 Ευθύνες χρήστη

Οι χρήστες πρέπει να γνωρίζουν τις ευθύνες τους όσον αφορά τη διατήρηση αποτελεσματικών ελέγχων πρόσβασης, π.χ. επιλέγοντας ισχυρούς κωδικούς πρόσβασης και κρατώντας τους εμπιστευτικούς.

9.4 Έλεγχος πρόσβασης συστήματος και εφαρμογών

Η πρόσβαση στις πληροφορίες πρέπει να περιορίζεται σύμφωνα με την πολιτική ελέγχου πρόσβασης, π.χ. μέσω ασφαλούς σύνδεσης, διαχείρισης κωδικού πρόσβασης, ελέγχου σε προνομιακά βοηθητικά προγράμματα και περιορισμένης πρόσβασης στον πηγαίο κώδικα του προγράμματος.

- ***Τμήμα 10: Κρυπτογραφία***

10.1 Κρυπτογραφικοί έλεγχοι

Πρέπει να υπάρχει μια πολιτική σχετικά με τη χρήση της κρυπτογράφησης, καθώς και κρυπτογραφικό έλεγχο ταυτότητας και ακεραιότητας, όπως ψηφιακές υπογραφές και κωδικοί ταυτοποίησης μηνυμάτων και διαχείριση κρυπτογραφικού κλειδιού.

- ***Τμήμα 11: Φυσική και περιβαλλοντική ασφάλεια***

11.1 Ασφαλείς περιοχές

Καθορισμένες φυσικές περιφέρειες και περιφράξεις, με φυσικούς ελέγχους εισόδου και διαδικασίες εργασίας, θα πρέπει να προστατεύουν τους χώρους, τα γραφεία, τα δωμάτια, τις περιοχές φόρτωσης / φορτοεκφόρτωσης κλπ. έναντι μη εξουσιοδοτημένης πρόσβασης. Πρέπει να αναζητηθούν συμβουλές ειδικών σχετικά με την προστασία από τις πυρκαγιές, τις πλημμύρες, τους σεισμούς, τις βόμβες κλπ.

11.2 Εξοπλισμός

Πρέπει να προστατευθεί και να συντηρηθεί ο εξοπλισμός (πρόκειται κυρίως για εξοπλισμό ΤΠΕ) συν τα μηχανήματα υποστήριξης (όπως είναι η τροφοδοσία και ο κλιματισμός) και η καλωδίωση. Ο εξοπλισμός και οι πληροφορίες δεν θα πρέπει να βγαίνουν εκτός εάν δεν είναι εξουσιοδοτημένοι και θα πρέπει να προστατεύονται επαρκώς τόσο εντός όσο και εκτός του χώρου. Οι πληροφορίες πρέπει να καταστρέφονται πριν από τη απόρριψη ή την επαναχρησιμοποίηση των μέσων αποθήκευσης. Πρέπει να εξασφαλίζεται ότι ο εξοπλισμός είναι ασφαλείς όταν δεν επιτηρείται και να υπάρχει σαφής πολιτική καθαρού γραφείου και οθόνης.

- ***Τμήμα 12: Ασφάλεια λειτουργίας***

12.1 Επιχειρησιακές διαδικασίες και αρμοδιότητες

Πρέπει να τεκμηριώνονται οι λειτουργίες και οι λειτουργίες της πληροφορικής. Πρέπει να ελέγχονται οι αλλαγές στις εγκαταστάσεις και τα συστήματα πληροφορικής. Πρέπει να γίνεται διαχείριση της ικανότητας και των επιδόσεων. Τα συστήματα ανάπτυξης, δοκιμής και λειτουργίας πρέπει να διαχωρίζονται.

12.2 Προστασία από κακόβουλο λογισμικό

Απαιτούνται έλεγχοι κακόβουλου λογισμικού, συμπεριλαμβανομένης της ευαισθητοποίησης του χρήστη.

12.3 Δημιουργία αντιγράφων ασφαλείας

Τα κατάλληλα αντίγραφα ασφαλείας θα πρέπει να λαμβάνονται και να διατηρούνται σύμφωνα με μια πολιτική δημιουργίας αντιγράφων ασφαλείας.

12.4 Καταγραφή και παρακολούθηση

Οι δραστηριότητες του χρήστη και του διαχειριστή / χειριστή του συστήματος, οι εξαιρέσεις, τα σφάλματα και τα συμβάντα ασφάλειας πληροφοριών πρέπει να καταγράφονται και να προστατεύονται. Τα ρολόγια πρέπει να συγχρονίζονται.

12.5 Έλεγχος επιχειρησιακού λογισμικού

Η εγκατάσταση του λογισμικού σε λειτουργικά συστήματα θα πρέπει να ελέγχεται.

12.6 Διαχείριση της τεχνικής ευπάθειας

Οι τεχνικές ευπάθειες θα πρέπει να διορθωθούν και θα πρέπει να υπάρχουν κανόνες που να διέπουν την εγκατάσταση του λογισμικού από τους χρήστες.

12.7 Σκέψεις ελέγχου συστημάτων πληροφοριών

Οι έλεγχοι στα πληροφορικά συστήματα θα πρέπει να σχεδιάζονται και να ελέγχονται ώστε να ελαχιστοποιούνται οι αρνητικές επιπτώσεις στα παραγωγικά συστήματα ή να γίνει ακατάλληλη πρόσβαση σε δεδομένα.

❖ ***13 Ασφάλεια επικοινωνιών***

13.1 Διαχείριση ασφάλειας δικτύου

Τα δίκτυα και οι υπηρεσίες δικτύου θα πρέπει να εξασφαλίζονται, για παράδειγμα με διαχωρισμό.

13.2 Μεταφορά πληροφοριών

Πρέπει να υπάρχουν πολιτικές, διαδικασίες και συμφωνίες (π.χ. συμφωνίες μη γνωστοποίησης) σχετικά με τη μεταφορά πληροφοριών προς / από τρίτους, συμπεριλαμβανομένης της ηλεκτρονικής ανταλλαγής μηνυμάτων.

- ***Τμήμα 14: Απόκτηση, ανάπτυξη και συντήρηση του συστήματος***

14.1 Απαιτήσεις ασφάλειας των πληροφοριακών συστημάτων

Οι απαιτήσεις ελέγχου ασφαλείας πρέπει να αναλύονται και να προσδιορίζονται, συμπεριλαμβανομένων των εφαρμογών και των συναλλαγών στο διαδίκτυο.

14.2 Ασφάλεια σε διαδικασίες ανάπτυξης και υποστήριξης

Οι κανόνες που διέπουν την ανάπτυξη ασφαλούς λογισμικού / συστημάτων πρέπει να ορίζονται ως πολιτική. Πρέπει να ελέγχονται οι αλλαγές στα συστήματα (εφαρμογές και λειτουργικά). Τα πακέτα λογισμικού δεν θα πρέπει να τροποποιούνται στην ιδανική περίπτωση ενώ θα πρέπει να τηρούνται οι μηχανικές αρχές ασφάλειας. Το περιβάλλον ανάπτυξης τους θα πρέπει να είναι ασφαλές ενώ αν η ανάπτυξη του ανατίθεται σε εξωτερικούς συνεργάτες θα πρέπει να ελέγχεται. Η ασφάλεια του συστήματος θα πρέπει να δοκιμαστεί και να καθοριστούν τα κριτήρια αποδοχής κινδύνου ώστε να συμπεριλαμβάνονται στις πτυχές ασφάλειας.

14.3 Στοιχεία ελέγχου

Τα δεδομένα των δοκιμών θα πρέπει να δημιουργούνται/επιλέγονται προσεκτικά και να ελέγχονται.

- ***15: Σχέσεις με προμηθευτές***

15.1 Ασφάλεια πληροφοριών στις σχέσεις προμηθευτών

Πρέπει να υπάρχουν πολιτικές, διαδικασίες, επίγνωση κ.λπ. για την προστασία των πληροφοριών του οργανισμού που είναι προσβάσιμες από τους υπεργολάβους πληροφοριακών συστημάτων και άλλους εξωτερικούς

προμηθευτές σε όλη την αλυσίδα του εφοδιασμού η οποία συμφωνείται στα πλαίσια των συμβάσεων ή των συμφωνιών.

15.2 Διαχείριση διανομής υπηρεσιών προμηθευτή

Η παράδοση υπηρεσιών από εξωτερικούς προμηθευτές πρέπει να παρακολουθείται και να αναθεωρείται / ελέγχεται βάσει των συμβάσεων / συμφωνιών. Οι αλλαγές στις υπηρεσίες θα πρέπει να ελέγχονται.

- ***Τμήμα 16: Διαχείριση περιστατικών ασφάλειας πληροφοριών***

16.1 Διαχείριση περιστατικών και βελτιώσεων ασφάλειας πληροφοριών

Πρέπει να υπάρχει κατανομή ευθυνών και διαδικασίες για τη διαχείριση (αναφορά, αξιολόγηση, ανταπόκριση και εκμάθηση) περιστατικών ασφαλείας των πληροφοριών, ατυχήματα και αδυναμίες συλλέγονται με συνέπεια και αποτελεσματικότητα για την συλλογή εγκληματολογικών στοιχείων.

- ***Τμήμα 17: Ασφάλεια πληροφοριών όσον αφορά τη διαχείριση της συνέχειας των επιχειρήσεων***

17.1 Συνέχεια της ασφάλειας των πληροφοριών

Η συνέχεια στην ασφάλεια των πληροφοριών θα πρέπει να σχεδιαστεί, να εφαρμοστεί και να αναθεωρηθεί ως αναπόσπαστο μέρος των συστημάτων διαχείρισης της επιχειρησιακής συνέχειας του οργανισμού.

17.2 Εφεδρείες

Οι εγκαταστάσεις των πληροφοριακών συστημάτων θα πρέπει να διαθέτουν επαρκή εφεδρεία για να ικανοποιήσουν τις απαιτήσεις σε διαθεσιμότητα.

- ***Τμήμα 18: Συμμόρφωση***

18.1 Συμμόρφωση με τις νομικές και συμβατικές απαιτήσεις

Ο οργανισμός πρέπει να εντοπίζει και να τεκμηριώνει τις υποχρεώσεις του προς τις εξωτερικές αρχές και άλλα τρίτα μέρη σε σχέση με την ασφάλεια των πληροφοριών, περιλαμβανομένης της πνευματικής ιδιοκτησίας, των

[επιχειρησιακών] εγγραφών, της ιδιωτικής ζωής / πληροφοριών προσωπικής ταυτοποίησης και της κρυπτογράφησης

18.2 Ανασκόπηση ασφάλειας πληροφοριών

Οι ρυθμίσεις του οργανισμού για την ασφάλεια των πληροφοριών θα πρέπει να ελέγχονται ανεξάρτητα (ελέγχεται) και να αναφέρονται στη διοίκηση. Οι διαχειριστές θα πρέπει επίσης να επανεξετάζουν τακτικά τη συμμόρφωση των υπαλλήλων και των συστημάτων με τις πολιτικές ασφαλείας, τις διαδικασίες κλπ. και να ξεκινούν διορθωτικές ενέργειες όπου χρειάζεται.

ΚΕΦΑΛΑΙΟ 5

«ΠΑΡΑΔΕΙΓΜΑ ΑΝΑΠΤΥΞΗΣ ΣΔΑΠ ΚΑΤΑ ISO/IEC 27001:2013 ΣΕ ΕΝΑΝ ΟΡΓΑΝΙΣΜΟ»

5.1 Ανάπτυξη ΣΔΑΠ σε έναν οργανισμό

Με τον όρο ανάπτυξη νοείται ο σχεδιασμός, η υλοποίηση, ο έλεγχος και τέλος η συνεχή βελτίωση ενός ΣΔΑΠ. Η μεθοδολογία που θα ακολουθήσουμε για να δώσουμε παρακάτω ένα γενικό παράδειγμα ανάπτυξης ενός ΣΔΑΠ κατά ISO/IEC 27001 σ' έναν οργανισμό και κατά επέκταση σε μια οποιαδήποτε υπηρεσία Ηλεκτρονικής Διακυβέρνησης είναι η PDCA (Plan – Do – Check – Act) την οποία περιγράψαμε αναλυτικά στο κεφάλαιο 3§ 3.7 και η οποία έχει αποδειχθεί ότι είναι μια πολύ πρακτική μέθοδος για την ανάπτυξη ενός ΣΔΑΠ. Αναλυτικότερα έχουμε:

5.1.1. <u>Φάση 1 (Σχεδιασμός): Θέσπιση του ΣΔΑΠ</u>

Ο φορέας στη φάση του σχεδιασμού του ΣΔΑΠ θα πρέπει να κάνει τα ακόλουθα (Λεταράκη, 2016):

- Να ορίσει το πεδίο εφαρμογής και τα όρια του ΣΔΑΠ ανάλογα με το είδος του οργανισμού, τη τοποθεσία του, τα αγαθά και την τεχνολογία του και να δικαιολογήσει τυχόν εξαιρέσεις.
- Να ορίσει μια πολιτική ασφαλείας.
- Να εξασφαλίσει τη δέσμευση της διοίκησης.
- Να ορίσει τη προσέγγιση που θα ακολουθεί ο οργανισμός για την αξιολόγηση του κινδύνου (risk assesment).
- Να αναπτύξει κριτήρια για αποδοχή κινδύνου και να οριστεί το αποδεκτό επίπεδο κινδύνου.
- Να αναγνωριστεί το ρίσκο.

- Να αναγνωριστούν οι επιπτώσεις σε περίπτωση απώλειας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας για κάθε αγαθό.
- Να επιλέξει τους ελέγχους που θα υλοποιήσει σύμφωνα με το Παράρτημα Α του προτύπου.
- Να ετοιμάσει την Δήλωση Εφαρμοσιμότητας, καταγράφοντας τους επιλεγμένους ελέγχους και δικαιολογώντας τυχόν εξαιρέσεις.

5.1.2. **Φάση 2 (Υλοποίηση): Υλοποίηση και λειτουργία του ΣΔΑΠ**

Στην φάση αυτή ο φορέας υλοποιεί και θέτει σε λειτουργία τις δράσεις που σχεδιάστηκαν στην προηγούμενη φάση. Συγκεκριμένα θα πρέπει να κάνει τα ακόλουθα (Λεταράκη, 2016):

- Να διατυπώσει ένα σχέδιο αντιμετώπισης του κινδύνου, το οποίο να αναγνωρίζει τις κατάλληλες ενέργειες από την μεριά της διαχείρισης, τους πόρους, τις αρμοδιότητες και τις προτεραιότητες για την διαχείριση των κινδύνων.
- Να υλοποιήσει το σχέδιο αντιμετώπισης του κινδύνου.
- Να υλοποιήσει τους επιλεγμένους ελέγχους.
- Να ορίσει μετρικές για την αξιολόγηση της αποτελεσματικότητας των επιλεγμένων ελέγχων.
- Να γίνει κατανομή ρόλων και αρμοδιοτήτων σχετικών με την ασφάλεια πληροφοριών.
- Να υλοποιήσει προγράμματα κατάρτισης και ενημέρωσης των εμπλεκόμενων μελών.
- Να διαχειρίζεται τις λειτουργίες και τους πόρους του ΣΔΑΠ.

5.1.3. **Φάση 3 (Έλεγχος): Παρακολούθηση του ΣΔΑΠ**

Στην φάση ελέγχου αξιολογούμε την απόδοση του ΣΔΑΠ και αναφέρουμε τα αποτελέσματα στη διοίκηση του φορέα. Συγκεκριμένα στη φάση αυτή (Λεταράκη, 2016):

- Ελέγχεται η καλή λειτουργία των διαδικασιών και των ελέγχων που ακολουθούνται ώστε να εντοπίζονται εγκαίρως τα πιθανά λάθη.
- Εντοπίζονται περιστατικά παραβίασης ασφαλείας και πιθανές ή επιτυχημένες προσπάθειες διαχείρισης τους.
- Η διοίκηση ελέγχει και καθορίζει αν οι δραστηριότητες ασφαλείας που έχουν δοθεί σε ανθρώπους ή έχουν υλοποιηθεί με τεχνολογικά μέσα, λειτουργούν όπως έχουν οριστεί.
- Εξετάζεται αν οι δράσεις που έγιναν για να επιλύσουν ένα κενό ασφαλείας είναι αποτελεσματικές.
- Προβαίνει σε τακτικές αξιολογήσεις της αποτελεσματικότητας του ΣΔΑΠ, λαμβάνοντας υπόψη τα αποτελέσματα από τους ελέγχους (audits), τα περιστατικά ασφαλείας, τις μετρήσεις αποτελεσματικότητας και τις προτάσεις από όλα τα ενδιαφερόμενα μέλη.
- Μετριέται η αποτελεσματικότητα των ελέγχων για να εξασφαλιστεί ότι τηρήθηκαν οι απαιτήσεις ασφαλείας.
- Επανεξετάζει την διαχείριση κινδύνου σε τακτά χρονικά διαστήματα και τους εν λόγω κινδύνους, λαμβάνοντας υπόψη τις αλλαγές στον οργανισμό, τη τεχνολογία, τους επιχειρηματικούς στόχους και διαδικασίες, τις εντοπισμένες απειλές και εξωτερικούς παράγοντες όπως αλλαγές στην νομοθεσία και το κοινωνικό κλίμα.
- Πραγματοποιεί εσωτερικούς ελέγχους του ΣΔΑΠ σε τακτά χρονικά διαστήματα.
- Ανανεώνει τα σχέδια ασφαλείας ώστε να συμπεριλαμβάνουν τα ευρήματα της παρακολούθησης και των δραστηριοτήτων επανελέγχου.

- Καταγράφει τις δράσεις ασφαλείας και τα γεγονότα που θα μπορούσαν να επηρεάσουν την αποτελεσματικότητα ή την απόδοση του ΣΔΑΠ.

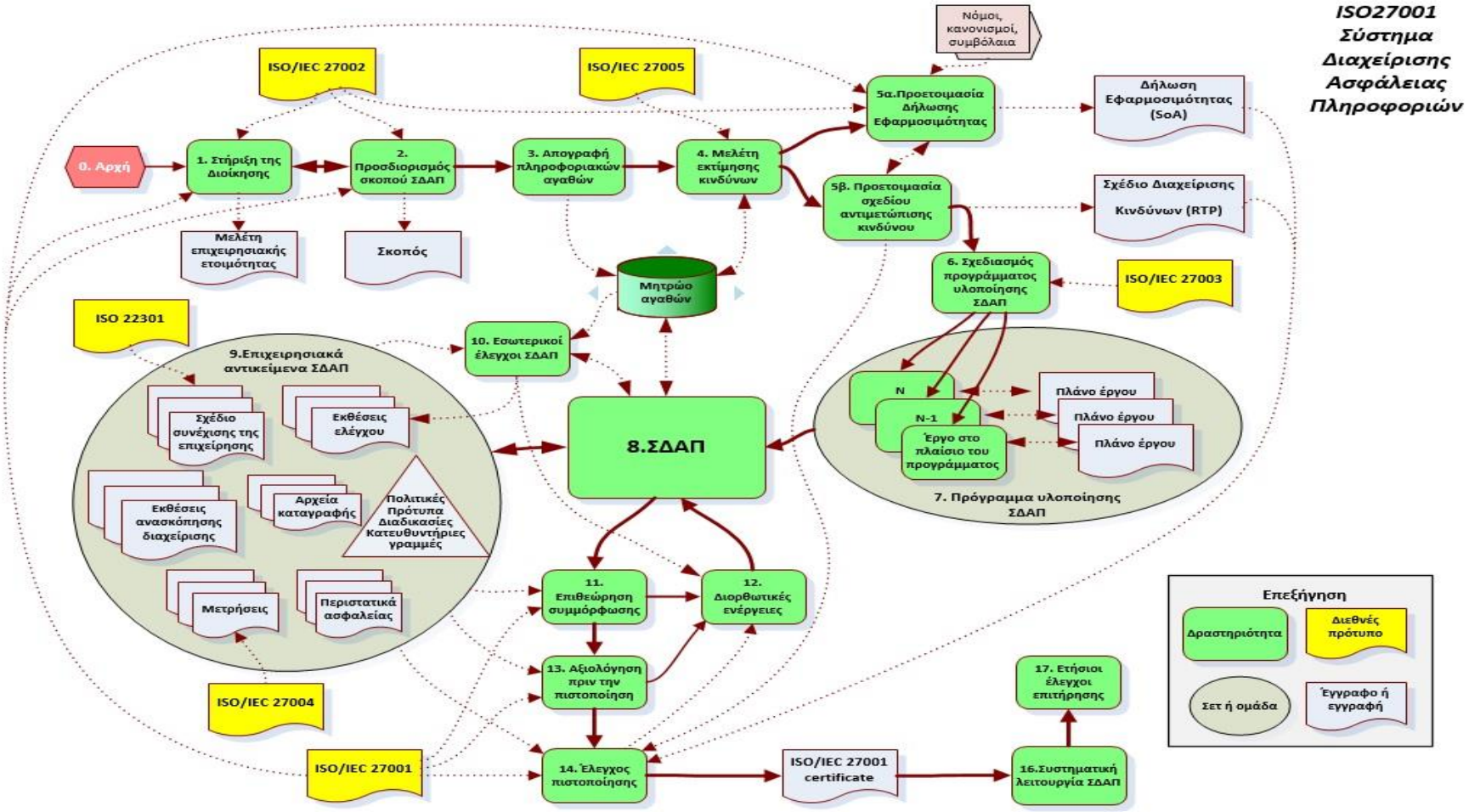
5.1.4. Φάση 4 (Διόρθωση): Συντήρηση και βελτίωση του ΣΔΑΠ

Στη φάση της διόρθωσης ο φορέας θα πρέπει να κάνει τακτικά τα ακόλουθα:

- Να επανελέγχει και να μετράει την αποτελεσματικότητα του ΣΔΑΠ.
- Να υλοποιεί τις αναγνωρισμένες βελτιώσεις στα πλαίσια του ΣΔΑΠ.
- Να παίρνει τα κατάλληλα μέτρα διορθωτικών ενεργειών.
- Να ενημερώνει για τις όποιες ενέργειες και βελτιώσεις σε όλα τα ενδιαφερόμενα μέλη.
- Να εξασφαλίζει ότι οι βελτιώσεις επιτυγχάνουν το σκοπό τους.
- Να καταγράφει τις ενέργειες και τα γεγονότα που επηρεάζουν το ΣΔΑΠ.

5.2 Διαδικασίες ανάπτυξης ΣΔΑΠ

Ο οργανισμός για να καταφέρει να υλοποιήσει όλες τις παραπάνω φάσεις και να πιστοποιηθεί με το ISO/IEC 27001, θα χρειαστεί να ακολουθήσει μια διαδικασία δεκατριών βημάτων όπως φαίνεται στο σχήμα 5.1.



ΣΧΗΜΑ 5-1 Η ΔΙΑΔΙΚΑΣΙΑ ΑΝΑΠΤΥΞΗΣ ΕΝΟΣ ΣΔΑΠ

(Πηγή: (ISO27K Forum, 2017)

Παρατηρώντας κάποιος το Σχήμα 5–1 σε συνδυασμό με όσα έχουμε πει στο κεφάλαιο 4 § 4.6 γίνεται αντιληπτό ότι η δήλωση εφαρμοσιμότητας (Statement of Applicability, SoA) και το σχέδιο διαχείρισης κινδύνων (Risk Treatment Plan, RTP) αποτελούν κεντρικά στοιχεία του ΣΔΑΠ. Οι είσοδοι στην διεργασία για την προετοιμασία της δήλωσης εφαρμοσιμότητας και της προετοιμασίας σχεδίου αντιμετώπισης κινδύνου είναι η μελέτη εκτίμησης κινδύνων η οποία κατέχει κεντρικό ρόλο στην όλη διεργασία ανάπτυξης του ΣΔΑΠ, τα μέτρα ασφαλείας του Παραρτήματος Α΄ του προτύπου ISO27001 τα οποία ουσιαστικά ταυτίζονται με τα περιεχόμενα του προτύπου ISO/IEC 27002 και τα ήδη υπάρχοντα μέτρα ασφαλείας (Κάτσικας Σ. Κ., 2014).

Οι στόχοι ασφαλείας του οργανισμού καθορίζονται λαμβάνοντας υπόψη τρεις πηγές: (α) την εκτίμηση των κινδύνων που αντιμετωπίζει ο οργανισμός, υπό το πρίσμα της συνολικής επιχειρησιακής στρατηγικής και των στόχων του οργανισμού, (β) το νομικό και κανονιστικό πλαίσιο καθώς και οι συμβατικές δεσμεύσεις που διέπουν τον οργανισμό και (γ) το σύνολο των αρχών, στόχων και επιχειρησιακών απαιτήσεων των σχετικών με τη διαχείριση, την επεξεργασία, την αποθήκευση, τη μετάδοση και την αρχειοθέτηση πληροφοριών που έχει υιοθετήσει ο οργανισμός (Κάτσικας Σ. Κ., 2014).

Στον πίνακα 5.1 παρουσιάζονται όλα τα μέτρα ασφαλείας που περιγράφονται στο Παράρτημα Α΄ του ISO/IEC 27001:2013, σημειώνεται δε ότι αρκετά από αυτά περιγράψαμε αναλυτικά στο Κεφάλαιο 4. Η αρίθμηση των Ρητρών ξεκινάει από τον αριθμό 5.

ISO/IEC 27001:2013 Παράρτημά Α΄ έλεγχοι		
Ρήτρα	**Ενότητα**	**Στόχος Ελέγχου / Έλεγχος**
5. Πολιτικές Ασφαλείας	5,1	Κατευθύνσεις της διοίκησης
	5.1.1	Πολιτικές για την πληροφορία
	5.1.2	Επισκόπηση των πολιτικών ασφάλειας πληροφοριών
6. Οργάνωση της ασφάλειας πληροφοριών	6,1	Εσωτερική Οργάνωση
	6.1.1	Ρόλοι και αρμοδιότητες
	6.1.2	Διαχωρισμός καθηκόντων
	6.1.3	Επικοινωνία με τις αρχές

	6.1.4	Επικοινωνία με ομάδες ειδικού ενδιαφέροντος
	6.1.5	Ασφάλεια πληροφοριών στη διαχείριση έργων
	6,2	Κινητές συσκευές και τηλεργασία
	6.2.1	Πολιτική κινητών συσκευών
	6.2.2	Τηλεργασία
7. Ασφάλεια ανθρωπίνων πόρων	7,1	Πριν την πρόσληψη
	7.1.1	Διαλογή
	7.1.2	Όροι και συνθήκες πρόσληψης
	7,2	Κατά τη διάρκεια της εργασιακής σχέσης
	7.2.1	Καθήκοντα διοίκησης
	7.2.2	Επίγνωση, εκπαίδευση και κατάρτιση στην ασφάλεια πληροφοριών
	7.2.3	Πειθαρχική διαδικασία
	7,3	Τερματισμός και αλλαγή εργασιακής σχέσης
	7.3.1	Τερματισμός ή αλλαγή καθηκόντων
8. Διαχείριση αγαθών	8,1	Αρμοδιότητα για τα αγαθά
	8.1.1	Μητρώο αγαθών
	8.1.2	Ιδιοκτησία αγαθών
	8.1.3	Αποδεκτή χρήση αγαθών
	8.1.4	Επιστροφή αγαθών
	8,2	Κατηγοριοποίηση πληροφοριών
	8.2.1	Κατηγοριοποίηση πληροφοριών
	8.2.2	Επισήμανση πληροφοριών
	8.2.3	Χειρισμός αγαθών
	8,3	Χειρισμός μέσων αποθήκευσης
	8.3.1	Διαχείριση αφαιρέσιμων μέσων αποθήκευσης
	8.3.2	Απόσυρση μέσων αποθήκευσης
	8.3.3	Μεταφορά φυσικών μέσων αποθήκευσης
9. Έλεγχος Πρόσβασης	9,1	Επιχειρησιακές απαιτήσεις του ελέγχου πρόσβασης
	9.1.1	Πολιτική ελέγχου πρόσβασης
	9.1.2	Πρόσβαση στα δίκτυα και στις υπηρεσίες δικτύου
	9,2	Διαχείριση πρόσβασης χρηστών
	9.2.1	Εγγραφή και διαγραφή χρηστών
	9.2.2	Παροχή πρόσβασης στους χρήστες
	9.2.3	Διαχείριση προνομιακών δικαιωμάτων πρόσβασης
	9.2.4	Διαχείριση μυστικών πληροφοριών που χρησιμοποιούνται για την αυθεντικοποίηση των χρηστών.
	9.2.5	Επανεξέταση των δικαιωμάτων πρόσβασης

		χρηστών
	9.2.6	Αφαίρεση ή προσαρμογή δικαιωμάτων πρόσβασης χρηστών
	9,3	Ευθύνες χρηστών
	9.3.1	Χρήση μυστικών πληροφοριών που χρησιμοποιούνται για την αυθεντικοποίηση των χρηστών
	9,4	Έλεγχος πρόσβασης στο σύστημα και σε εφαρμογές
	9.4.1	Περιορισμός πρόσβασης σε πληροφορίες
	9.4.2	Ασφαλείς διαδικασίες σύνδεσης (log-on)
	9.4.3	Σύστημα διαχείρισης συνθηματικών
	9.4.4	Χρήση προνομιακών βοηθητικών προγραμμάτων
	9.4.5	Έλεγχος πρόσβασης σε πηγαίο κώδικα
10. Κρυπτογραφία	10,1	Κρυπτογραφικά μέτρα ασφαλείας
	10.1.1	Πολιτική χρήσης κρυπτογραφικών μέσων ασφαλείας
	10.1.2	Διαχείριση κλειδιών
11. Φυσική και περιβαλλοντική ασφάλεια	11,1	Ασφαλείς περιοχές
	11.1.1	Φυσική περίμετρος ασφαλείας
	11.1.2	Έλεγχοι φυσικής εισόδου
	11.1.3	Ασφάλεια γραφείων, χώρων και εγκαταστάσεων
	11.1.4	Προστασία έναντι εξωτερικών και περιβαλλοντικών απειλών
	11.1.5	Εργασία σε ασφαλείς περιοχές
	11.1.6	Περιοχές παράδοσης και φόρτωσης
	11,2	Εξοπλισμός
	11.2.1	Χωροθέτηση και προστασία εξοπλισμού
	11.2.2	Υπηρεσίες υποστήριξης
	11.2.3	Ασφάλεια καλωδιώσεων
	11.2.4	Συντήρηση εξοπλισμού
	11.2.5	Απόσυρση αγαθών
	11.2.6	Ασφάλεια εξοπλισμού και αγαθών εκτός εγκαταστάσεων
	11.2.7	Ασφαλής απόσυρση ή επαναχρησιμοποίηση εξοπλισμού
	11.2.8	Εξοπλισμός χρηστών που λειτουργεί χωρίς εποπτεία
	11.2.9	Πολιτική καθαρού γραφείου και καθαρής οθόνης
12. Ασφάλεια κατά την λειτουργία	12,1	Διαδικασίες και καθήκοντα κατά τη λειτουργία
	12.1.1	Τεκμηριωμένες διαδικασίες λειτουργίας

	12.1.2	Διαχείριση αλλαγών
	12.1.3	Διαχείριση δυνατοτήτων
	12.1.4	Διαχωρισμός του περιβάλλοντος ανάπτυξης, δοκιμής και λειτουργίας
	12,2	Προστασία από κακόβουλο λογισμικό
	12.2.1	Μέτρα προστασίας έναντι κακόβουλου λογισμικού
	12,3	Αντίγραφα ασφαλείας
	12.3.1	Αντίγραφα ασφαλείας πληροφοριών
	12,4	Καταγραφή και παρακολούθηση
	12.4.1	Καταγραφή συμβάντων
	12.4.2	Προστασία καταγεγραμμένων πληροφοριών
	12.4.3	Αρχεία καταγραφής διαχειριστών και χειριστών
	12.4.4	Συγχρονισμός ρολογιών
	12,5	Έλεγχος λειτουργικού λογισμικού
	12.5.1	Εγκατάσταση λογισμικού σε συστήματα εν λειτουργία
	12,6	Διαχείριση τεχνικών ευπαθειών
	12.6.1	Διαχείριση τεχνικών ευπαθειών
	12.6.2	Περιορισμοί στην εγκατάσταση λογισμικού
	12,7	Έλεγχος πληροφοριακών συστημάτων
	12.7.1	Μέτρα για τον έλεγχο πληροφοριακών συστημάτων
13. Ασφάλεια επικοινωνιών	13,1	Διαχείριση ασφάλειας δικτύων
	13.1.1	Μέτρα ασφαλείας για τα δίκτυα
	13.1.2	Ασφάλεια υπηρεσιών δικτύου
	13.1.3	Διαχωρισμός δικτύων
	13,2	Μετάδοση πληροφοριών
	13.2.1	Πολιτικές και διαδικασίες για τη μετάδοση πληροφοριών
	13.2.2	Συμβάσεις για τη μετάδοση πληροφοριών
	13.2.3	Ηλεκτρονικά μηνύματα
	13.2.4	Συμβάσεις εμπιστευτικότητας ή μη αποκάλυψης
14. Κτήση, ανάπτυξη και συντήρηση συστημάτων	14,1	Προδιαγραφές ασφάλειας πληροφοριακών συστημάτων
	14.1.1	Ανάλυση και καθορισμός προδιαγραφών ασφάλειας
	14.1.2	Ασφάλεια υπηρεσιών επιπέδου εφαρμογής σε δημόσια δίκτυα
	14.1.3	Προστασία συναλλαγών μέσω υπηρεσιών εφαρμογής
	14,2	Ασφάλεια στις διεργασίες ανάπτυξης και υποστήριξης

	14.2.1	Πολιτική ασφαλούς ανάπτυξης
	14.2.2	Διαδικασίες ελέγχου αλλαγών συστήματος
	14.2.3	Τεχνική αναθεώρηση εφαρμογών κατόπιν αλλαγών στη λειτουργική πλατφόρμα
	14.2.4	Περιορισμοί αλλαγών σε πακέτα λογισμικού
	14.2.5	Αρχές ανάπτυξης ασφαλών συστημάτων
	14.2.6	Ασφαλές περιβάλλον ανάπτυξης
	14.2.7	Ανάπτυξη από υπεργολάβους
	14.2.8	Δοκιμές ασφάλειας συστημάτων
	14.2.9	Δοκιμές αποδοχής συστημάτων
	14,3	Δεδομένα δοκιμών
	14.3.1	Προστασία δεδομένων δοκιμών
15. Σχέσεις με τους προμηθευτές	15,1	Ασφάλεια στις σχέσεις με τους προμηθευτές
	15.1.1	Πολιτική ασφαλείας πληροφοριών στις σχέσεις με τους προμηθευτές
	15.1.2	Αντιμετώπιση της ασφάλειας στις συμβάσεις με τους προμηθευτές
	15.1.3	Αλυσίδα εφοδιασμού τεχνολογιών πληροφορικής και επικοινωνιών
	15,2	Διαχείριση παράδοσης υπηρεσιών από προμηθευτές
	15.2.1	Παρακολούθηση και επανεξέταση υπηρεσιών από προμηθευτές
	15.2.2	Διαχείριση αλλαγών στις υπηρεσίες από προμηθευτές
16. Διαχείριση περιστατικών παραβίασης ασφάλειας	16,1	Διαχείριση περιστατικών παραβίασης ασφάλειας και βελτιώσεις
	16.1.1	Καθήκοντα και διαδικασίες
	16.1.2	Αναφορά περιστατικών παραβίασης ασφάλειας
	16.1.3	Αναφορά αδυναμιών ασφαλείας
	16.1.4	Εκτίμηση σοβαρότητας περιστατικών παραβίασης ασφάλειας και λήψη αποφάσεων
	16.1.5	Αντίδραση σε περιστατικά παραβίασης ασφαλείας
	16.1.6	Εκμάθηση από τα περιστατικά παραβίασης ασφαλείας
	16.1.7	Συλλογή στοιχείων
17. Θέματα ασφάλειας πληροφοριών στη διαχείριση της επιχειρησιακής συνέχειας	17,1	Συνέχεια της ασφάλειας πληροφοριών
	17.1.1	Σχεδιασμός της συνέχειας της ασφάλειας πληροφοριών
	17.1.2	Υλοποίηση της συνέχειας της ασφάλειας πληροφοριών

	17.1.3	Επιβεβαίωση, επανεξέταση και αξιολόγηση της συνέχειας της ασφάλειας πληροφοριών
	17,2	Πλεονασμοί
	17.2.1	Διαθεσιμότητα εγκαταστάσεων επεξεργασίας πληροφοριών
18. Συμμόρφωση	18,1	Συμμόρφωση με νομικές και συμβατικές υποχρεώσεις
	18.1.1	Καταγραφή εφαρμοστέων νομικών και συμβατικών υποχρεώσεων
	18.1.2	Πνευματικά δικαιώματα
	18.1.3	Προστασία αρχείων
	18.1.4	Ιδιωτικότητα και προστασία πληροφοριών προσωπικού χαρακτήρα
	18.1.5	Κανονισμοί σχετικοί με κρυπτογραφικά μέτρα ασφαλείας
	18,2	Επιθεωρήσεις της ασφάλειας πληροφοριών
	18.2.1	Ανεξάρτητη επιθεώρηση της ασφάλειας πληροφοριών
	18.2.2	Συμμόρφωση με τις πολιτικές και τα πρότυπα ασφαλείας
	18.2.3	Επιθεώρηση τεχνικής συμμόρφωσης

ΠΙΝΑΚΑΣ 5.1 ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΠΑΡΑΡΤΗΜΑ Α΄ ΤΟΥ ISO/IEC 27001

(Πηγή : (ISO/IEC 27001, 2013))

Ένας οργανισμός δεν χρειάζεται να επιλέξει και να αναπτύξει όλα τα παραπάνω μέτρα ασφαλείας για να διαχειριστεί τους κινδύνους του, εξαρτώνται στην πραγματικότητα από τους στόχους ασφαλείας που έχει θέσει ο οργανισμός, το ποσοστό αποδοχής του κινδύνου που έχει αποφασίσει και το πεδίο εφαρμογής του ΣΔΑΠ, αλλά ό,τι και αν είναι, πρέπει να παρουσιάζεται στην Δήλωση Εφαρμοσιμότητας (SoA).

Αφού έχουν πλέον επιλεγεί τα μέτρα ασφαλείας θα χρειαστεί να γίνει μια ανάλυση χάσματος (gap analysis) για να μπορέσουμε να προσδιορίσουμε σε τι κατάσταση βρίσκεται η υλοποίηση τους. Υπάρχουν διάφορα μοντέλα με τα οποία μπορούμε να μετρήσουμε το επίπεδο ωριμότητας της διεργασίας υλοποίησης των

μέτρων ασφαλείας, ενδεικτικά αναφέρουμε τα : COBIT 5 Maturity Model και το Carnegie Mellon Software Engineering Institute Capability Maturity Model (CCM).

Με την ολοκλήρωση των παραπάνω, ο οργανισμός μπορεί να προχωρήσει στην ετοιμασία της Δήλωσης Εφαρμοσιμότητας (SoA), αυτό βέβαια δεν σημαίνει ότι μετά την δημιουργία της ότι η δουλειά μας τελείωσε εδώ, η δήλωση θα πρέπει να αναθεωρείται και να ενημερώνεται κάθε φορά που υπάρχουν αλλαγές στα μέτρα ασφαλείας ή στο επίπεδο συμμόρφωσης ή στις απαιτήσεις που οδηγούν στην επιλογή μέτρων ασφαλείας. Εν συνεχεία, θα προχωρήσουμε στην διαμόρφωση του σχεδίου διαχείρισης κινδύνων και στην υλοποίηση των επιλεγμένων μέτρων.

Με την ολοκλήρωση και την διαμόρφωση του σχεδίου διαχείρισης κινδύνων, ο οργανισμός προχωράει σε όλες τις απαραίτητες ενέργειες προκειμένου να γεφυρώσει το χάσμα που υπάρχει ανάμεσα στο επιθυμητό επίπεδο ασφαλείας και το ισχύον, μια δραστηριότητα η οποία απαιτεί κόπο και χρόνο. Είναι πολύ συνηθισμένο λοιπόν η φάση της υλοποίησης σχεδίων διαχείρισης κινδύνων να διαρκεί μήνες ή ακόμη και χρόνια. Μέσα όμως από αυτή την διαδικασία βελτιώνεται ο βαθμός ωριμότητας του ΣΔΑΠ ενώ ταυτόχρονα επικαιροποιείται η Δήλωση Εφαρμοσιμότητας αναλόγως.

5.3 Τεκμηρίωση του ΣΔΑΠ

Είναι σημαντικό να είμαστε σε θέση να επιδείξουμε τη σχέση των επιλεγμένων μέτρων ασφάλειας με τα αποτελέσματα της διεργασίας ανάλυσης και διαχείρισης κινδύνων και στη συνέχεια, με την πολιτική και τους στόχους του ΣΔΑΠ. Για τον λόγο αυτό απαιτείται τεκμηρίωση, που πρέπει να περιλαμβάνει: τους στόχους και την πολιτική του ΣΔΑΠ, το πεδίο εφαρμογής του ΣΔΑΠ, την περιγραφή της μεθοδολογίας εκτίμησης κινδύνων, την έκθεση εκτίμησης κινδύνων και το σχέδιο διαχείρισης κινδύνων, τις διαδικασίες που περιγράφουν πώς θα μετράται η αποτελεσματικότητα των μέτρων ασφαλείας, τα διάφορα αρχεία που απαιτούνται ρητά από το πρότυπο ISO/IEC 27001 και τη δήλωση εφαρμογής (Κάτσικας Σ. Κ., 2014).

5.4 Προκαταρκτική αξιολόγηση και ενέργειες μετά την πιστοποίηση.

Πριν μπει ο οργανισμός που θέλει να πιστοποιηθεί στη διαδικασία πιστοποίησης κατά ISO/IEC 27001, καλό θα είναι να επιθεωρήσει ενδελεχώς το ΣΔΑΠ και τη δήλωση εφαρμογής γιατί κατά την πιστοποίηση θα χρειαστεί να αποδείξει τη συμμόρφωσή μας με την απαίτηση του προτύπου περί συνεχούς βελτίωσης. Οι ελεγκτές της πιστοποίησης θα αναζητήσουν αποδείξεις ότι το ΣΔΑΠ λειτουργεί και βελτιώνεται συνεχώς. Τέτοιες αποδείξεις μπορεί να είναι αρχεία διεργασιών, όπως εκθέσεις εκτίμησης κινδύνων, επανεξετάσεις από την διοίκηση, αναφορές περιστατικών παραβίασης ασφάλειας, διορθωτικές ενέργειες κ.λπ. Επομένως, το ΣΔΑΠ πρέπει να αφεθεί να λειτουργήσει ομαλά για ένα διάστημα, ώστε να δημιουργηθεί το απαιτούμενο ιστορικό αρχείο της λειτουργίας και της βελτίωσης του, πριν ζητηθεί η πιστοποίηση του (Κάτσικας Σ. Κ., 2014).

Αφού ο οργανισμός καταφέρει να πιστοποιηθεί κατά ISO/IEC 27001 δεν σημαίνει ότι πλέον έχει τελειώσει. Η διοίκηση του οργανισμού οφείλει να επανεξετάζει το ΣΔΑΠ τουλάχιστον μια φορά τον χρόνο, προκειμένου να διασφαλίζει την καταλληλότητα, την επάρκεια και την αποτελεσματικότητα του. Να επανεξετάζει τα περιθώρια βελτίωσης της πολιτικής και των στόχων ασφαλείας και την ανάγκη αλλαγών στο ΣΔΑΠ. Τα αποτελέσματα αυτής της διαδικασίας τεκμηριώνονται και συντηρούνται σε αρχεία.

ΚΕΦΑΛΑΙΟ 6

«ΣΥΜΠΕΡΑΣΜΑΤΑ»

6.1 Συμπεράσματα

Διαπιστώσαμε από όλα όσα έχουμε περιγράψει στα προηγούμενα κεφάλαια ότι οι Τεχνολογίες Πληροφοριών και Πληροφορικής παίζουν πλέον πρωταρχικό ρόλο στην οργάνωση, λειτουργία και βιωσιμότητα μιας επιχείρησης, ενός δημόσιου οργανισμού, μιας υπηρεσίας Ηλεκτρονικής Διακυβέρνησης κ.τ.λ. Παράλληλα, αυξάνονται οι νομοθετικές απαιτήσεις για τη διαφύλαξη της πληροφορίας (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Αρχή Διατήρησης Απορρήτου των Επικοινωνιών κλπ). Η ασφάλεια των πληροφοριών είναι κάτι περισσότερο από ένα πρόγραμμα κατά των ιών (antivirus) και ένα τοίχος προστασίας (firewall). Όλο και περισσότερες επιχειρήσεις αντιλαμβάνονται τις διαφορετικές και συνεχώς αυξανόμενες απαιτήσεις για τη διαχείριση της ασφάλειας της πληροφορίας και επενδύουν στην ενεργητική προστασία της. Η πληροφορία εξάλλου αποτελεί το σημαντικότερο περιουσιακό στοιχείο ενός οργανισμού και συνεπώς οι τρόποι, οι μέθοδοι και οι διαδικασίες που επιλέγονται να εφαρμοστούν προς την κατεύθυνση της ασφαλούς διαχείρισής της, επηρεάζουν άμεσα ή έμμεσα και το επιχειρησιακό αποτέλεσμα.

Το πρότυπο ISO 27001 είναι σήμερα σε οργανωτικό επίπεδο, συνυφασμένο με την έννοια της ασφάλειας της πληροφορίας και περιέχει τις απαιτήσεις για την δημιουργία, εφαρμογή και βελτίωση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών. Σκοπό έχει να εξασφαλίσει ότι εμπεριέχονται επαρκείς και κατάλληλοι έλεγχοι σε θέματα εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας της πληροφορίας για να προστατεύσουν την πληροφορία και τα δεδομένα «ενδιαφερόμενων μερών». Τα ενδιαφερόμενα μέρη, στα οποία απευθύνεται, μπορεί να είναι πελάτες, οργανισμοί και επιχειρήσεις, προσωπικό, συνεργάτες αλλά και η κοινωνία γενικότερα. Το συγκεκριμένο πρότυπο μπορεί να χρησιμοποιηθεί από οποιονδήποτε οργανισμό ανεξάρτητα από το μέγεθος και την δραστηριότητά του, καθώς αναφέρεται στην ασφάλεια της πληροφορίας και όχι στην ασφάλεια των υπολογιστών και των εφαρμογών του.

Κίνδυνοι από τους οποίους δύναται να προφυλαχθεί ένας οργανισμός με την κατάλληλη εφαρμογή ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών μπορεί να είναι ενδεικτικά:

- απώλεια εγγράφων.
- παραποίηση δεδομένων εγγράφων (ηθελημένη ή μη).
- κακή χρήση δικαιωμάτων και προνομίων πρόσβασης σε επιχειρησιακές πληροφορίες.
- αποποίηση ευθυνών ή ενεργειών.
- εξάντληση της πληροφοριακής υποδομής (χωρητικότητα, ικανότητα).
- χρησιμοποίηση παράνομου ή παραποιημένου λογισμικού.

Ορισμένες από τις απαιτήσεις που θα πρέπει να καλύψει ο οργανισμός που εφαρμόζει ένα τέτοιο σύστημα είναι:

- ορισμός του αποδεκτού επιπέδου κινδύνου και αποδοχή παραμένοντος κινδύνου.
- ορισμός ρόλων και αρμοδιοτήτων.
- ορισμός σκοπού και στόχων για το σύστημα.
- παροχή πόρων.
- ανασκόπηση από τη διοίκηση.

Μέσω της εφαρμογής των απαιτήσεων του προτύπου, η επιχείρηση, ο δημόσιος οργανισμός, μια υπηρεσία Ηλεκτρονικής Διακυβέρνησης είναι σε θέση να γνωρίζει, σε πρακτικό και άμεσα λειτουργικό επίπεδο, από τι και σε ποιο βαθμό κινδυνεύει. Με βάση τη γνώση αυτή, δύναται να επιλέξει τους τρόπους και τη μεθοδολογία που θα ακολουθήσει για να αντιμετωπίσει αποτελεσματικά τους κινδύνους αυτούς.

Τέλος, ο Γενικός Κανονισμός Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης (ΕΕ) - ο οποίος εισάγεται επί του παρόντος σε ολόκληρη την Ευρώπη και πέρα από

την τελική προθεσμία εφαρμογής του Μαΐου 2018 - προβλέπει πολυάριθμες ρυθμίσεις και ελέγχους προστασίας προσωπικών δεδομένων, πολλοί από τους οποίους συνιστώνται επίσης από το ISO / IEC 27001: 2013, ISO / IEC 27002: 2013 και άλλα πρότυπα "ISO27k". Οι οργανισμοί που διαθέτουν σήμερα ISO27k ISMS (Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών) είναι πιθανό να έχουν πολλές από τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων - GDPR ήδη σε ισχύ, αλλά ενδέχεται να χρειαστούν κάποιες προσαρμογές. Άλλοι οργανισμοί μπορεί να επιλέξουν να εφαρμόσουν ένα ISO27k ISMS ως ένα γενικό πλαίσιο για τη διαχείριση της ιδιωτικής ζωής και των προσωπικών πληροφοριών στο πλαίσιο της ευρύτερης διαχείρισης των κινδύνων πληροφόρησης, της ασφάλειας των πληροφοριών και της συναφούς συμμόρφωσης, διαχείρισης περιστατικών και ζητημάτων συνέχισης της επιχείρησης. Στο Παράρτημα Ι γίνεται μια προσπάθεια χαρτογράφησης μεταξύ του GDPR και της οικογένειας των προτύπων ISO27k.

ΠΑΡΑΡΤΗΜΑ Ι

Οι έλεγχοι ISO27k χωρίς το πρόθεμα «A» βρίσκονται στο κύριο σώμα του ISO / IEC 27001: 2013. Εκείνα που έχουν προταθεί με «A» παρατίθενται στο Παράρτημα A του ISO / IEC 27001: 2013 και εξηγούνται λεπτομερέστερα στο ISO / IEC 27002: 2013. Επιπλέον πρότυπα του ISO27k συμπληρώνουν διάφορες λεπτομέρειες (π.χ. ISO / IEC 27005 σχετικά με τη διαχείριση του κινδύνου πληροφοριών και ISO / IEC 27018 σχετικά με την προστασία της ιδιωτικής ζωής στις εφαρμογές του cloud computing), ενώ άλλα πρότυπα και πόροι του ISO και μη παρέχουν πολύ περισσότερες πληροφορίες και σε ορισμένες περιπτώσεις προτείνει εναλλακτικές ή συμπληρωματικές προσεγγίσεις και ελέγχους.

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		**Οικογένεια ISO27K**	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
1	Ο GDPR αφορά την προστασία και την ελεύθερη κυκλοφορία των "προσωπικών δεδομένων", που ορίζονται στο άρθρο 4 ως "κάθε πληροφορία που σχετίζεται με ένα φυσικό πρόσωπο που έχει ταυτοποιηθεί ή μπορεί να προσδιοριστεί (« το πρόσωπο στο οποίο αναφέρονται τα δεδομένα »). Αναγνωρίσιμο φυσικό πρόσωπο είναι το πρόσωπο εκείνο το οποίο μπορεί να αναγνωριστεί, άμεσα ή έμμεσα, χρησιμοποιώντας κάποιο αναγνωριστικό όπως ένα όνομα, έναν αναγνωριστικό αριθμό, δεδομένα της γεωγραφικής θέσης του, ένα ηλεκτρονικό αναγνωριστικό ή μπορεί να είναι ένας ή περισσότεροι παράγοντες που είναι συγκεκριμένοι για την φυσική, φυσιολογική, γενετική, ψυχική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα αυτού του φυσικού προσώπου».	A.18.1.4 *κ.λπ.*.	Τα πρότυπα ISO27k εστιάζουν στους κινδύνους της πληροφορίας και ιδιαίτερα στη διαχείριση των ελέγχων της ασφάλειας των πληροφοριών, περιορίζοντας τους απρόβλεπτους κινδύνους που μπορούν να προκύψουν από την διαρροή πληροφοριών των οργανισμών. Στο πλαίσιο του GDPR, η ιδιωτικότητα είναι σε μεγάλο βαθμό ένα ζήτημα εξασφάλισης προσωπικών πληροφοριών των ανθρώπων και ιδιαίτερα των ευαίσθητων δεδομένων που αποθηκεύονται στους υπολογιστές. Τα πρότυπα ISO27k αναφέρουν συγκεκριμένα υποχρεώσεις συμμόρφωσης σχετικά με την προστασία της ιδιωτικής ζωής και την προστασία των προσωπικών πληροφοριών (πιο τυπικά γνωστές ως προσωπικές πληροφορίες - PII - σε ορισμένες χώρες) στον έλεγχο A.18.1.4.A.18.1.4.
2	Το GDPR αφορά την «επεξεργασία προσωπικών δεδομένων στο σύνολο ή εν μέρει με αυτοματοποιημένα μέσα ...» (ουσιαστικά συστήματα πληροφορικής, εφαρμογές και δίκτυα) και σε επιχειρηματικό ή εταιρικό / οργανωτικό πλαίσιο (οι ιδιωτικές οικιακές χρήσεις δεν εμπίπτουν στο πεδίο εφαρμογής).	Πολλοί	Το ISO27k εστιάζει γενικά στην πληροφορία, όχι μόνο σε δεδομένα υπολογιστικών συστημάτων, εφαρμογών και δικτύων. Βασίζεται σ' ένα ευρύτερο πλαίσιο χτισμένο γύρω από ένα «σύστημα διαχείρισης». Το ISO27k ασχολείται συστηματικά με τους κινδύνους και τους ελέγχους των πληροφοριών στο σύνολο τους σ' έναν οργανισμό, συμπεριλαμβανομένων

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		Οικογένεια ISO27K	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
			και θεμάτων πέραν της ιδιωτικότητας και συμμόρφωσης.
3	Ο GDPR αφορά δεδομένα προσωπικού χαρακτήρα για τους πολίτες της Ευρωπαϊκής Ένωσης, είτε αυτά μεταποιούνται στην ΕΕ είτε αλλού	A.18.1.4 *κ.λπ.*.	Το ISO27k έχει παγκόσμιο πεδίο εφαρμογής. Οποιοσδήποτε οργανισμός που αλληλεπιδρά με ανθρώπους στην Ευρωπαϊκή Ένωση μπορεί να εμπίπτει στον GDPR, ειδικά αν συλλέγει προσωπικές πληροφορίες.
4	Οι όροι που σχετίζονται με το απόρρητο του GDPR ορίζονται εδώ τυπικά.	3	Το ISO / IEC 27000 ορίζει τους περισσότερους όρους ISO27k, συμπεριλαμβανομένων ορισμένων όρων απορρήτου. Πολλοί οργανισμοί έχουν τα δικούς τους γλωσσάρια σε αυτόν τον τομέα. **Στην περίπτωση αυτή θα πρέπει να ελεγχθούν ότι οι εταιρικοί ορισμοί δεν έρχονται σε αντίθεση με τον GDPR.**
Κεφάλαιο 1 - Γενικές διατάξεις			
5	Τα δεδομένα προσωπικού χαρακτήρα πρέπει: α) να υποβάλλονται σε νόμιμη, δίκαιη και διαφανή επεξεργασία, · β) συλλέγονται για συγκεκριμένους, ρητούς και νόμιμους σκοπούς μόνο, · γ) να είναι επαρκή σχετικά και περιορισμένα, · δ) να είναι ακριβή, ε) να μην φυλάσσονται παραπάνω χρονικό διάστημα από αυτό που απαιτείται, στ) να υποβάλλονται σε επεξεργασία με ασφάλεια, ώστε να εξασφαλίζεται η ακεραιότητα και η εμπιστευτικότητα τους. Αυτή είναι η τελευταία ενσωμάτωση των αρχικών αρχών του ΟΟΣΑ που δημοσιεύθηκε το 1980. Ο "ελεγκτής" είναι υπεύθυνος για όλα αυτά.	6.1.2, A.8.1.1 A.8.2 A.8.3 A.9.1.1 A.9.4.1 A.10 A.13.2 A.14.1.1 A.15 A.17 A.18 ... Στην ουσία όλα 5 A.6.1.1	Οι επιχειρηματικές διαδικασίες καθώς και οι εφαρμογές, τα συστήματα και τα δίκτυα πρέπει να εξασφαλίζουν επαρκώς τις προσωπικές τους πληροφορίες, απαιτώντας μια ολοκληρωμένη δέσμη τεχνολογικών, διαδικαστικών, φυσικών και άλλων ελέγχων, ξεκινώντας από την αξιολόγηση των συναφών κινδύνων πληροφόρησης. Βλ. Επίσης «προστασία της ιδιωτικής ζωής από το σχεδιασμό» και «προστασία της ιδιωτικής ζωής από προεπιλογή» (άρθρο 25). Προκειμένου να ικανοποιηθούν αυτές οι απαιτήσεις, οι οργανισμοί πρέπει να γνωρίζουν πού είναι οι προσωπικές πληροφορίες, να τις ταξινομήσουν και να εφαρμόσουν τα κατάλληλα μέτρα για την αντιμετώπιση των (α) - (στ). Παρόλο που δεν αναφέρεται ως τέτοια, η λογοδοσία είναι μια σημαντική έννοια στο τμήμα «Ηγεσία» του ISO / IEC 27001.

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		Οικογένεια ISO27K	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
6	Η νόμιμη επεξεργασία προσωπικών δεδομένων πρέπει: α) να έχει συναινέσει από το αντικείμενο για τον συγκεκριμένο σκοπό, β) να απαιτείται από την σύμβαση, γ) να είναι αναγκαία για άλλους λόγους συμμόρφωσης, δ) να είναι αναγκαία για την προστασία των ζωτικών συμφερόντων κάποιου, ε) απαιτείται για λόγους δημοσίου συμφέροντος ή κάποια δημόσια αρχή και στ) να είναι περιορισμένη εάν το άτομο είναι παιδί. Σημείωση: υπάρχουν αρκετές λεπτομερείς και ρητές απαιτήσεις σχετικά με τη νόμιμη επεξεργασία – πρέπει να δει κάποιος τον GDPR Σημείωση: επίσης τα κράτη μέλη της ΕΕ μπορούν να επιβάλλουν πρόσθετους κανόνες.	6.1.2 A.14.1.1 A.18.1.1 *κ.λπ.*	Αυτό θα πρέπει να καλυφθεί κατά την αξιολόγηση και την αντιμετώπιση των κινδύνων πληροφόρησης. Θα επηρεάσει τον σχεδιασμό επιχειρηματικών διαδικασιών / δραστηριοτήτων, εφαρμογών, συστημάτων κλπ. ενός οργανισμού (π.χ. μπορεί να είναι απαραίτητο να καθοριστεί η ηλικία κάποιου πριν προχωρήσει στη συλλογή και χρήση των προσωπικών του πληροφοριών). Αυτές είναι οι επιχειρηματικές απαιτήσεις για τον περιορισμό και την προστασία των προσωπικών πληροφοριών, απαιτούνται πολλοί έλεγχοι ασφαλείας για την μείωση των μη αποδεκτών κινδύνων πληροφόρησης που δεν μπορούν να αποφευχθούν (μη συλλέγοντας / χρησιμοποιώντας τα δεδομένα) ή να μοιραστούν (π.χ. επικαλούμενη κάποιο άλλο μέρος για να πάρει τη συγκατάθεσή του και να συλλέξει τα δεδομένα - έναν κίνδυνο από μόνος του
7	Η συναίνεση του υποκειμένου των δεδομένων πρέπει να ενημερώνεται, να παρέχεται ελεύθερα και να μπορεί αποσύρεται εύκολα ανά πάσα στιγμή.	A.8.2.3 A.12.1.1 A.13.2.4? A.18.1.3 6.1.2 A.14.1.1 A.8.3.2 A.13.2 *κ.λπ.*	Υπάρχει μια απαίτηση να ζητείτε η ενημερωμένη συγκατάθεση για επεξεργασία (διαφορετικά πρέπει να σταματάει) και αυτό να μπορεί να καταδειχθεί. Πρέπει να υπάρχουν διαδικασίες για αυτό και τα αρχεία που αποδεικνύουν τη συγκατάθεση πρέπει να προστατεύονται και να διατηρούνται. Η απόσυρση της συγκατάθεσης συνεπάγεται την δυνατότητα εντοπισμού και κατάργησης των προσωπικών πληροφοριών, ίσως κατά τη διάρκεια της επεξεργασίας τους και ίσως επίσης από αντίγραφα ασφαλείας και αρχείων, καθώς και επιχειρηματικές διαδικασίες για έλεγχο και διεκπεραίωση αιτημάτων.
8	Ειδικοί περιορισμοί ισχύουν για τη συναίνεση για τα παιδιά.	Δείτε Άρθρο 7	Αυτοί οι ειδικοί περιορισμοί ισχύουν κατά τον χρόνο συλλογής των πληροφοριών (π.χ. λήψη συγκατάθεσης γονέα).

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		Οικογένεια ISO27K	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
9	Ειδικοί περιορισμοί ισχύουν για ιδιαίτερα ευαίσθητα δεδομένα που αφορούν τη φυλή, τις πολιτικές απόψεις, τη θρησκεία, τη σεξουαλικότητα, τις γενετικές πληροφορίες και άλλα βιομετρικά στοιχεία κ.λπ. Η επεξεργασία αυτών των πληροφοριών απαγορεύεται από προεπιλογή, εκτός εάν δοθεί συναίνεση και απαιτείται επεξεργασία (όπως ορίζεται στο άρθρο).	A.8.2.1 A.8.2.3 A.14.1.1	Βλ.7 παραπάνω. Είναι σημαντικό να προσδιοριστεί πού μπορούν να υποβάλλονται σε επεξεργασία τα ευαίσθητα δεδομένα, είτε αυτά είναι πραγματικά απαραίτητα, είτε να αποκτηθεί ρητή συναίνεση - παράγοντες που πρέπει να λαμβάνονται υπόψη κατά το σχεδιασμό συστημάτων, εφαρμογών και επιχειρηματικών διαδικασιών.
10	Ειδικοί περιορισμοί ισχύουν επίσης για τα δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.	A.7.1 A.8.2.1 A.8.2.3 6.1.2 A.14.1.1 A.7.1 κ.λπ.	Οποιαδήποτε χρήση αυτών των πληροφοριών θα πρέπει να προσδιορίζεται και να γίνεται μόνο υπό συγκεκριμένες συνθήκες. Αυτές οι πληροφορίες θα πρέπει κατά προτίμηση να μην διατηρούνται εκτός από τις αρχές, αλλά μπορεί να απαιτούνται για ελέγχους ιστορικού, χαρτογράφηση κινδύνου πιστωτικών / απάτης κλπ.
11	Ορισμένοι περιορισμοί δεν ισχύουν εάν δεν είναι δυνατή η αναγνώριση ενός ατόμου από τα δεδομένα που διατηρούνται.	A.8.2.1 A.8.2.3 6.1.2 A.14.1.1 κ.λπ.	Αποφεύγοντας τους κινδύνους πληροφόρησης (χωρίς να ξέρουμε ποια είναι τα θέματα) είναι μια καλή επιλογή, όπου είναι εφικτό να τίθεται το εξής ερώτημα: χρειάζεται η επιχείρηση να γνωρίζει πραγματικά την ταυτότητα ενός ατόμου ή θα αρκεί η συγκέντρωση πληροφοριών / στατιστικών στοιχείων;
Κεφάλαιο 3 - Δικαιώματα του προσώπου στο οποίο αναφέρονται τα δεδομένα			
12	Οι επικοινωνία με τα πρόσωπα στα οποία αναφέρονται τα δεδομένα πρέπει να είναι διαφανής, σαφής και εύκολα κατανοητή.	A.12.1.1 A.14.1.1 A.16 κ.λπ.	Βλέπε παραπάνω. Αυτό επηρεάζει τη διατύπωση διαδικτυακών φορμών, των ειδοποιήσεων, των σεναρίων κλπ. συν τις διαδικασίες. Μπορεί επίσης να είναι σχετική με τη διαχείριση περιστατικών, για παράδειγμα ύπαρξη μηχανισμών που επιτρέπουν στους ανθρώπους να διερευνούν ή να διαμαρτύρονται σε σχέση με τα δικά τους προσωπικά στοιχεία (υποδηλώνοντας ένα μέσο για τον εντοπισμό και την ταυτοποίησή τους), για την ταχεία ανταπόκριση τους και για την τήρηση αρχείων όπως π.χ. επικοινωνιών (π.χ. για τον περιορισμό ή την χρέωση υπερβολικών αιτημάτων).

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		Οικογένεια ISO27K	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
13	Όταν συλλέγονται προσωπικά δεδομένα, πρέπει να δίνονται στους πολίτες (ή να τα διαθέτουν ήδη) αρκετά συγκεκριμένα στοιχεία, όπως λεπτομέρειες σχετικά με τους «ελεγκτές» και τους «υπεύθυνους προστασίας δεδομένων», ανεξάρτητα από το εάν οι πληροφορίες τους θα εξαχθούν (ιδίως εκτός ΕΕ), πόσο καιρό χρονικά θα διατηρείται η πληροφορία, τα δικαιώματά τους και ο τρόπος διερεύνησης / καταγγελίας κλπ.	A.8.2.1 A.8.2.3 A.12.1.1 A.14.1.1 A.16 κ.λπ.	Πρέπει να καθοριστούν και να εφαρμοστούν οι διαδικασίες για την παροχή πληροφοριών δίκαιης επεξεργασίας, οι πληροφορίες σχετικά με τον υπεύθυνο επεξεργασίας δεδομένων και οι σκοποί επεξεργασίας των δεδομένων. Αυτό εξαρτάται εν μέρει από τον εντοπισμό του τόπου όπου χρησιμοποιούνται οι προσωπικές πληροφορίες.
14	Παρόμοιες απαιτήσεις κοινοποίησης ισχύουν στο άρθρο 13 εάν οι πληροφορίες προσωπικού χαρακτήρα αποκτώνται έμμεσα (π.χ. από μια εμπορική λίστα αλληλογραφίας;), οι άνθρωποι πρέπει να ενημερώνονται μέσα σε ένα μήνα και κατά την πρώτη επικοινωνία μαζί τους.	A.8.2.1 A.8.2.3 A.12.1.1 A.14.1 A.16 κ.λπ.	Βλέπε άρθρο 13.
15	Οι άνθρωποι έχουν το δικαίωμα να μάθουν αν ο οργανισμός διατηρεί τις προσωπικές του πληροφορίες, για ποιο σκοπό χρησιμοποιούνται, σε οποίους μπορούν να αποκαλυφθούν κλπ. καθώς και να ενημερώνονται για το δικαίωμα υποβολής καταγγελίας, διόρθωσης ή διαγραφής κ.λπ. .	A.8.1.1 A.8.2.1 A.12.1.1 A.13.2.1 A.14.1.1 κ.λπ.	Τα δικαιώματα των υποκειμένων περιλαμβάνουν τη δυνατότητα απόκτησης ενός αντιγράφου των δικών τους πληροφοριών (που υποδηλώνει και πάλι την ανάγκη ταυτοποίησης και πιστοποίησης πριν ενεργήσουν σε τέτοια αιτήματα), αποκαλύπτοντας τη φύση της επεξεργασίας π.χ. τη λογική πίσω και τις συνέπειες του "προφίλ", καθώς και πληροφορίες σχετικά με τους ελέγχους, αν εξάγονται τα δεδομένα τους. Μπορεί επίσης να επηρεάσει αντίγραφα ασφαλείας και αρχειοθέτησης. Βλέπε επίσης άρθρο 7 για την ανάκληση συγκατάθεσης.
16	Οι άνθρωποι έχουν το δικαίωμα να διορθώνουν, να συμπληρώνουν, να διευκρινίζουν τα προσωπικά τους στοιχεία κ.λπ..	A.12.1.1 A.14.1 A.9 A.16? A.12.3 A.18.1.3	Υποστηρίζει λειτουργικές απαιτήσεις για τον έλεγχο, την επεξεργασία και την επέκταση των αποθηκευμένων πληροφοριών, με διάφορους ελέγχους σχετικά με την αναγνώριση, τον έλεγχο ταυτότητας, την πρόσβαση, την επικύρωση κλπ. Μπορεί επίσης να επηρεάσει αντίγραφα ασφαλείας και αρχειοθέτησης.
17	Οι άνθρωποι έχουν το δικαίωμα να ξεχαστούν, δηλαδή να διαγράψουν τα	6.1.2	Πρόκειται για μια μορφή απόσυρσης της συγκατάθεσης (βλ. Άρθρο 7).

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		Οικογένεια ISO27K	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
	προσωπικά τους στοιχεία και να μην χρησιμοποιούνται πλέον.	A.14.1.1 A.9 A.16 A.12.3 A.8.3.2	Υποστηρίζει τις λειτουργικές απαιτήσεις του συστήματος και της διαδικασίας ώστε να μπορεί να διαγράψει συγκεκριμένες αποθηκευμένες πληροφορίες, με διάφορους ελέγχους σχετικά με την αναγνώριση, τον έλεγχο ταυτότητας, την πρόσβαση, την επικύρωση κλπ. Μπορεί επίσης να επηρεάσει αντίγραφα ασφαλείας και αρχειοθέτησης.
18	Οι άνθρωποι έχουν το δικαίωμα να περιορίζουν την επεξεργασία των προσωπικών τους πληροφοριών.	6.1.2 A.8.2.1 A.8.2.3 A.12.1.1 A.14.1.1 A.16 A.12.3 A.18.1.1	Βλέπε άρθρα 7, 12 κλπ. Μπορεί να χρειαστούν τρόποι για να εντοπιστούν τα συγκεκριμένα δεδομένα που πρέπει να περιοριστούν και να εφαρμόσει νέους κανόνες χειρισμού / επεξεργασίας. Σημειώστε ότι μπορεί επίσης να επηρεάσει τα αντίγραφα ασφαλείας και αρχειοθέτησης.
19	Οι άνθρωποι έχουν δικαίωμα να γνωρίζουν το αποτέλεσμα των αιτημάτων για διόρθωση, συμπλήρωση, διαγραφή, περιορισμό των προσωπικών τους πληροφοριών κ.λπ.	A.12.1.1 6.1.2 A.14.1.1 A.16 κ.λπ.	Η ενημέρωση του εντολέα είναι ένα συμβατικό μέρος της διαδικασίας διαχείρισης περιστατικών, αλλά μπορεί να υπάρξει ξεχωριστή ή παράλληλη διαδικασία ειδικά για καταγγελίες, αιτήματα κ.λπ., καθώς οι συντάκτες δεν είναι συνήθως υπάλληλοι / εμπιστευματοδόχοι.
20	Οι άνθρωποι έχουν δικαίωμα να αποκτήσουν ένα «φορητό» ηλεκτρονικό αντίγραφο των προσωπικών τους δεδομένων για να το χρησιμοποιήσουν προκειμένου να μεταβούν σε διαφορετικό ελεγκτή.	6.1.2 A.13 A.14.1.1 A.8.3 A.10 A.18.1.3 κ.λπ.	Ανάλογα με το σκοπό του οργανισμού, αυτό μπορεί να φαίνεται απίθανο σενάριο στην πράξη (χαμηλός κίνδυνος) και μπορεί να αντιμετωπιστεί καλύτερα με εξαίρεση, χειροκίνητα, χωρίς αυτόματες λειτουργίες του πληροφοριακού συστήματος. Θα πρέπει να λαμβάνετε υπόψιν ότι τα δεδομένα που εξάγονται πρέπει να περιορίζονται στα αναγνωρισμένα και επικυρωμένα πρόσωπα και η επικοινωνία θα πρέπει να γίνεται με ασφάλεια, πιθανώς να είναι κρυπτογραφημένα. Μπορεί επίσης να συνεπάγεται τη διαγραφή ή τον περιορισμό των δεδομένων και την επιβεβαίωσή τους (άρθρα 17, 18 και 19).

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		Οικογένεια ISO27K	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
21	Οι άνθρωποι έχουν το δικαίωμα να αντιταχθούν στην χρήση των πληροφοριών τους για λόγους προφίλ και εμπορίας.	6.1.2 A.12.1.1 A.14.1.1 A.16 A.12.3 κ.λπ.	Δείτε άρθρο 18. Μπορεί να χρειαστούν τρόποι για τον εντοπισμό συγκεκριμένων δεδομένων που δεν θα πρόκειται να υποβληθούν σε επεξεργασία και την εφαρμογή νέων κανόνων χειρισμού / επεξεργασίας.
22	Οι άνθρωποι έχουν το δικαίωμα να επιμένουν ότι οι βασικές αποφάσεις που απορρέουν από την αυτόματη επεξεργασία των προσωπικών τους πληροφοριών αξιολογούνται / επανεξετάζονται χειροκίνητα.	6.1.2 A.12.1.1 A.14.1.1 A.16	Τα συστήματα υποστήριξης λήψης αποφάσεων και λήψης αποφάσεων που περιλαμβάνουν προσωπικές πληροφορίες πρέπει να επιτρέπουν τη μη αυτόματη αναθεώρηση και την αντικατάσταση, με τις κατάλληλες εξουσιοδοτήσεις, ελέγχους πρόσβασης και ακεραιότητας κ.λπ.
23	Οι εθνικοί νόμοι ενδέχεται να τροποποιούν ή να παρακάμπτουν διάφορα δικαιώματα και περιορισμούς για την εθνική ασφάλεια και άλλους σκοπούς.	A.18.1.1	Αυτό αφορά πρωτίστως τις αρχές / τους δημόσιους οργανισμούς και τα συστήματά τους (π.χ. αστυνομία, τελωνεία, μετανάστευση, ένοπλες δυνάμεις), αλλά μπορεί να επηρεάσει ορισμένους ιδιωτικούς / εμπορικούς οργανισμούς, είτε κατά κανόνα (π.χ νομικό τομέα, αμυντική βιομηχανία, κανόνες για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες στις χρηματοπιστωτικές υπηρεσίες;) ή κατ 'εξαίρεση (που συνεπάγεται μια νομικά ορθή χειρωνακτική διαδικασία για την αξιολόγηση και την αντιμετώπιση τέτοιων εξαιρετικών καταστάσεων).
Κεφάλαιο 4 - Έλεγχος και επεξεργασία			
24	Ο «ελεγκτής» (γενικά ο οργανισμός που κατέχει και επωφελείται από την επεξεργασία των προσωπικών στοιχείων) είναι υπεύθυνος για την εφαρμογή κατάλληλων ελέγχων προστασίας προσωπικών δεδομένων	4, 5, 6, 7, 8, 9, 10 και πολλά	Αυτή είναι μια επίσημη υπενθύμιση ότι πρέπει να εφαρμοστεί ένα κατάλληλο, εκτεταμένο δίκτυο ελέγχων ιδιωτικότητας, συμπεριλαμβανομένων πολιτικών και διαδικασιών, καθώς και τεχνικών,

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		Οικογένεια ISO27K	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
	(συμπεριλαμβανομένων πολιτικών και κωδικών δεοντολογίας) λαμβάνοντας υπόψη τους κινδύνους, τα δικαιώματα και τις λοιπές απαιτήσεις μέσα και ίσως πέρα από το GDPR.	του Παραρτήματος Α	φυσικών και άλλων ελέγχων που αντιμετωπίζουν τους κινδύνους πληροφόρησης και τις υποχρεώσεις συμμόρφωσης. Η κλίμακα αυτού απαιτεί συνήθως μια δομημένη, συστηματική προσέγγιση της ιδιωτικής ζωής. Δεδομένων των αλληλεπικαλύψεων, είναι φυσιολογικό να ενσωματωθεί ή τουλάχιστον να ευθυγραμμιστεί και να συντονιστεί η ιδιωτική ζωή με το ISO27k ISMS και άλλες πτυχές, όπως η συμμόρφωση και η διαχείριση της συνέχισης των επιχειρήσεων - με άλλα λόγια, είναι θέμα διακυβέρνησης.
25	Λαμβάνοντας υπόψη τους κινδύνους, το κόστος και τα οφέλη, θα πρέπει να υπάρχει επαρκής προστασία για τις προσωπικές πληροφορίες από το σχεδιασμό τους και από προεπιλογή.	6 και πολλά του Παραρτήματος Α	Υπάρχουν επιχειρησιακοί λόγοι για την κατάλληλη επένδυση στην ιδιωτική ζωή, συμπεριλαμβανομένων των κινδύνων πληροφόρησης και των απαιτήσεων συμμόρφωσης, καθώς και επιλογών εφαρμογής με διάφορες δαπάνες και οφέλη: η επεξεργασία αυτών είναι ένας καλός τρόπος για να εξασφαλιστεί η υποστήριξη και η συμμετοχή της διοίκησης. να σχεδιάζει, να παραδίδει, να εφαρμόζει και να διατηρεί τις ρυθμίσεις περί απορρήτου. Η προστασία της ιδιωτικής ζωής από σχεδιασμό και από προεπιλογή είναι παραδείγματα αρχών προστασίας της ιδιωτικής ζωής που διέπουν τις προδιαγραφές, το σχεδιασμό, την ανάπτυξη, τη λειτουργία και τη συντήρηση πληροφοριακών συστημάτων και διαδικασιών που σχετίζονται με την ιδιωτικότητα συμπεριλαμβανομένων σχέσεων και συμβάσεων με τρίτους π.χ. ISPs και CSPs.
26	Όταν οι οργανισμοί είναι από κοινού υπεύθυνοι για τον προσδιορισμό και την εκπλήρωση των απαιτήσεων προστασίας της ιδιωτικής ζωής σε συνεργασία, πρέπει να διευκρινίσουν και να εκπληρώσουν τους αντίστοιχους ρόλους και ευθύνες τους.	5.3 9.1 A.13.2 A.15 A.16 A.18.1	Οι οργανισμοί πρέπει να διαχειρίζονται τις σχέσεις με τους με τους άλλους επιχειρηματικούς εταίρους, διασφαλίζοντας ότι σε καμιά πτυχή που αφορά την προστασία της ιδιωτικής ζωής αλλά και άλλων πληροφοριών δεν υπάρχουν ρωγμές. Αυτό περιλαμβάνει, για παράδειγμα, από κοινού διερεύνηση και επίλυση περιστατικών ιδιωτικού απορρήτου, παραβιάσεων ή αιτημάτων πρόσβασης, επίτευξη και διατήρηση ενός εγγυημένου επιπέδου συμμόρφωσης με τον GDPR και σεβασμό των συναινετικών σκοπών για τους οποίους αρχικά συγκεντρώθηκαν προσωπικές πληροφορίες, ανεξάρτητα από το πού καταλήγουν.

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		Οικογένεια ISO27K	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
27	Οι οργανισμοί εκτός Ευρώπης πρέπει να ορίσουν επισήμως τους αντιπροσώπους προστασίας της ιδιωτικής ζωής στην Ευρώπη, εφόσον πληρούν ορισμένες προϋποθέσεις (π.χ. προσφέρουν αγαθά και υπηρεσίες σε Ευρωπαίους).	5.3 7.5.1 A.15? A.18.1.4	Αυτή είναι μια από τις πολλές διατυπώσεις συμμόρφωσης: ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων πρέπει να είναι ο κατάλληλος και να βεβαιώνει ότι όλα έγιναν σωστά.
28	Εάν ένας οργανισμός χρησιμοποιεί ένα ή περισσότερα τρίτα μέρη για να επεξεργαστεί προσωπικές πληροφορίες ("επεξεργαστές"), πρέπει να βεβαιωθεί ότι και αυτοί συμμορφώνονται με τον GDPR.	8.2 9.1 A.15 A.18.1.1 A.18.1.3 A.18.1.4	Αυτό ισχύει για τους παρόχους υπηρεσιών διαδικτύου και τους κεντρικούς αντισυμβαλλομένους, τα κέντρα δεδομένων που ανατίθενται σε εξωτερικούς συνεργάτες κλπ., καθώς και άλλες εμπορικές υπηρεσίες, όπου ο οργανισμός διαβιβάζει προσωπικές πληροφορίες σε τρίτους, π.χ. για το τμήμα μάρκετινγκ και διαχείρισης ανθρώπινου δυναμικού, τις υπηρεσίες μισθοδοσίας, τις φορολογικές υπηρεσίες, τις υπηρεσίες συνταξιοδότησης και ιατρικές υπηρεσίες για τους εργαζόμενους. Εφαρμόζεται επίσης στο λήπτη: οι πάροχοι υπηρεσιών πρέπει να αναμένουν να ερωτηθούν σχετικά με τη κατάσταση συμμόρφωσης τους με τον GDPR, οι πολιτικές απορρήτου και άλλοι έλεγχοι (π.χ. οι τυχόν υπεργολάβοι) και να συμπεριληφθούν σε συμβάσεις και συμφωνίες ρήτρες / όροι συμμόρφωσης και διασφάλισης. Οι κίνδυνοι πληροφόρησης πρέπει να προσδιορίζονται, να αξιολογούνται και να αντιμετωπίζονται με τον συνήθη τρόπο και στις δύο πλευρές.
29	Οι επεξεργαστές πρέπει να επεξεργάζονται μόνο τις προσωπικές πληροφορίες σύμφωνα με τις οδηγίες του ελεγκτή και τους ισχύοντες νόμους.	Τα περισσότερα	Οι επεξεργαστές πρέπει να εξασφαλίζουν και να ελέγχουν τις προσωπικές πληροφορίες με τον ίδιο τρόπο με τους ελεγκτές. Μπορούν να είναι υπεύθυνοι για προσωπικές πληροφορίες σχετικά με τους υπαλλήλους κ.λπ. Έτσι ότι θα έχουν όλες τις απαραίτητες ρυθμίσεις για την προστασία της ιδιωτικής ζωής στο χέρι ούτως ή άλλως: είναι απλώς μια περίπτωση επέκτασης τους για να καλύψουν τις πληροφορίες των πελατών και διαχείριση της ιδιωτικής ζωής στις σχέσεις με τους πελάτες (π.χ. ή άλλες έρευνες, περιστατικά και ζητήματα).
30	Οι υπεύθυνοι επεξεργασίας πρέπει να διατηρούν καταγεγραμμένη τεκμηρίωση σχετικά με την ιδιωτική ζωή, τους σκοπούς για τους οποίους συλλέγονται και	7.5	Πολλές σημαντικές διατυπώσεις.

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		Οικογένεια ISO27K	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
	υποβάλλονται σε επεξεργασία οι προσωπικές πληροφορίες, «κατηγορίες» προσώπων στα οποία αναφέρονται τα δεδομένα και προσωπικά δεδομένα κ.λπ.		
31	Οι οργανισμοί πρέπει να συνεργάζονται με τις αρχές (π.χ. για την προστασία της ιδιωτικής ζωής) ή με διαμεσολαβητές προστασίας δεδομένων.	A.6.1.3	Μια άλλη διατύπωση.
32	Οι οργανισμοί πρέπει να εφαρμόζουν, να λειτουργούν και να διατηρούν κατάλληλα τεχνικά και οργανωτικά μέτρα ασφαλείας για τις προσωπικές πληροφορίες, για την αντιμετώπιση των κινδύνων πληροφόρησης.	8.2 8.3 και πολλά του Παραρτήματος Α	Το GDPR αναφέρει ορισμένα παραδείγματα ελέγχου (όπως κρυπτογράφηση, ανωνυμοποίηση και ανθεκτικότητα) που καλύπτουν θέματα εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας δεδομένων, καθώς και μέτρα δοκιμών / διασφάλισης και συμμόρφωσης των εργαζομένων (συνεπάγονται πολιτικές και διαδικασίες, ευαισθητοποίηση / κατάρτιση και επιβολή / ενίσχυση συμμόρφωσης). Το ISO27k ISMS παρέχει ένα συνεκτικό, ολοκληρωμένο και δομημένο πλαίσιο για τη διαχείριση της ιδιωτικής ζωής παράλληλα με άλλους ελέγχους κινδύνου και ασφάλειας πληροφοριών, συμμόρφωσης κ.λπ.
33	Παραβιάσεις της ιδιωτικής ζωής που έχουν ως αποτέλεσμα να εκτεθούν ή να βλαφθούν προσωπικές πληροφορίες πρέπει να κοινοποιούνται αμέσως στις αρχές (εντός 3 ημερών από τη στιγμή που θα τις γνωστοποιήσουν, εκτός εάν δικαιολογούνται καθυστερήσεις).	A.16 A.18.1.4	Οι παραβιάσεις κ.λπ. κανονικά θα αντιμετωπίζονται ως περιστατικά στο πλαίσιο της διαδικασίας διαχείρισης των συμβάντων του ΣΔΑΠ, αλλά ταυτόχρονα θα πρέπει να πληρούνται και οι ειδικές υποχρεώσεις του GDPR (όπως είναι η προθεσμία των 3 ημερών για την κοινοποίηση του συμβάντος στις αρχές). Να σημειωθεί ότι οι απώλειες ή οι κλοπές συσκευών πληροφορικής που περιέχουν προσωπικές πληροφορίες πιθανόν να μην κοινοποιούνται εάν τα δεδομένα είναι ισχυρώς κρυπτογραφημένα χωρίς αυτό να είναι και βέβαιο. Να σημειωθεί επίσης ότι από την στιγμή που θα ξεκινήσει το περιστατικό δεν είναι σαφώς καθορισμένο το πλαίσιο: είναι πιθανό να συγκεντρωθούν και να αξιολογηθούν οι διαθέσιμες πληροφορίες προφανώς πρώτα για να διαπιστωθεί εάν πράγματι έχει συμβεί ένα ανακοινώσιμο περιστατικό, δηλαδή θα πρέπει να διασφαλισθεί ότι το περιστατικό είναι γνήσιο και όχι κάποιος ψευδής συναγερμός.
34	Παραβιάσεις της ιδιωτικής ζωής που έχουν ως αποτέλεσμα να εκτεθούν ή να	A.16	Εκτός από τους νομικούς και ηθικούς προβληματισμούς και την

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		Οικογένεια ISO27K	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
	βλαφθούν οι προσωπικές πληροφορίες των ανθρώπων και κατά συνέπεια ενδέχεται να βλάψουν τα συμφέροντά τους πρέπει να κοινοποιούνται στους πληγέντες «χωρίς αδικαιολόγητη καθυστέρηση».	A.18.1.4	καθοδήγηση από τις αρχές προστασίας προσωπικών δεδομένων, υπάρχουν προφανώς σημαντικά επιχειρηματικά ζητήματα σχετικά με το χρονοδιάγραμμα και τη φύση της αποκάλυψης. Αυτό κανονικά θα αποτελούσε μέρος της διαδικασίας διαχείρισης περιστατικών για σοβαρά ή σημαντικά περιστατικά, στα οποία θα συμμετείχαν ανώτερα στελέχη, ειδικοί και σύμβουλοι. Αποφεύγοντας ακριβώς αυτή την κατάσταση και το σχετικό επιχειρηματικό κόστος, η διαταραχή και η επιδείνωση είναι ένα από τα ισχυρότερα επιχειρήματα για να καταστεί η ιδιωτικότητα μια εταιρική επιταγή και να επενδύσουμε κατάλληλα σε κατάλληλα προληπτικά μέτρα. Το ίδιο σημείο ισχύει και για άλλα σοβαρά / σημαντικά γεγονότα πληροφόρησης φυσικά.
35	Οι κίνδυνοι ιδιωτικού απορρήτου, συμπεριλαμβανομένων των δυνητικών επιπτώσεων, πρέπει να αξιολογούνται, ιδίως όταν εξετάζονται νέες τεχνολογίες / συστήματα / ρυθμίσεις ή διαφορετικά οι κίνδυνοι μπορεί να είναι σημαντικοί (π.χ. «ο προσδιορισμός του προφίλ» που ορίζεται στο άρθρο 4 ως «οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που αποτελείται από χρήση προσωπικών δεδομένων για την αξιολόγηση ορισμένων προσωπικών στοιχείων που σχετίζονται με ένα φυσικό πρόσωπο, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών σχετικά με τις επιδόσεις του φυσικού προσώπου στην εργασία, οικονομική κατάσταση, υγεία, προσωπικές προτιμήσεις, συμφέροντα, αξιοπιστία, συμπεριφορά, τοποθεσία ή κινήσεις "). Οι «σημαντικές επικίνδυνες καταστάσεις» πρέπει να οριστούν από τις εθνικές αρχές προστασίας της ιδιωτικής ζωής, προφανώς.	6.1.2 A.6.1.3 A.8.2.1 ISO/IEC 27005 και ISO 31000	Και πάλι, υπάρχουν σοβαροί επιχειρηματικοί και δεοντολογικοί λόγοι για τον εντοπισμό, την αξιολόγηση και τη διαχείριση των κινδύνων πληροφόρησης (συμπεριλαμβανομένων των κινδύνων ιδιωτικής ζωής και συμμόρφωσης), εκτός από τις υποχρεώσεις του GDPR. Οι κίνδυνοι που σχετίζονται με την προστασία της ιδιωτικής ζωής θα πρέπει πιθανώς να συμπεριληφθούν στα μητρώα εταιρικών κινδύνων παράλληλα με διάφορους άλλους κινδύνους. Ο GDPR υπονοεί επίσης την ενσωμάτωση της εκτίμησης των κινδύνων για την προστασία της ιδιωτικής ζωής στο πλαίσιο των συνήθων δραστηριοτήτων εκτίμησης κινδύνου για έργα αλλαγής επιχειρήσεων, νέες εξελίξεις συστημάτων πληροφορικής κλπ.
36	Οι κίνδυνοι ιδιωτικού απορρήτου που αξιολογούνται ως "υψηλοί" [μη καθορισμένοι] θα πρέπει να κοινοποιούνται στις αρχές, δίνοντάς τους την ευκαιρία να τους σχολιάσουν.	6.1.2 A.6.1.3 A.8.2.1 ISO/IEC 27005 και ISO 31000	Η απαίτηση του GDPR έχει καλές προθέσεις αλλά ασαφείς ιδιότητες: μπορεί να καλύπτεται από εταιρικές πολιτικές σχετικά με τον ακριβή ορισμό των «υψηλών» κινδύνων για την προστασία της ιδιωτικής ζωής αλλά από την άλλη, η συμμετοχή των αρχών μπορεί να είναι χρήσιμη όσον αφορά την επίσημη θέση για την καταλληλότητα και την επάρκεια των προτεινόμενων ελέγχων – όμως αυτό καταλήγει σε επιχειρηματικό κίνδυνο

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		Οικογένεια ISO27K	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
			και στρατηγική απόφαση της διοίκησης.
37	Ένας υπεύθυνος προστασίας δεδομένων πρέπει να αναγνωρίζεται επισήμως υπό καθορισμένες συνθήκες, π.χ. δημόσιους οργανισμούς, οργανισμούς που παρακολουθούν τακτικά και συστηματικά τους πολίτες σε μεγάλη κλίμακα ή εκείνοι που εκτελούν ευρείας κλίμακας επεξεργασία ευαίσθητων προσωπικών πληροφοριών σχετικά με το ποινικό μητρώο.	5.3 A.6.1.1 A.18.1.4	Εκτός από την υποχρέωση του GDPR, ο ρόλος του "Υπευθύνου προστασίας προσωπικών δεδομένων" (ή κάποιος άλλος ισοδύναμος τίτλος) είναι πολύ ευρύτερα εφαρμόσιμος και πολύτιμος, πλήρως ή μερικώς, επισήμως ή ανεπισήμως, υποχρεωτικός ή όχι. Υπάρχουν σαφώς πολλές απόψεις για την προστασία της ιδιωτικής ζωής όμως ένα καθορισμένο εταιρικό πλαίσιο για την προστασία της ιδιωτικής ζωής (ιδανικά ένας ειδικός εξειδικευμένος σε θέματα προστασίας της ιδιωτικής ζωής ή εμπειρογνώμονας) έχει νόημα για σχεδόν όλους τους οργανισμούς. Αυτό είναι ένα άλλο ζήτημα διακυβέρνησης.
38	[Εάν ορίζεται επισήμως] ο υπεύθυνος προστασίας δεδομένων πρέπει να υποστηρίζεται από τον οργανισμό και να ασχολείται με ζητήματα ιδιωτικού απορρήτου.	5.3 A.6.1.1 A.18.1.4	Βλέπε παραπάνω. Οι διατυπώσεις, χωρίς την στήριξη της διοίκησης και την δέσμευση του οργανισμού, ένας υπεύθυνος προστασίας προσωπικών δεδομένων είναι αδύναμος και άσκοπος.
39	[Εάν ορίζεται επισήμως], ο υπεύθυνος προστασίας δεδομένων πρέπει να παρέχει συμβουλές σχετικά με θέματα ιδιωτικότητας, να παρακολουθεί τη συμμόρφωση, να συνεργάζεται με τις αρχές, να ενεργεί ως σημείο επαφής, να αντιμετωπίζει τους κινδύνους για την προστασία της ιδιωτικής ζωής κλπ.	5.3 A.6.1.1 A.18.1.4	Βλέπε παραπάνω. Οι απαιτήσεις του GDPR θα αποτελέσουν τη βάση της περιγραφής του ρόλου του Υπευθύνου Προστασίας Προσωπικών Δεδομένων.
40	Διάφορες αρχές, ενώσεις και φορείς του κλάδου της βιομηχανίας αναμένεται να καταρτίσουν κώδικες δεοντολογίας που θα επεξεργάζονται τον GDPR και το ιδιωτικό απόρρητο και να τους εγκρίνουν τυπικά (με έναν μη καθορισμένο μηχανισμό) και (όπου χρειάζεται) με την εφαρμογή δικών τους μηχανισμών συμμόρφωσης.	5.3, A.6.1.1 A.18.1.4	Παρόλο που πρόκειται για μια γενναία προσπάθεια να προσθέσουμε το βάρος στους κώδικες της βιομηχανίας, αγωνίζεται να επιτύχει μια πλήρη νομική εντολή, αλλά η ηθική υποχρέωση είναι σαφής: η ιδιωτικότητα είναι κάτι περισσότερο από απλή συμμόρφωση με επίσημες, νομικές υποχρεώσεις. Εκτός αυτού, οι κώδικες (και τα πρότυπα ISO27k!) Προσφέρουν οδηγίες καλής πρακτικής και η συμμόρφωση που μπορεί να δημιουργήσει εμπορικά / εμπορικά πλεονεκτήματα.

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		Οικογένεια ISO27K	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
41	Τα όργανα που βρίσκονται πίσω από τους κώδικες δεοντολογίας πρέπει να παρακολουθούν τη συμμόρφωση (από τα μέλη τους), ανεξάρτητα και με την επιφύλαξη της νομικής και κανονιστικής συμμόρφωσης που διενεργείται από τις εθνικές αρχές.	5.3 A.6.1.1 A.18.1.4	Βλέπε παραπάνω.
42	Πρέπει να αναπτυχθούν και να καταχωρηθούν συστήματα εθελοντικής πιστοποίησης προστασίας δεδομένων που προσφέρουν σφραγίδες συμμόρφωσης και σήματα (που ισχύουν για 3 έτη).	5.3 A.6.1.1 A.18.1.4	Παρόμοια συστήματα υπάρχουν ήδη: ο GDPR τους δίνει κάποια επίσημη αναγνώριση, επιπλέον των εμπορικών πλεονεκτημάτων που ήδη εκμεταλλεύονται.
43	Οι οργανισμοί πιστοποίησης που χορηγούν σφραγίδες και σήματα συμμόρφωσης πρέπει να είναι αρμόδιοι και διαπιστευμένοι για το σκοπό αυτό. Η Ευρωπαϊκή Επιτροπή μπορεί να επιβάλει τεχνικά πρότυπα για τα συστήματα πιστοποίησης.	5.3 A.6.1.1 A.18.1.4	Αυτό θα βελτιώσει την αξιοπιστία και τη σημασία των σφραγίδων και σημάτων απορρήτου, αλλά μπορεί επίσης να αυξήσει το κόστος. Δεδομένου ότι είναι εθελοντικά, ανεξάρτητα από το εάν πρέπει να πιστοποιηθεί ή όχι, και ποια συστήματα συμμετοχής είναι εμπορικά / επιχειρηματικά θέματα για τη διοίκηση.
Κεφάλαιο 5 - Μεταφορές δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς			
44	Οι διεθνείς μεταφορές και επεξεργασία προσωπικών πληροφοριών πρέπει να πληρούν τις απαιτήσεις που ορίζονται στα επόμενα Άρθρα.	-	Προοίμιο.
45	Μεταφορές δεδομένων σε χώρες των οποίων οι ρυθμίσεις περί απορρήτου (νόμοι, κανονισμοί, επίσημοι μηχανισμοί συμμόρφωσης ...) κρίνονται ικανοποιητικοί από την Ευρωπαϊκή Επιτροπή (δηλ. Συμμορφώνονται με το GDPR) δεν απαιτούν επίσημη εξουσιοδότηση ή ειδικές πρόσθετες διασφαλίσεις.	A.18.1.4	Οι περισσότερες διατυπώσεις πρέπει να διεκπεραιωθούν από την Επιτροπή. Η συμμόρφωση προϋποθέτει την αποφυγή μεταφορών σε άλλες χώρες, την παρακολούθηση των επίσημων καταλόγων αλλαγών και τη διασφάλιση της ύπαρξης κατάλληλων συμβάσεων / συμφωνιών και άλλων ελέγχων απορρήτου, όπως συμβαίνει με άλλες μεταφορές δεδομένων τρίτων (βλ. ιδίως το άρθρο 28).
46	Μεταφορές δεδομένων σε χώρες των οποίων οι ρυθμίσεις περί απορρήτου (νόμοι, κανονισμοί, επίσημοι μηχανισμοί συμμόρφωσης ...) δεν κρίνονται ικανοποιητικοί από την Ευρωπαϊκή Επιτροπή (δηλαδή συμμορφώνονται με τον GDPR), αλλά πληρούν ορισμένα άλλα κριτήρια, απαιτούν πρόσθετες	A.18.1.4	Ουσιαστικά, ο οργανισμός πρέπει να εφαρμόσει και να διασφαλίσει την επάρκεια των ελέγχων ιδιωτικότητας πριν από τη μεταφορά προσωπικών δεδομένων σε αυτές τις χώρες και, στη συνέχεια, π.χ. κατάλληλες συμβατικές ρήτρες και δραστηριότητες συμμόρφωσης.

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		Οικογένεια ISO27K	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
	διασφαλίσεις.		
47	Οι εθνικές αρχές μπορούν να εγκρίνουν νομικά δεσμευτικούς κανόνες απορρήτου που επιτρέπουν μεταφορές σε μη εγκεκριμένες χώρες.	A.18.1.4	Οι διατυπώσεις μπορούν να επηρεάσουν τους συμβατικούς όρους, τις ρυθμίσεις συμμόρφωσης, τις υποχρεώσεις κ.λπ. Συμβουλή: μπορεί να μην αξίζει την επιδείνωση, τους κινδύνους και το κόστος.
48	Οι απαιτήσεις για ευρωπαϊκές οργανώσεις από αρχές εκτός Ευρώπης για αποκάλυψη προσωπικών δεδομένων ενδέχεται να είναι άκυρες, εκτός εάν καλύπτονται από διεθνείς συμφωνίες ή συνθήκες.	A.18.1.4, A.16	Τέτοιες καταστάσεις θα αντιμετωπίζονταν κανονικά από νομικούς και ρυθμιστικούς ειδικούς συμμόρφωσης - αλλά θα μπορούσαν να ξεκινούν ως περιστατικά.
49	Ωστόσο, ισχύουν περισσότερες προϋποθέσεις για τη μεταφορά προσωπικών πληροφοριών σε μη εγκεκριμένες χώρες, π.χ. ρητή συγκατάθεση των υποκειμένων των δεδομένων.	A.18.1.4	Η Επιτροπή σκοπίμως δυσκολεύει, ή μάλλον αποδίδει μεγάλη προσοχή, καθώς οι κίνδυνοι για την προστασία της ιδιωτικής ζωής είναι υψηλότεροι.
50	Οι διεθνείς αρχές θα συνεργαστούν για την ιδιωτική ζωή.	-	-
Κεφάλαιο 6 - Ανεξάρτητες εποπτικές αρχές			
51-59	[Ανησυχία εθνικών φορέων για την εποπτεία της ιδιωτικής ζωής.]	-	-
Κεφάλαιο 7 - Συνεργασία και συνέπεια			
60-76	[Οι εποπτικές αρχές ανησυχούν και το Συμβούλιο προστασίας δεδομένων της ΕΕ.]	-	-
Κεφάλαιο 8 - Διορθωτικά μέτρα, ευθύνη και κυρώσεις			
77-81	[Οι εποπτικές αρχές μπορούν να ασχολούνται με τις καταγγελίες περί ιδιωτικού απορρήτου.]	-	-
82	Όποιος πληγεί από παραβιάσεις του GDPR έχει δικαίωμα αποζημίωσης από τον	A.18.1.4	-

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		Οικογένεια ISO27K	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
	ελεγκτή (ες) ή τον μεταποιητή (ες).		
83	Τα διοικητικά πρόστιμα που επιβάλλονται από τις εποπτικές αρχές είναι «αποτελεσματικά, αναλογικά και αποτρεπτικά». Καθορίζονται διάφορα κριτήρια. Ανάλογα με τις παραβάσεις και τις περιστάσεις, τα πρόστιμα ενδέχεται να φτάσουν τα 20 εκατομμύρια ευρώ ή το 4% του συνολικού ετήσιου κύκλου εργασιών παγκοσμίως για το προηγούμενο έτος, εάν είναι μεγαλύτερα.	6 A.18.1.4	Τεράστια πρόστιμα προβλέπονται και σαφώς αποτελούν ισχυρό αποτρεπτικό παράγοντα, που αντιπροσωπεύει ένα σημαντικό μέρος του δυνητικού αντικτύπου των παραβιάσεων της ιδιωτικής ζωής κ.λπ. στην εκτίμηση της οργάνωσης σχετικά με τη συμμόρφωση με τους κανονισμούς GDPR και άλλους κινδύνους για την προστασία της ιδιωτικής ζωής.
84	Μπορούν να επιβληθούν και άλλες κυρώσεις. Πρέπει επίσης να είναι "αποτελεσματικές, ανάλογες και αποτρεπτικές".	6 A.18.1.4	Βλέπε παραπάνω.
Κεφάλαιο 9 - Διατάξεις σχετικές με ειδικές καταστάσεις επεξεργασίας			
85	Οι χώρες πρέπει να εξισορροπήσουν τα δικαιώματα ιδιωτικής ζωής / προστασίας δεδομένων με την ελευθερία έκφρασης, τη δημοσιογραφία, την ακαδημαϊκή έρευνα κλπ. Μέσω κατάλληλων νόμων.	6 A.18.1.1 A.18.1.4	Τα ζητήματα που απορρέουν από το άρθρο αυτό μπορούν να καταλήξουν σε διαφορετικές νομικές ερμηνείες στο δικαστήριο και, συνεπώς, και πάλι υπάρχουν κίνδυνοι πληροφόρησης που πρέπει να εντοπιστούν, να εκτιμηθούν και να αντιμετωπιστούν σε περίπτωση προσωπικών πληροφοριών.
86	Τα προσωπικά δεδομένα σε επίσημα έγγραφα μπορούν να κοινολογηθούν εάν τα έγγραφα απαιτούνται τυπικά για να αποκαλυφθούν σύμφωνα με τους νόμους περί «ελευθερίας ενημέρωσης».	6 A.18.1.1 A.18.1.4	Μπορεί να είναι εφικτή η επεξεργασία προσωπικών ή άλλων ευαίσθητων πληροφοριών - βλ. ISO / IEC 27038.
87	Οι χώρες μπορούν να επιβάλλουν περαιτέρω ελέγχους απορρήτου για τους εθνικούς αριθμούς ταυτότητας.	6 A.18.1.1 A.18.1.4	Οι εθνικοί αριθμοί ταυτότητας μπορούν να χρησιμοποιηθούν ως μυστικοί προσωπικοί έλεγχοι ταυτότητας, οπότε πρέπει να παραμείνουν εμπιστευτικοί για να μειωθεί ο κίνδυνος κλοπής ταυτότητας. Στην πραγματικότητα είναι ευαίσθητες προσωπικές πληροφορίες, υπονοώντας την ανάγκη για κρυπτογράφηση και άλλους ελέγχους ασφάλειας / ιδιωτικότητας.
88	Οι χώρες ενδέχεται να επιβάλλουν περαιτέρω περιορισμούς στην εταιρική	6	Οι νόμοι για την απασχόληση ενδέχεται να διασταυρώνονται με τον GDPR

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)		Οικογένεια ISO27K	
Άρθρο	Περίγραμμα/Περίληψη	Έλεγχος	Παρατηρήσεις
	επεξεργασία και τη χρήση προσωπικών πληροφοριών σχετικά με τους υπαλλήλους, π.χ. για την προστασία της ανθρώπινης αξιοπρέπειας και των θεμελιωδών δικαιωμάτων.	A.18.1.1 A.18.1.4	και το ιδιωτικό απόρρητο, περιπλέκοντας περαιτέρω τη συμμόρφωση και μεταβάλλοντας τους κινδύνους πληροφόρησης σε αυτόν τον τομέα.
89	Όπου πρόκειται να αρχειοθετηθούν προσωπικά δεδομένα, π.χ. για ερευνητικούς και στατιστικούς σκοπούς, οι κίνδυνοι για την προστασία της ιδιωτικής ζωής πρέπει να αντιμετωπιστούν μέσω κατάλληλων ελέγχων, όπως η ψευδονομία και η ελαχιστοποίηση των δεδομένων όπου αυτό είναι εφικτό.	6 A.18.1.4	Οι ανησυχίες για την προστασία της ιδιωτικής ζωής παραμένουν εφ 'όσον τα υποκείμενα των δεδομένων είναι ζωντανά (ίσως και περισσότερο εάν οι οικογένειές τους ή οι κοινότητες ενδέχεται να επηρεαστούν από παραβιάσεις). Λαμβάνοντας υπόψη αυτό, οι κίνδυνοι πληροφόρησης πρέπει να προσδιορίζονται, να αξιολογούνται και να αντιμετωπίζονται κατάλληλα με τον συνήθη τρόπο.
90	Οι χώρες μπορούν να θεσπίσουν πρόσθετους νόμους που αφορούν το απόρρητο των εργαζομένων και τις υποχρεώσεις περί απορρήτου.	6 A.18.1.1 A.18.1.4	Οι νόμοι για την απασχόληση ή τον απόρρητο μπορεί να διασταυρώνονται με τον GDPR και το ιδιωτικό απόρρητο, ακόμα περισσότερο περιπλέκοντας τη συμμόρφωση και μεταβάλλοντας τους κινδύνους πληροφόρησης σε αυτόν τον τομέα.
91	Οι προϋπάρχοντες κανόνες περί ιδιωτικότητας για εκκλησίες και θρησκευτικούς συλλόγους μπορούν να συνεχιστούν, "υπό την προϋπόθεση ότι θα ευθυγραμμιστούν με τον GDPR.	A.18.1.4	Ένα εξαιρετικά διφορούμενο άρθρο.
Κεφάλαιο 10 - Κατ 'εξουσιοδότηση πράξεις και εκτελεστικές πράξεις			
92-99	[Ανησυχία για τον τρόπο με τον οποίο η ΕΕ εκδίδει το GDPR.]	A.18.1.1	Δεν σχετίζονται με τις ρυθμίσεις απορρήτου ενός συγκεκριμένου οργανισμού, εκτός από το βαθμό που χρειάζεται να συμμορφώνονται με τους ισχύοντες νόμους και κανονισμούς.

ΠΙΝΑΚΑΣ ΠΑΡΑΡΤΗΜΑΤΟΣ Ι ΑΝΤΙΠΑΡΑΒΟΛΗ GDPR ΚΑΙ ISO27001

(Πηγή : (ISO27K Forum, 2017))

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Almarabeh, T., & AbuAli, A. (2010). A general framework for e-government: definition maturity challenges, opportunities, and success. *European Journal of Scientific Research, 39*(1), σσ. 29-42.
2. Arnason, S. T., & Willett, K. D. (2007). *How to achieve 27001 certification: An example of applied compliance management.* CRC Press.
3. BSI, I. (2005). Sicherheitsmanagement und IT-Grundschutz-BSI-Standards zur IT-Sicherheit.
4. Cannon, J. (2004). *Privacy: What Developers and IT Professionals Should Know.* London: Addison-Wesley.
5. Danziger, J. N., & Andersen, K. V. (2002). The Impacts of Information Technology on Public Administration: an Analysis of Empirical Research from the "Golden Age" of Transformation. *International Journal of Public Administration [1], 25*(5), σσ. 591-627.
6. De Vivo, M., de Vivo, G. O., & Germinal, I. (1998, April). Internet security attacks at the basic levels. *ACM SIGOPS Operating Systems Review, 32*(2), σσ. 4-15.
7. Demopoulos, T. (n.d.). *Demopoulos Assosiates*. Ανάκτηση από Web της Demopoulos Assosiates: http://demop.com/articles.html
8. EC. (2017). Ευρωπαϊκό πλαίσιο διαλειτουργικότητας - Στατηγική εφαρμογής. Βρυξέλες.
9. EUR-Lex. (2003). *«Ηλεκτρονική διακυβέρνηση»: η επιγραμμική δημόσια διοίκηση.* Ανάκτηση από Πρόσβαση στο δίκαιο της Ευρωπαϊκής Ένωσης: http://europa.eu/legislation_summaries/information_society/strategies/l24226b_el.htm
10. Field, T. E. (2003). *OECD E-Government Studies The E-Government Imperative.* OECD Publishing.
11. Gouscos, D., Georgiadis, P., & Sagris, T. (2000, October). From Introvert IT Systems to Extrovert e-Services: e-Government as an enabler for e-Citizens and e-Business A

Framework of Principles. *In Electronic Business and Electronic Work 2000 Conference, eBusiness and eWork Virtual Conference*.

12. Grönlund, Å., & Horan, T. (2005). Introducing e-gov: history, definitions, and issues. *Communications of the association for information systems, 15*(1), σσ. 713-729.

13. Hahamis, P., lles, J., & Healy, M. (2005). e-Government in Greece: opportunities for improving the efficiency and effectiveness of local government. *Electronic Journal of e-government, 3*(4), σσ. 185-192.

14. Hansen, M. (2016). Data Protection by Design and by Default à la European General Data Protection Regulation. *Privacy and Identity Management. Facing up to Next Steps*, σσ. 27-38.

15. Howard, M. (2001). E-government across the globe: how will'e'change government. *e-Govenment, 90, 80*.

16. ISO/IEC. (2017, September). *The ISO Survey of Management System Standard Certifications 2016.* International Organization for Standardization. Ανάκτηση Σεπτέμβριος 7, 2017, από http://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/00._Executive_summary_2016_Survey.pdf?nodeid=19208898&vernum=-2

17. ISO/IEC 27000. (2016). *Information technology - Security techniques - Information security management systems - Overview and vocabulary*. International Organization for Standardization.

18. ISO/IEC 27001. (2013). *Information technology - Security Techniques - Information Security Management Systems - Requirements* . International Organization for Standardization.

19. ISO/IEC 27002. (2013). *Information technology - Security techniques - Code of practice for information security controls.* International Organization for Standardization.

20. Iso27001security.com. (2017). *ISO27K Information Security*. Ανάκτηση Οκτώβριος 11, 2017, από http://www.iso27001security.com/index.html

21.ISO27K Forum. (2017). ISMS implementation and certification process flowchart v4. Ανάκτηση Σεπτέμβριος 27, 2017, από Iso27001security.com: http://www.iso27001security.com/html/toolkit.html

22.ISO27K Forum. (2017, June). *Iso27001security.com.* Ανάκτηση Σεπτέμβριος 27, 2017, από http://www.iso27001security.com/ISO27k_Standards_listing.pdf

23.ISO27K Forum. (2017). *Iso27001security.com.* Ανάκτηση Σεπτέμβριος 10, 2017, από http://www.iso27001security.com/html/27002.html

24.ISO27K Forum. (2017). *Iso27001security.com.* Ανάκτηση Σεπτέμβριος 16, 2017, από http://www.iso27001security.com/html/timeline.html

25.Markellos, K., Markellou, P., Panayiotaki, A., & Stergianeli, E. (2007). Current State of Greek E-Government Initiatives. *Journal of Business Systems, Governance and Ethics, 2*(3), σσ. 67-88.

26.Middleton, M. R. (2007). Approaches to evaluation of websites for public sector services. In Kommers, Piet, Eds. *Proceedings IADIS Conference on e-Society*, σσ. 279-284.

27.Mohammad, H., Almarabeh, T., & Ali, A. A. (2009). E-government in Jordan. *European Journal of Scientific Research, 35*(2), σσ. 188-197.

28.Ndou, V. (2004). E-government for developing countries: opportunities and challenges. *The electronic journal of information systems in developing countries, 18*.

29.OECD. (1980). *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data.* Ανάκτηση Σεπτέμβριος 20, 2016, από OECD: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

30.OECD. (2013). *2013 OECD Privacy Guidelines*. Ανάκτηση September 20, 2017, από OECD: http://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

31.Pardo, T. (2000). *Realizing the promise of digital government: It's more than building a web site.* Albany, NY: Center for Technology in Goverment.

32.Pelnekar, C. (2011). Planning for and Imlpementing ISO 27001. *ISACA Journal, 4*(4), σσ. 1-8.

33. Regulation, G. (2016). 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. *Official Journal of the European Union (OJ), 59*, σσ. 1-88.

34. Ronaghan, S. A. (2002). *Benchmarking e-government: a global perspective.* Assessing the progress of the UN member states. United Nations Division for Public Economics and Public Administration & American Society for Public Administration.

35. Roßnagel, A., & Nebel, M. (2016). *Die neue Datenschutzgrundverordnung – Ist das Datenschutzrecht nun für heutige Herausforderungen gerüstet?* Policy Paper.

36. Seifert, W. J., & Petersen, R. E. (2002). The Promise of All Things E? Expectations and Challenges of Emergent Electronic Government. *Perspectives on Global Development and Technology, 1*(2), σσ. 193-212.

37. Singh, S., & Karaulia, D. S. (2011, December). E-governance: information security issues. *Proceedings of the International Conference on Computer Science and Information Technology*, σσ. 120-124.

38. Slidesharenet. (2015, August). Ανάκτηση Σεπτέμβριος 16, 2017, από Slidesharenet: https://www.slideshare.net/BryPoenya/infosec-audit-lecture4-51384073

39. The World Bank. (2001). Ανάκτηση Μάϊος 18, 2017, από http://www.worldbank.org/en/topic/ict/brief/e-government

40. Tsoumas, B. (2007). *Ontologies as a means for developing Information Systems Security Management Practices.* Ανάκτηση Σεμπτέμβριος 27, 2017, από https://www.infosec.aueb.gr/Publications/PhD%20Thesis%20Tsoumas%20Bill.pdf

41. United Nations. (2014). *E-Goverment Knowledge Database*. Ανάκτηση September 12, 2017, από https://publicadministration.un.org/egovkb/en-us/Data/Region-Information

42. United Nations. (2016). *E-Government Survey 2016 E-Government in support of sustainable development.* New York: UN.

43. Vrakas, N., Kalloniatis, C., & Lambrinoudakis, C. (2010). Privacy requirements engineering for trustworthy e-government services. *Trust and Trustworthy Computing*, σσ. 298-307.

44. ΑΠΔΠΧ. (2016). *Θεσμικό πλαίσιο για την προστασία των προσωπικών δεδομένων*. Ανάκτηση 9 21, 2017, από Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα: http://www.dpa.gr/portal/page?_pageid=33,23367&_dad=portal&_schema=PORTAL

45. Αποστολάκης, Ι., Λουκής, Ε., & Χάλαρης, Ι. (2004). *Ηλεκτρονική Διακυβέρνηση.* Εθνική Σχολή Δημόσιας Διοίκησης.

46. Βεργή, Ε. (2009). *Η Διακυβέρνηση στην εποχή του Web 2.0.* Αθήνα: Παρατηρητήριο για την Κοινωνία της Πληροφορίας. Ανάκτηση Σεπτέμβριος 13, 2017, από http://www.infosoc.gr/NR/rdonlyres/5CDB2236-DD00-410C-B5AB-D4CF80E5AF93/6870/EGOV_%CE%97%CE%BB%CE%94%CE%B9%CE%B1%CE%BA%CF%85%CE%B2%CE%AD%CF%81%CE%BD%CE%B7%CF%83%CE%B7Web2.pdf

47. Γιαννουκάκου, Α. (2011). *Ηλεκτρονική Διακυβέρνηση.* ΕΚΔΔΑ.

48. Γκρίτζαλης, Σ., Γκρίτζαλης, Δ., & Κάτσικας, Σ. (2004). *Ασφάλεια Δικτύων Υπολογιστών.* Αθήνα: Παπασωτηρίου.

49. Διακονικολάου, Κ., & Μυλωνόπουλος, Ν. (2004). *Το παρόν και το μέλλον των Ηλεκτρονικών Υπηρεσιών του Κράτους προς τις Επιχειρήσεις (Government to Business) στην Ελλάδα.* E-Business Forum.

50. Δρογκάρης, Π. (2013). *Ασφάλεια και προστασία της ιδιωτικότητας σε πληροφοριακά συστήματα ηλεκτρονικής διακυβέρνησης.* (Doctoral dissertation, Πανεπιστήμιο Αιγαίου. Σχολή Θετικών Επιστημών. Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων).

51. Ευρωπαϊκή Επιτροπή. (2017). *Ευρωπαϊκό πλαίσιο διαλειτουργικότητας - Στατηγική εφαρμογής.* Βρυξέλλες.

52. Ευρωπαϊκό Κοινοβούλιο. (1995). Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου για την προστασία των φυσικών προσώπων

έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. *Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων*, 1-9.

53. Ευρωπαϊκό Κοινοβούλιο. (2006). Οδηγία 2006/123/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Δεκεμβρίου 2006 , σχετικά με τις υπηρεσίες στην εσωτερική αγορά. *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, 1-33.

54. Καλλονιάτης, Χ. (2011). *Ασφάλεια Δεδομένων στην Κοινωνία της Πληροφορίας - Ιδιωτικότητα.* Μυτιλήνη: Πανεπιστήμιο Αιγαίου.

55. Καλογήρου, Γ., Παναγιωτόπουλος, Π., Τσακανίκας, Ά., & Σιώκας, Ε. (2015). Ηλεκτρονική Διακυβέρνηση. Στο *Κοινωνία της Πληροφορίας & Οικονομία της Γνώσης* (σσ. 154-190). Ελληνικά Ακαδημαϊκά Συγγράμματα και Βοηθήματα.

56. Καρδάρη, Β. Μ. (2011). Εφαρμογή του προτύπου ISO/IEC 27001: 2005 στη διαχείριση κρίσιμων πληροφοριών της υπηρεσίας πολιτικής αεροπορίας. (Master's thesis).

57. Κάτσικας, Σ. (2016). *Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών – ΣΔΑΠ.* Ανάκτηση Σεπτέμβριος 16, 2017, από https://evdoxos.ds.unipi.gr/modules/document/file.php/DS134/2016-2017/%CE%A3%CF%85%CF%83%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1%CE%B4%CE%B9%CE%B1%CF%87%CE%B5%CE%AF%CF%81%CE%B9%CF%83%CE%B7%CF%82%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82 2016-201

58. Κάτσικας, Σ. Κ. (2014). *Διαχείριση Της Ασφάλειας Πληροφοριών.* Πεδίο.

59. Κιοσσέ, Ε. (2011). Η πορεία της Ηλεκτρονικής Διακυβέρνησης στις χώρες της ΕΕ και την Ελλάδα-Οι επιδόσεις των χωρών. (Master's Thesis).

60. ΚτΠ. (2008). *Ελληνικό Πλαίσιο Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Πρότυπα Διαλειτουργικότητας.* Ανάκτηση Σεπτέμβριος 15, 2017, από http://www.e-gif.gov.gr/portal/pls/portal/docs/211041.PDF

61.Λεταράκη, Δ. (2016). *Σύστημα διαχείρισης ασφάλειας πληροφοριών κατά ISO27001:2013-Υλοποίηση web εφαρμογής για audits.* (Master's Thesis, Πανεπιστήμιο Πειραιώς).

62.Λιουδάκης, Γ. (2008). *Προστασία Προσωπικών Δεδομένων Σε Έξυπνα Περιβάλλοντα.* Διδακτορική διατριβή.

63.Μαυρίδης, Ι. (2015). *Ασφάλεια πληροφοριών στο διαδίκτυο.* Κάλλιπος.

64.Μήτρου, Λ. (2010). Η Προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνίες. Η νομική διάσταση. Στο Κ. Λαμπρινουδάκης, *Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών* (σσ. 505-552). Αθήνα: Παπασωτηρίου.

65.Παπαδάκης, Α., Μαυροειδής, Β., & Ρηγοπούλου, Ε. (2012). *Ηλεκτρονική Διακυβέρνηση και Πολίτες.* Υπουργείο Εσωτερικών,Αποκέντρωσης & Ηλεκτρονικής Διακυβέρνησης.

66.Παρασκευάς, Μ., Ασημακόπουλος, Γ., & Τριανταφύλλου, Β. (2015). *Κοινωνία της Πληροφορίας.* Κάλλιπος.

67.Παρατηρητήριο για τη Διοικητική Μεταρρύθμιση. (2013). *Εξέλιξη των 20 βασικών υπηρεσιών Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα.* Αθήνα: ΚτΠ Α.Ε.

68.Πετροπούλου, Ν. Α. (2015). *Η ηλεκτρονική διακυβέρνηση στην Ελλάδα και την Ευρώπη.* Πτυχιακή Εργασία, Τ.Ε.Ι Δυτικής Ελλάδος. Ανάκτηση Σεπτέμβριος 27, 2017, από http://repository.library.teimes.gr/xmlui/bitstream/handle/123456789/3345/

69.ΠΗΔ. (2012). *Πλαίσιο Ψηφιακής Αυθεντικοποίησης.* Ανάκτηση Σεπτέμβριος 18, 2017, από e-gif.gov.gr: http://www.e-gif.gov.gr/portal/pls/portal/docs/840023.PDF

70.Ράπτης, Χ. (2016). *Η ασφάλεια των δεδομένων στην ηλεκτρονική διακυβέρνηση:νομικές πτυχές.* Ανάκτηση Σεπτέμβριος 27, 2016, από http://dspace.lib.uom.gr/handle/2159/19586