ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

# ΟΔΗΓΟΣ ΑΥΤΟΑΞΙΟΛΟΓΗΣΗΣ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΟΡΓΑΝΙΣΜΩΝ (CYBERSECURITY SELF ASSESSMENT TOOL)


# ΟΔΗΓΟΣ ΑΥΤΟΑΞΙΟΛΟΓΗΣΗΣ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΟΡΓΑΝΙΣΜΩΝ

(CYBERSECURITY SELF ASSESSMENT TOOL)

ΑΚΡΙΒΕΣ ΑΝΤΙΓΡΑΦΟ

**ΥΨηΔ 20/07/2022**
**Α.Π.: 31877 ΕΞ 2022**

**ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ**
ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΔΙΕΥΘΥΝΣΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΤΜΗΜΑ ΑΠΑΙΤΗΣΕΩΝ ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ
ΤΜΗΜΑ ΚΑΝΟΝΙΣΤΙΚΗΣ ΣΥΜΜΟΡΦΩΣΗΣ
Ταχ. Δ/νση: Χανδρή 1 & Θεσ/κης
ΤΚ: 18346 Μοσχάτο Αττικής
Πληροφορίες: Ι. Αλεξάκης, Α. Σταμούλης
Τηλ.: 210 4802916
E-mail: cyber-assessment@mindigital.gr

**Θέμα: Έκδοση Οδηγού Αυτοαξιολόγησης της ασφάλειας των συστημάτων δικτύου και πληροφοριών των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών (ΦΕΒΥ)**

**ΑΠΟΦΑΣΗ**

Έχοντας υπόψη:

1. Το ν. 4622/2019 «Επιτελικό Κράτος: οργάνωση, λειτουργία και διαφάνεια της Κυβέρνησης, των κυβερνητικών οργάνων και της κεντρικής δημόσιας διοίκησης» (Α' 133).
2. Το π.δ. 81/2019 «Σύσταση, συγχώνευση, μετονομασία και κατάργηση Υπουργείων και καθορισμός των αρμοδιοτήτων τους - Μεταφορά υπηρεσιών και αρμοδιοτήτων μεταξύ Υπουργείων» (Α΄119).
3. Του π.δ. 40/2020 «Οργανισμός του Υπουργείου Ψηφιακής Διακυβέρνησης» (Α΄85).
   i. Την υπ΄ αριθμ. Υ6/2019 απόφαση του Πρωθυπουργού «Ανάθεση αρμοδιοτήτων στον Υπουργό Επικρατείας» ( Β΄2902).
   ii. Την υπ' αριθμ. 4498/09.11.2020 κοινή απόφαση του Πρωθυπουργού και του Υπουργού Επικρατείας «Διορισμός μετακλητού Γενικού Γραμματέα Τηλεπικοινωνιών και Ταχυδρομείων του Υπουργείου Ψηφιακής Διακυβέρνησης» (ΦΕΚ ΥΟΔΔ 951).
   iii. Την υπ' αριθμ. 4695/24.11.2020 απόφαση του Υπουργού Επικρατείας «Τροποποίηση της υπό στοιχεία ΓΔΟΔΥ/ ΔΔΥ/1656/10.12.2019 Απόφασης του Υπουργού Επικρατείας «Μεταβίβαση του δικαιώματος υπογραφής «Με εντολή Υπουργού» στον Γενικό Γραμματέα Τηλεπικοινωνιών και Ταχυδρομείων του Υπουργείου Ψηφιακής Διακυβέρνησης», όπως ισχύει (ΦΕΚ Β' 5347).
4. Το ν. 4577/2018 «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις» (Α' 199).
5. Την υπ' αριθμ. 1027/2019 απόφαση του Υπουργού Επικρατείας «Θέματα εφαρμογής και διαδικασιών του ν. 4577/2018 (Α'199)» (Β' 3739).

**ΑΠΟΦΑΣΙΖΟΥΜΕ**

1. Εκδίδουμε Οδηγό Αυτοαξιολόγησης της ασφάλειας των συστημάτων δικτύου και πληροφοριών των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών (ΦΕΒΥ), όπως αυτός προβλέπεται στις διατάξεις της παραγράφου 6 του άρθρου 4 και 17 της υπ' αριθμ. 1027/2019 απόφασης του Υπουργού Επικρατείας «Θέματα εφαρμογής και διαδικασιών του ν. 4577/2018 (Α'199)» (Β' 3739).
2. Η αυτοαξιολόγηση διενεργείται σε ετήσια βάση ή κατόπιν πρόκλησης σοβαρής διατάραξης της παροχής βασικής υπηρεσίας από συμβάν κυβερνοασφάλειας, με τη χρήση του παρόντος Οδηγού. Ο Υπεύθυνος Ασφάλειας Πληροφοριών και Δικτύων του οργανισμού κοινοποιεί στην Εθνική Αρχή Κυβερνοασφάλειας τα αποτελέσματα της αυτοαξιολόγησης, συνοδευόμενα από σχετικό πλάνο διορθωτικών ή βελτιωτικών ενεργειών, εντός προθεσμίας που τάσσεται από την ως άνω Αρχή.
3. Ο Οδηγός Αυτοαξιολόγησης της ασφάλειας των συστημάτων δικτύου και πληροφοριών των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών προσαρτάται στην παρούσα απόφαση και αποτελεί αναπόσπαστο τμήμα αυτής.

**Ο ΓΕΝΙΚΟΣ ΓΡΑΜΜΑΤΕΑΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΤΑΧΥΔΡΟΜΕΙΩΝ**

**Δρ. ΑΘΑΝΑΣΙΟΣ ΣΤΑΒΕΡΗΣ – ΠΟΛΥΚΑΛΑΣ**

**Εσωτερική διανομή:**
1. Γραφείο Υπουργού Επικρατείας
2. Γενική Διεύθυνση Κυβερνοασφάλειας
3. Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας

# ΟΔΗΓΙΕΣ

## ΓΕΝΙΚΑ

Ο παρών Οδηγός αποτελεί ένα μηχανισμό με τον οποίο οι Οργανισμοί μπορούν να διενεργήσουν αυτοαξιολόγηση του επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών τους. Ο Οδηγός περιέχει συνολικά 234 σημεία ελέγχου χωρισμένα σε 19 θεματικές ενότητες, οι οποίες είναι οι εξής:

1. Διοίκηση κυβερνοασφάλειας και διαχείριση επικινδυνότητας
2. Καταγραφή υλικού και λογισμικού
3. Ασφαλής παραμετροποίηση εξοπλισμού και εφαρμογών
4. Έλεγχος εκτέλεσης προγραμμάτων και υπηρεσιών
5. Διαχείριση λογαριασμών και έλεγχος πρόσβασης
6. Αυθεντικοποίηση χρηστών
7. Ασφάλεια δικτύων
8. Προστασία από κακόβουλο λογισμικό
9. Τήρηση και ανάλυση αρχείων καταγραφής συμβάντων (event logs)
10. Ασφάλεια διαδικτυακών εφαρμογών
11. Απομακρυσμένη εργασία
12. Χρήση κρυπτογραφίας
13. Εκπαίδευση και ευαισθητοποίηση σε θέματα κυβερνοασφάλειας
14. Διαχείριση κινδύνων στην εφοδιαστική αλυσίδα
15. Υλοποίηση τεχνικών ελέγχων κυβερνοασφάλειας
16. Μέτρα φυσικής ασφάλειας εγκαταστάσεων
17. Λήψη αντιγράφων ασφαλείας (backup)
18. Αντιμετώπιση περιστατικών κυβερνοασφάλειας
19. Διασφάλιση επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή

Ο Οδηγός απευθύνεται κυρίως σε δημόσιους και ιδιωτικούς Οργανισμούς που αποτελούν σημαντικές και κρίσιμες υποδομές για τη χώρα, όπως είναι οι φορείς εκμετάλλευσης βασικών υπηρεσιών καθώς και κρατικοί φορείς (Υπουργεία, Ανεξάρτητες Αρχές, Βουλή των Ελλήνων, Προεδρία της Δημοκρατίας). Ζητούμενο για τους εν λόγω Οργανισμούς είναι η επίτευξη ενός υψηλού επιπέδου κυβερνοασφάλειας, προκειμένου τα συστήματα δικτύου και πληροφοριών τους να προστατεύονται επαρκώς από τις συνεχώς εξελισσόμενες κυβερνοαπειλές, να αποκτήσουν την ικανότητα να ανταποκρίνονται έγκαιρα σε περιστατικά κυβερνοεπιθέσεων και να ανακτούν άμεσα τη λειτουργικότητα και τη συνέχιση της παροχής των υπηρεσιών τους.

Με τον Οδηγό αυτοαξιολόγησης ολοκληρώνεται η Δράση «Ανάπτυξη πλαισίου προαγωγής της αριστείας στον τομέα της κυβερνοασφάλειας (cybersecurity excellence management framework)» της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020-2025. Η Δράση ολοκληρώθηκε εξ ολοκλήρου in-house από την Εθνική Αρχή Κυβερνοασφάλειας - Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας και περιλαμβάνει τον Οδηγό αυτοαξιολόγησης καθώς και το Εγχειρίδιο Κυβερνοασφάλειας (Cybersecurity Handbook). Ο Οδηγός αυτοαξιολόγησης και το Εγχειρίδιο Κυβερνοασφάλειας θα πρέπει να χρησιμοποιούνται από κοινού, καθώς τα σημεία ελέγχου του Οδηγού στηρίζονται σε πολύ μεγάλο βαθμό στα controls του Εγχειριδίου Κυβερνοασφάλειας.

Το Εγχειρίδιο Κυβερνοασφάλειας είναι διαθέσιμο για λήψη εδώ.

## ΟΔΗΓΙΕΣ ΧΡΗΣΗΣ

Βασικά χαρακτηριστικά του Οδηγού:

### 01. ΕΝΟΤΗΤΑ «ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΑΥ ΤΟΑΞΙΟΛΟΓΗΣΗΣ»

Αναπτύσσονται οι ερωτήσεις (σημεία ελέγχου) του Οδηγού. Συνολικά περιέχονται 234 σημεία ελέγχου χωρισμένα σε 19 θεματικές ενότητες. Κάθε απάντηση λαμβάνει συγκεκριμένους πόντους, οι οποίοι αθροίζονται προκειμένου να εξαχθεί η βαθμολογία (score) για κάθε θεματική ενότητα. Η αντιστοίχιση πόντων και απαντήσεων απεικονίζεται στον παρακάτω πίνακα:

| ΠΟΝΤΟΙ | ΑΠΑΝΤΗΣΗ |
|---|---|
| 0 | «Δεν απαντήθηκε», «Όχι», «Δεν υλοποιείται» |
| 1 | «Εν μέρει», «Υλοποιείται σε κάποια συστήματα», «Υλοποιείται σε κάποιες εφαρμογές» |
| 2 | «Σε μεγάλο βαθμό», «Υλοποιείται στα περισσότερα συστήματα», «Υλοποιείται στις περισσότερες εφαρμογές» |
| 3 | «Ναι», «Πλήρως», «Υλοποιείται σε όλα τα συστήματα», «Υλοποιείται σε όλες τις εφαρμογές» |

Ειδικά για τις ερωτήσεις που αφορούν πολιτικές ασφάλειας και διαδικασίες (συνολικά 20), η αντιστοίχιση πόντων και απαντήσεων έχει ως εξής:

| ΠΟΝΤΟΙ | ΑΠΑΝΤΗΣΗ |
|---|---|
| 0 | «Δεν απαντήθηκε», «Δεν υπάρχει πολιτική ασφάλειας» |
| 1 | «Η πολιτική ασφάλειας ασκείται εμπειρικά», «Πολιτική και διαδικασίες ασκούνται εμπειρικά» |
| 2 | «Υπάρχει μερικώς γραπτή πολιτική ασφάλειας», «Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες» |
| 3 | «Υπάρχει γραπτή πολιτική ασφάλειας», «Υπάρχει γραπτή πολιτική και διαδικασίες» |
| 4 | «Η πολιτική ασφάλειας είναι γραπτή και εγκεκριμένη», «Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες» |

Δεδομένου ότι δεν έχουν όλα τα σημεία ελέγχου την ίδια βαρύνουσα σημασία, η βαθμολογία για κάθε σημείο ελέγχου πολλαπλασιάζεται με συγκεκριμένο συντελεστή βαρύτητας και με αυτόν τον τρόπο προκύπτει το συνολικό score. Οι συντελεστές βαρύτητας είναι οι 1, 2 και 3.

Επίσης, δεξιά του score κάθε ερώτησης διατίθεται χώρος προκειμένου ο αυτοαξιολογούμενος φορέας να εισάγει παρατηρήσεις / σχόλια, εφόσον το επιθυμεί.

## 02. ΕΝΟΤΗΤΑ «ΑΠΟΤΕΛΕΣΜΑΤΑ»

Απεικονίζονται με γραφιστικό τρόπο τα αποτελέσματα, τα οποία εξάγονται ταυτόχρονα με την επιλογή κάθε απάντησης. Πιο συγκεκριμένα, υπάρχουν δύο είδη διαγραμμάτων:

**α)** Η βαθμολογία που έχει επιτευχθεί, ως ποσοστό επί % της μέγιστης βαθμολογίας, για κάθε θεματική ενότητα ξεχωριστά αλλά και στο σύνολο. Εδώ, απεικονίζονται επίσης η αντίστοιχη απομένουσα επικινδυνότητα που προκύπτει εάν αφαιρεθεί η βαθμολογία από την τιμή 100%, καθώς και η κατάσταση της επικινδυνότητας, η οποία και εκφράζεται στην κλίμακα Low Risk / Medium Risk / High Risk / Critical Risk. Ανάλογα με τη βαθμολογία που έχει επιτευχθεί, τα γραφήματα απεικονίζονται με διαφορετικό χρώμα ως εξής:

| ΒΑΘΜΟΛΟΓΙΑ | ΚΑΤΑΣΤΑΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ | ΧΡΩΜΑ ΓΡΑΦΗΜΑΤΟΣ |
|---|---|---|
| 76% - 100% | Low Risk | Μπλε |
| 51% - 75% | Medium Risk | Πράσινο |
| 26% - 50% | High Risk | Πορτοκαλί |
| 0% - 25% | Critical Risk | Κόκκινο |

**Τονίζουμε ότι το διάγραμμα της συνολικής βαθμολογίας (και επικινδυνότητας) είναι ενδεικτικό, καθώς το επίπεδο κυβερνοασφάλειας σε έναν Οργανισμό ισούται με το επίπεδο κυβερνοασφάλειας του πιο αδύναμου κρίκου (weakest link). Για το λόγο αυτό, οι Οργανισμοί οφείλουν να εφιστούν την προσοχή τους στα επί μέρους διαγράμματα, ανά θεματική ενότητα, προκειμένου να εντοπίσουν τις συγκεκριμένες ελλείψεις που πρέπει να διορθωθούν.**

**β)** Ο βαθμός ωριμότητας των πολιτικών ασφάλειας και διαδικασιών. Η ανάπτυξη γραπτών και εγκεκριμένων πολιτικών και διαδικασιών που διέπουν την κυβερνοασφάλεια, σε συνδυασμό με την τακτική αξιολόγησή τους, αποτελεί το θεμέλιο ενός ολοκληρωμένου συστήματος διαχείρισης ασφάλειας πληροφοριών και ταυτόχρονα έναν βασικό δείκτη ωριμότητας για την κυβερνοασφάλεια σε έναν Οργανισμό.

Εδώ, λαμβάνεται το score από τις συνολικά 20 ερωτήσεις του Οδηγού που αφορούν σε πολιτικές ασφάλειας και διαδικασίες και το αποτέλεσμα απεικονίζεται ως ποσοστό επί % της μέγιστης βαθμολογίας στις συγκεκριμένες ερωτήσεις.

## ΟΙ ΚΥΡΙΟΙ ΣΤΟΧΟΙ ΤΟΥ ΟΔΗΓΟΥ ΑΥΤΟΑΞΙΟΛΟΓΗΣΗΣ ΕΙΝΑΙ:

**α)** Να παρέχει ένα πρακτικό μέσο μέτρησης του επιπέδου κυβερνοασφάλειας ενός Οργανισμού σε συγκεκριμένα βασικά θεματικά πεδία.

**β)** Να αποτελέσει χρήσιμο βοήθημα για τους Οργανισμούς στο να εντοπίσουν τις ελλείψεις εκείνες που αυξάνουν σημαντικά το βαθμό επικινδυνότητας για τα πληροφοριακά τους συστήματα, προκειμένου να προβούν στην επιλογή των κατάλληλων τεχνικών και οργανωτικών μέτρων που θα ενδυναμώσουν το επίπεδο κυβερνοασφάλειας.

**γ)** Να αποτελέσει απαραίτητο εργαλείο για την εισήγηση και λήψη αποφάσεων (evidence-based decision making) σε σχέση με την κυβερνοασφάλεια.

# ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΑΥΤΟΑΞΙΟΛΟΓΗΣΗΣ

| 1. ΔΙΟΙΚΗΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 1.1 | Ο Οργανισμός διαθέτει διακριτή οργανική μονάδα αρμόδια για την ασφάλεια των πληροφοριακών συστημάτων. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 1.2 | Ο Οργανισμός έχει ορίσει στέλεχός του ως υπεύθυνο ασφάλειας πληροφοριακών συστημάτων (chief information security officer - CISO), με βασικές αρμοδιότητες την παροχή στρατηγικού επιπέδου οδηγιών για θέματα κυβερνοασφάλειας, την επίβλεψη και παρακολούθηση του συστήματος διαχείρισης ασφάλειας πληροφοριών, τη διασφάλιση της συμμόρφωσης του Οργανισμού με τις αντίστοιχες νομοθετικές και κανονιστικές ρυθμίσεις και το συντονισμό των στόχων της κυβερνοασφάλειας με τους επιχειρησιακούς στόχους του Οργανισμού. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 1.3 | Ο Οργανισμός παρέχει στον CISO όλους τους απαραίτητους υλικοτεχνικούς, οικονομικούς και ανθρώπινους πόρους για την άσκηση των καθηκόντων του, καθώς και πόρους απαραίτητους για τη διατήρηση της εμπειρογνωσίας του. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 1.4 | Ο Οργανισμός έχει ορίσει πρόσωπο ως υπεύθυνο προστασίας δεδομένων (data protection officer), με σκοπό την εξασφάλιση επαρκούς προστασίας της ιδιωτικότητας και τη συμμόρφωση του Οργανισμού με τη νομοθεσία περί προστασίας δεδομένων προσωπικού χαρακτήρα. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |
| 1.5 | Ο Οργανισμός έχει εγκαθιδρύσει με ξεκάθαρο τρόπο ρόλους και ευθύνες όσον αφορά στην κυβερνοασφάλεια για το σύνολο του προσωπικού, καθώς και για τους προμηθευτές και παρόχους υπηρεσιών. Οι ρόλοι και ευθύνες αναθεωρούνται περιοδικά με σκοπό τη διασφάλιση της καταλληλότητάς τους. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 1.6 | Ο Οργανισμός δεσμεύει ποσό στον ετήσιο προϋπολογισμό του που αφορά αποκλειστικά στη διαχείριση και υλοποίηση έργων κυβερνοασφάλειας. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |

| 1. ΔΙΟΙΚΗΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 1.7 | Η οργανωτική προσέγγιση και διαχείριση των ζητημάτων κυβερνοασφάλειας υποστηρίζεται και καθοδηγείται ενεργά από το ανώτατο επίπεδο ηγεσίας του Οργανισμού. Οι αποφάσεις που λαμβάνονται κοινοποιούνται με αποτελεσματικό τρόπο σε στελέχη και υπηρεσιακές δομές με τους κατάλληλους ρόλους και αρμοδιότητες για πρακτική εφαρμογή. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 1.8 | Ο Οργανισμός έχει εκπονήσει καταγεγραμμένη και εγκεκριμένη πολιτική ασφάλειας, η οποία περιγράφει τη διαχειριστική του προσέγγιση ως προς την ασφάλεια των συστημάτων δικτύου και πληροφοριών. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική ασφάλειας<br>Η πολιτική ασφάλειας ασκείται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική ασφάλειας<br>Υπάρχει γραπτή πολιτική ασφάλειας<br>Η πολιτική ασφάλειας είναι γραπτή και εγκεκριμένη | 3 | 0 | |
| 1.9 | Η πολιτική ασφάλειας του Οργανισμού έχει λάβει την έγκριση της ανώτατης διοίκησης. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 1.10 | Η πολιτική ασφάλειας του Οργανισμού παραπέμπει και σε άλλες πολιτικές και διαδικασίες, οι οποίες εξειδικεύουν σε θεματικά πεδία τον τρόπο εφαρμογής τεχνικών και οργανωτικών μέτρων προστασίας. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 1.11 | Ο Οργανισμός αναθεωρεί τις πολιτικές ασφάλειας σε περιοδική βάση ή όταν συμβούν σημαντικές αλλαγές στο οργανωσιακό, επιχειρησιακό, τεχνικό και νομικό περιβάλλον του Οργανισμού. Οι αναθεωρημένες πολιτικές λαμβάνουν την έγκριση της ανώτατης διοίκησης. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 1.12 | Οι διαδικασίες που εξειδικεύουν θεματικά τα ζητήματα κυβερνοασφάλειας αναθεωρούνται σε περιοδική βάση ή όταν συμβούν σημαντικές αλλαγές στο οργανωσιακό, επιχειρησιακό, τεχνικό και νομικό περιβάλλον του Οργανισμού. Οι αναθεωρημένες διαδικασίες λαμβάνουν την έγκριση οργανικής μονάδας ή ειδικής ομάδας σε ιεραρχικό επίπεδο ανάλογο με την κρισιμότητά τους. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |

| 1. ΔΙΟΙΚΗΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 1.13 | Οι πολιτικές και διαδικασίες που σχετίζονται με την κυβερνοασφάλεια ενσωματώνονται αρμονικά με τις υπόλοιπες οργανωσιακές και επιχειρησιακές διαδικασίες του Οργανισμού. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 1.14 | Ο Οργανισμός υλοποιεί διαδικασίες αποτίμησης επικινδυνότητας (risk assessment), με τις οποίες εντοπίζονται, αναλύονται, αξιολογούνται και διαχειρίζονται οι κίνδυνοι για τα συστήματα δικτύου και επικοινωνιών. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 1.15 | Η αποτίμηση επικινδυνότητας διενεργείται όταν λάβουν χώρα σημαντικές αλλαγές που περιλαμβάνουν: α) τεχνικές αλλαγές στα συστήματα που υποστηρίζουν την παροχή κρίσιμων υπηρεσιών του Οργανισμού, β) αλλαγές στο περιβάλλον κυβερνοαπειλών. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 1.16 | Ο Οργανισμός υλοποιεί διαδικασίες αποτίμησης επικινδυνότητας (risk assessment) εφαρμόζοντας διεθνώς αποδεκτές μεθοδολογίες, το αποτέλεσμα των οποίων συνιστά ένα ολοκληρωμένο σύνολο τεκμηριωμένων απαιτήσεων και μέτρων ασφάλειας με σκοπό την επαρκή αντιμετώπιση των κινδύνων. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 1.17 | Τα αποτελέσματα και συμπεράσματα της αποτίμησης επικινδυνότητας επικοινωνούνται σε εύλογο χρονικό διάστημα σε πρόσωπα με ρόλους λήψης αποφάσεων και αντίστοιχης ευθύνης και λογοδοσίας. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 1.18 | Ο Οργανισμός αξιολογεί περιοδικά την αποτελεσματικότητα των διαδικασιών αποτίμησης επικινδυνότητας και εφαρμόζει βελτιώσεις στα σημεία που απαιτείται. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 1.19 | Ο Οργανισμός έχει αναπτύξει βασικούς δείκτες απόδοσης (key performance indicators), με τους οποίους αξιολογεί όλες τις πολιτικές και διαδικασίες που σχετίζονται με την κυβερνοασφάλεια. Τα αποτελέσματα της αξιολόγησης κοινοποιούνται στην ανώτατη διοίκηση. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 1.20 | Ο Οργανισμός υλοποιεί πρόγραμμα συλλογής γνώσης για κυβερνοαπειλές (cyber threat intelligence program), με σκοπό τη διαμόρφωση επαρκούς αντίληψης για τους μηχανισμούς, τους δείκτες και τη συμπεριφορά υπαρχόντων και αναδυόμενων απειλών στον κυβερνοχώρο. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |

| 1. ΔΙΟΙΚΗΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 1.21 | Ο Οργανισμός έχει πιστοποιηθεί ότι υλοποιεί ένα ολοκληρωμένο σύστημα διαχείρισης ασφάλειας πληροφοριών (information security management system), με σκοπό την επαρκή προστασία της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων του. Παραδείγματα αποτελούν τα ISO 27001, PCI DSS, NIST Cyber security framework, ISA/IEC 62443 κ.α. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |

| 2. ΚΑΤΑΓΡΑΦΗ ΥΛΙΚΟΥ ΚΑΙ ΛΟΓΙΣΜΙΚΟΥ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 2.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στην καταγραφή και ορθή χρήση του υλικού εξοπλισμού πληροφορικής, συστημάτων, εφαρμογών και δεδομένων. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική ασφάλειας<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 2.2 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στην ορθή χρήση των κινητών συσκευών (laptops, tablets, smartphones), καθώς και των μεταφερόμενων μέσων αποθήκευσης (usb, εξωτερικών σκληρών δίσκων, cd, dvd). | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική ασφάλειας<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |

| 2. ΚΑΤΑΓΡΑΦΗ ΥΛΙΚΟΥ ΚΑΙ ΛΟΓΙΣΜΙΚΟΥ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 2.3 | Ο Οργανισμός τηρεί ακριβή και επικαιροποιημένο κατάλογο (asset inventory) με όλα τα αγαθά πληροφορικής (υλικό και λογισμικό) που τηρούνται στις φυσικές υποδομές του, καθώς και τις εφαρμογές που φιλοξενούνται σε cloud περιβάλλοντα. Ο κατάλογος περιέχει λεπτομερή στοιχεία, όπως όνομα, ιδιοκτήτης, IP διεύθυνση (εάν είναι static), MAC διεύθυνση, έκδοση, περιγραφή λειτουργίας, τοποθεσία κ.λπ. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 2.4 | Ο Οργανισμός έχει ορίσει έναν ιδιοκτήτη (owner) για κάθε αγαθό πληροφορικής, με σκοπό να υπάρχει ευθύνη και λογοδοσία καθ' όλη τη διάρκεια του κύκλου ζωής του αγαθού. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 2.5 | Ο Οργανισμός έχει ταξινομήσει τα αγαθά πληροφορικής (υλικό, λογισμικό, δεδομένα) σε διακριτές ομάδες ανάλογα με την κρισιμότητα και ευαισθησία τους για τις επιχειρησιακές λειτουργίες του. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 2.6 | Ο Οργανισμός έχει αναγνωρίσει τα ευαίσθητα δεδομένα που επεξεργάζεται, σύμφωνα με τη νομοθεσία περί προστασίας δεδομένων προσωπικού χαρακτήρα, καθώς και τα κρίσιμα επιχειρησιακά δεδομένα, σύμφωνα με τις κανονιστικές απαιτήσεις και τις επιχειρησιακές ανάγκες του. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 2.7 | Ο Οργανισμός υλοποιεί διαδικασία ασφαλούς απόσυρσης σταθερών και μεταφερόμενων συσκευών, μέσω της οποίας επιβεβαιώνεται η διαγραφή κρίσιμων και προσωπικών δεδομένων από τις συσκευές πριν την απόσυρση. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |
| 2.8 | Ο Οργανισμός διασφαλίζει ότι οι ιδιόκτητες κινητές συσκευές (laptops, tablets, smartphones) που οι εργαζόμενοι φέρουν στο χώρο εργασίας ("bring your own device") δεν έχουν δυνατότητα πρόσβασης σε κρίσιμα ή ευαίσθητα συστήματα του Οργανισμού. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 2.9 | Ο Οργανισμός διασφαλίζει ότι εάν οι ιδιόκτητες κινητές συσκευές (laptops, tablets, smartphones) που οι εργαζόμενοι φέρουν στο χώρο εργασίας ("bring your own device") αποκτήσουν πρόσβαση στο Internet, αυτό γίνεται μόνο μέσω δικτύου που είναι διαχωρισμένο από το υπόλοιπο δίκτυο του Οργανισμού. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 2.10 | Ο Οργανισμός διασφαλίζει ότι εφόσον οι ιδιόκτητες κινητές συσκευές (laptops, tablets, smartphones) που οι εργαζόμενοι φέρουν στο χώρο εργασίας ("bring your own device") αποκτήσουν πρόσβαση σε κρίσιμα ή ευαίσθητα δεδομένα, τότε ελέγχονται και διαμορφώνονται με τα κατάλληλα μέτρα προστασίας από τις τεχνικές υπηρεσίες του Οργανισμού. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |

| 2. ΚΑΤΑΓΡΑΦΗ ΥΛΙΚΟΥ ΚΑΙ ΛΟΓΙΣΜΙΚΟΥ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 2.11 | Ο Οργανισμός χρησιμοποιεί εργαλείο που προγραμματισμένα σαρώνει το δίκτυό του και εντοπίζει τις συσκευές που είναι συνδεδεμένες σε αυτό, μαζί με τα χαρακτηριστικά τους, με σκοπό την τακτική επικαιροποίηση του καταλόγου και τον εντοπισμό τυχόν μη εξουσιοδοτημένων συσκευών. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |

| 3. ΑΣΦΑΛΗΣ ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ ΕΞΟΠΛΙΣΜΟΥ ΚΑΙ ΕΦΑΡΜΟΓΩΝ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 3.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στην ασφαλή παραμετροποίηση εξοπλισμού, λειτουργικών συστημάτων και εφαρμογών. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική ασφάλειας<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 3.2 | Ο Οργανισμός εφαρμόζει εγκεκριμένη διαδικασία ασφαλούς παραμετροποίησης (secure configuration process), με βάση διεθνώς αποδεκτά πρότυπα και οδηγίες, για τα λειτουργικά συστήματα των σταθμών εργασίας, των servers και των δικτυακών συσκευών, προσαρμοσμένες στην πολιτική ασφάλειας του Οργανισμού. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήματα<br>Υλοποιείται σε όλα τα συστήματα | 3 | 0 | |

| 3. ΑΣΦΑΛΗΣ ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ ΕΞΟΠΛΙΣΜΟΥ ΚΑΙ ΕΦΑΡΜΟΓΩΝ | | | | | |
|---|---|---|---|---|---|
| Α/Α | ΕΡΩΤΗΜΑΤΑ | ΑΠΑΝΤΗΣΕΙΣ | ΒΑΡΥΤΗΤΑ | SCORE | ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ |
| 3.3 | Ο Οργανισμός χρησιμοποιεί μόνο υποστηριζόμενες εκδόσεις για τα λειτουργικά συστήματα των σταθμών εργασίας, των servers και των δικτυακών συσκευών. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήματα<br>Υλοποιείται σε όλα τα συστήματα | 3 | 0 | |
| 3.4 | Ο Οργανισμός υλοποιεί εγκεκριμένη διαδικασία απόσυρσης εξοπλισμού, λειτουργικών συστημάτων και εφαρμογών για τα οποία έχει λήξει η υποστήριξη από τον κατασκευαστή ή πάροχο. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήματα<br>Υλοποιείται σε όλα τα συστήματα | 1 | 0 | |
| 3.5 | Ο Οργανισμός κάνει λήψη των ενημερώσεων ασφάλειας και των αναβαθμίσεων λογισμικού για τα λειτουργικά συστήματα των σταθμών εργασίας, των servers και των δικτυακών συσκευών με αυτοματοποιημένο τρόπο, κατ' ελάχιστο σε μηνιαία βάση. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήματα<br>Υλοποιείται σε όλα τα συστήματα | 3 | 0 | |
| 3.6 | Ο Οργανισμός κάνει λήψη των ενημερώσεων ασφάλειας και των αναβαθμίσεων λογισμικού για τις επιχειρησιακές εφαρμογές του με αυτοματοποιημένο τρόπο, κατ' ελάχιστο σε μηνιαία βάση. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 3 | 0 | |

| 3. ΑΣΦΑΛΗΣ ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ ΕΞΟΠΛΙΣΜΟΥ ΚΑΙ ΕΦΑΡΜΟΓΩΝ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 3.7 | Ο Οργανισμός χρησιμοποιεί μόνο τις τελευταίες και ενημερωμένες εκδόσεις για σημαντικές client εφαρμογές, όπως είναι λογισμικό γραφείου, αναγνώστες pdf, web browsers και browser plugins, καθώς και email clients. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 3 | 0 | |
| 3.8 | Ο Οργανισμός χρησιμοποιεί μόνο τις τελευταίες και ενημερωμένες εκδόσεις για κάθε server εφαρμογή του που είναι προσβάσιμη από το Internet. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήματα<br>Υλοποιείται σε όλα τα συστήματα | 3 | 0 | |
| 3.9 | Ο Οργανισμός υλοποιεί firewall ως εφαρμογή σε κάθε σταθμό εργασίας και server (host-based), το οποίο έχει ρυθμιστεί να εμποδίζει κάθε δικτυακή σύνδεση από και προς τη συσκευή με εξαίρεση τις θύρες και υπηρεσίες που απαιτούνται με βάση τις επιχειρησιακές ανάγκες. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήματα<br>Υλοποιείται σε όλα τα συστήματα | 3 | 0 | |
| 3.10 | Ο Οργανισμός υλοποιεί τις παρακάτω ρυθμίσεις στις δικτυακές συσκευές: | | | | |
| 3.10.1 | • Έχει απενεργοποιηθεί κάθε περιττή υπηρεσία (service). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 3.10.2 | • Στα switches έχει ενεργοποιηθεί η λειτουργία "port security". | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 3.10.3 | • Στους δρομολογητές (routers) έχουν απενεργοποιηθεί τα interfaces και τα πρωτόκολλα δρομολόγησης που δεν χρησιμοποιούνται. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |

| 3. ΑΣΦΑΛΗΣ ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ ΕΞΟΠΛΙΣΜΟΥ ΚΑΙ ΕΦΑΡΜΟΓΩΝ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 3.10.4 | • Στα switches έχουν απενεργοποιηθεί οι θύρες που δεν χρησιμοποιούνται. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 3.10.5 | • Εφαρμόζεται αυθεντικοποίηση δύο παραγόντων (2-factor authentication) για την πρόσβαση στο διαχειριστικό περιβάλλον όλων των κρίσιμων δικτυακών συσκευών. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 3.11 | Ο Οργανισμός διασφαλίζει ότι σε όσα συστήματα έχουν ταξινομηθεί ως κρίσιμα δεν είναι εφικτή η σύνδεση φορητών μέσων αποθήκευσης (USB, εξωτερικών σκληρών δίσκων, CD, DVD), εάν δεν υπάρχει γι' αυτό αυστηρή επιχειρησιακή ανάγκη. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 3.12 | Ο Οργανισμός διασφαλίζει ότι τα προεπιλεγμένα συνθηματικά (default passwords) σε κάθε νέο προϊόν τροποποιούνται κατά την πρώτη εγκατάσταση του προϊόντος. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήματα<br>Υλοποιείται σε όλα τα συστήματα | 2 | 0 | |
| 3.13 | Ο Οργανισμός τηρεί πλήρη αντίγραφα ασφαλείας (system images) των λειτουργικών συστημάτων του, με τις βασικές ρυθμίσεις ασφάλειας, σε κρυπτογραφημένη μορφή, με περιορισμούς στην πρόσβαση και με έλεγχο ακεραιότητας των αρχείων (file integrity monitoring). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |

| 4. ΕΛΕΓΧΟΣ ΕΚΤΕΛΕΣΗΣ ΠΡΟΓΡΑΜΜΑΤΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ | | | | | |
|---|---|---|---|---|---|
| Α/Α | ΕΡΩΤΗΜΑΤΑ | ΑΠΑΝΤΗΣΕΙΣ | ΒΑΡΥΤΗΤΑ | SCORE | ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ |
| 4.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στον έλεγχο εγκατάστασης και εκτέλεσης προγραμμάτων και υπηρεσιών στο δίκτυο και στα συστήματά του. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 4.2 | Ο Οργανισμός διασφαλίζει ότι στους servers και στους σταθμούς εργασίας λειτουργούν μόνο οι θύρες (ports), τα πρωτόκολλα και οι δικτυακές υπηρεσίες που είναι απαραίτητες για τη διεκπεραίωση των επιχειρησιακών λειτουργιών του. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 3 | 0 | |
| 4.3 | Ο Οργανισμός διασφαλίζει ότι αν υπάρξει επιχειρησιακή ανάγκη σε χρήστες με standard δικαιώματα (non-privileged) να εγκαταστήσουν λογισμικό, αυτό μπορεί να συμβεί μόνο με εγκεκριμένες εφαρμογές που αποθηκεύονται σε αποθετήρια λογισμικού που ελέγχονται από τον Οργανισμό. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 4.4 | Ο Οργανισμός έχει δημιουργήσει κατάλογο με εξουσιοδοτημένες εφαρμογές και συστατικά τους (βιβλιοθήκες, αρχεία διαμόρφωσης κ.α.) και έχει διασφαλίσει ότι μόνο αυτές θα επιτρέπεται να εκτελούνται στους servers και στους σταθμούς εργασίας (application whitelisting). | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 2 | 0 | |

| 4. ΕΛΕΓΧΟΣ ΕΚΤΕΛΕΣΗΣ ΠΡΟΓΡΑΜΜΑΤΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 4.5 | Ο Οργανισμός εφαρμόζει κατάλληλες τεχνικές, έτσι ώστε μόνο εγκεκριμένα scripts, δηλαδή συγκεκριμένα .ps1, .py κ.λπ. αρχεία να επιτρέπεται να εκτελούνται. Η εκτέλεση μη εγκεκριμένων scripts εμποδίζεται. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 2 | 0 | |
| 4.6 | Ο Οργανισμός διενεργεί σε τακτική βάση αυτοματοποιημένο port scanning στο σύνολο του δικτύου του Οργανισμού με σκοπό την ανίχνευση μη εξουσιοδοτημένων ανοικτών δικτυακών θυρών και υπηρεσιών σε συστήματα. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | | |
| 4.7 | Ο Οργανισμός διασφαλίζει ότι οι χρήστες με standard δικαιώματα (non-privileged) δεν μπορούν να απενεργοποιήσουν ή να τροποποιήσουν τις ρυθμίσεις ασφάλειας στο λειτουργικό τους σύστημα. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | | |
| 4.8 | Ο Οργανισμός έχει διασφαλίσει ότι σε περιβάλλον Microsoft Windows και σε λογαριασμούς χρηστών με standard δικαιώματα (non-privileged) οι μηχανές εκτέλεσης script κώδικα είναι απενεργοποιημένες. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | | |
| 4.9 | Ο Οργανισμός υλοποιεί κατάλληλες ρυθμίσεις στο firewall της εξωτερικής περιμέτρου του δικτύου, ώστε αυτό να εμποδίζει την εισερχόμενη από και εξερχόμενη προς το Internet επικοινωνία στις παρακάτω θύρες: TCP 445 (SMB), UDP 137 (NetBIOS Name Resolution), UDP 138 (NetBIOS Datagram Service) και TCP 139 (NetBIOS Session Service). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | | |
| 4.10 | Ο Οργανισμός υλοποιεί κατάλληλες ρυθμίσεις ώστε να εμποδίζονται οι εισερχόμενες SMB συνδέσεις στην TCP θύρα 445 σε όσους σταθμούς εργασίας και servers δεν φιλοξενούν κοινόχρηστο περιεχόμενο (shares). | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 2 | | |
| 4.11 | Ο Οργανισμός έχει απενεργοποιήσει τις εκδόσεις SMBv1 και v2 στο εσωτερικό δίκτυο και έχει αναβαθμίσει στην έκδοση v3 ή στην πλέον πρόσφατη. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | | |

| 5. ΔΙΑΧΕΙΡΙΣΗ ΛΟΓΑΡΙΑΣΜΩΝ ΚΑΙ ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ | | | | | |
|---|---|---|---|---|---|
| Α/Α | ΕΡΩΤΗΜΑΤΑ | ΑΠΑΝΤΗΣΕΙΣ | ΒΑΡΥΤΗΤΑ | SCORE | ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ |
| 5.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στη διαχείριση των λογαριασμών χρηστών και στον έλεγχο πρόσβασης στο δίκτυο, στα συστήματα, στις εφαρμογές και στα δεδομένα του. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 5.2 | Ο Οργανισμός έχει διασφαλίσει ότι το προσωπικό του Οργανισμού και οι εξωτερικοί συνεργάτες που αποκτούν λογαριασμό χρήστη αναγνωρίζονται (identified) με μοναδικό τρόπο, με σκοπό τη διασφάλιση λογοδοσίας (accountability). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 5.3 | Ο Οργανισμός εφαρμόζει αυτοματοποιημένη διαδικασία χορήγησης πρόσβασης στα αγαθά του με κάθε πρόσληψη νέου προσωπικού, χορήγησης δικαιωμάτων ή αλλαγής ρόλου σε χρήστες. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |
| 5.4 | Ο Οργανισμός εφαρμόζει αυτοματοποιημένη διαδικασία για την ανάκληση πρόσβασης στα αγαθά του, μέσω της άμεσης απενεργοποίησης λογαριασμών με κάθε διακοπή εργασίας υπαλλήλου, ανάκλησης δικαιωμάτων ή αλλαγής ρόλου σε χρήστες. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 5.5 | Ο Οργανισμός έχει απενεργοποιήσει τους προεπιλεγμένους (default) λογαριασμούς στα αγαθά και στο λογισμικό του, όπως είναι οι root, administrator ή και άλλοι προϋπάρχοντες εταιρικοί λογαριασμοί. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 3 | 0 | |
| 5.6 | Ο Οργανισμός τηρεί κατάλογο (inventory) με όλους τους λογαριασμούς χρηστών, ο οποίος περιέχει κατ' ελάχιστον το ονοματεπώνυμο, την ημερομηνία έναρξης / λήξης, τα προνόμια και την Υπηρεσία εργασίας του υπαλλήλου. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |

| 5. ΔΙΑΧΕΙΡΙΣΗ ΛΟΓΑΡΙΑΣΜΩΝ ΚΑΙ ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ | | | | | |
|---|---|---|---|---|---|
| Α/Α | ΕΡΩΤΗΜΑΤΑ | ΑΠΑΝΤΗΣΕΙΣ | ΒΑΡΥΤΗΤΑ | SCORE | ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ |
| 5.7 | Ο Οργανισμός τηρεί κατάλογο (inventory) με όλους τους λογαριασμούς υπηρεσιών (service accounts) που χρησιμοποιούνται. Ο κατάλογος θα πρέπει να περιέχει κατ' ελάχιστο τον ιδιοκτήτη (owner), το σκοπό και την ημερομηνία αναθεώρησης. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |
| 5.8 | Ο Οργανισμός απενεργοποιεί λογαριασμούς χρηστών ύστερα από συγκεκριμένο χρονικό διάστημα αδρανούς δραστηριότητας (π.χ. 3 μήνες). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |
| 5.9 | Ο Οργανισμός εκχωρεί δικαιώματα πρόσβασης με βάση διακριτούς ρόλους, έτσι ώστε οι χρήστες να έχουν πρόσβαση αποκλειστικά και μόνο στο είδος της πληροφορίας που είναι απαραίτητη για την εκτέλεση των εργασιακών καθηκόντων τους, με βάση τις αρχές των ελάχιστων προνομίων (least privilege) και της ανάγκης γνώσης (need to know). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 5.10 | Ο Οργανισμός διασφαλίζει ότι στους χρήστες που εκτελούν αποκλειστικά μη διαχειριστικές εργασίες καθημερινής ρουτίνας (π.χ. χρήση προγραμμάτων word, excel, adobe reader, ανάγνωση και αποστολή e-mail, περιήγηση στο Internet κ.λπ.) χορηγείται αποκλειστικά standard λογαριασμός απλού χρήστη (non-privileged account). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 5.11 | Ο Οργανισμός διασφαλίζει ότι στους χρήστες που λόγω καθηκόντων εκτελούν διαχειριστικές εργασίες χορηγείται λογαριασμός αυξημένων προνομίων που χρησιμοποιείται αποκλειστικά για τις εργασίες αυτές. Οι εν λόγω λογαριασμοί δεν έχουν πρόσβαση σε υπηρεσίες email και Internet. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 5.12 | Ο Οργανισμός διασφαλίζει ότι στους χρήστες που λόγω καθηκόντων έχουν λογαριασμό αυξημένων προνομίων (privileged account) χορηγείται δεύτερος standard λογαριασμός απλού χρήστη (non-privileged account) για την εκτέλεση μη διαχειριστικών εργασιών καθημερινής ρουτίνας (π.χ. χρήση προγραμμάτων word, excel, adobe reader, ανάγνωση και αποστολή e-mail, περιήγηση στο Internet κ.λπ.). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 5.13 | Ο Οργανισμός έχει υλοποιήσει κεντρική διαχείριση λογαριασμών μέσω υπηρεσίας καταλόγου (π.χ. Active directory service). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 5.14 | Ο Οργανισμός εφαρμόζει την τεχνική της «διπλής εξουσιοδότησης» ("dual authorization"), έτσι ώστε να απαιτείται η έγκριση δύο εξουσιοδοτημένων χρηστών για την εκτέλεση ιδιαίτερα κρίσιμων και ευαίσθητων εντολών ή λειτουργιών. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |

| 6. ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΧΡΗΣΤΩΝ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 6.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στην αυθεντικοποίηση των χρηστών, με σκοπό την αποφυγή μη εξουσιοδοτημένης πρόσβασης στα πληροφοριακά του συστήματα. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 6.2 | Ο Οργανισμός υλοποιεί μηχανισμούς αυθεντικοποίησης που επιβάλλουν τη δημιουργία ισχυρών κωδικών πρόσβασης για τα πληροφοριακά του συστήματα. Ως ισχυροί κωδικοί πρόσβασης θεωρούνται εκείνοι που έχουν μήκος τουλάχιστον δώδεκα (12) χαρακτήρων και περιέχουν σωρευτικά τουλάχιστον ένα (1) κεφαλαίο γράμμα, ένα (1) μικρό γράμμα, έναν (1) αριθμό και έναν (1) ειδικό χαρακτήρα και δεν περιέχουν ονόματα ή κοινές λέξεις που υπάρχουν σε λεξικά. Οι μηχανισμοί δημιουργίας ισχυρών κωδικών μπορεί να περιλαμβάνουν και τη δυνατότητα δημιουργίας φράσεων (passphrases). | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 6.3 | Ο Οργανισμός εφαρμόζει πολυπαραγοντική αυθεντικοποίηση (multi-factor authentication) για την πρόσβαση μέσω δικτύου σε όλους τους διαχειριστικούς λογαριασμούς, συμπεριλαμβανομένων και των λογαριασμών τρίτων παρόχων. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 6.4 | Ο Οργανισμός εφαρμόζει πολυπαραγοντική αυθεντικοποίηση (multi-factor authentication) για όλες τις απομακρυσμένες συνδέσεις (remote access connections) στο δίκτυό του. Η εν λόγω απαίτηση υλοποιείται για το σύνολο των υπαλλήλων του φορέα (σε μη προνομιούχους και σε διαχειριστικούς λογαριασμούς), καθώς και για τρίτα μέρη στα πλαίσια συμβατικής τους υποχρέωσης για παροχή υπηρεσιών υποστήριξης ή συντήρησης των συστημάτων του Οργανισμού. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 6.5 | Ο Οργανισμός εφαρμόζει πολυπαραγοντική αυθεντικοποίηση (multi-factor authentication) για κάθε χρήστη που επιθυμεί πρόσβαση σε κρίσιμα ή ευαίσθητα δεδομένα. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |

| 6. ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΧΡΗΣΤΩΝ | | | | | |
|---|---|---|---|---|---|
| Α/Α | ΕΡΩΤΗΜΑΤΑ | ΑΠΑΝΤΗΣΕΙΣ | ΒΑΡΥΤΗΤΑ | SCORE | ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ |
| 6.6 | Ο Οργανισμός έχει ορίσει μέγιστο όριο (τριών έως πέντε) συνεχόμενων ανεπιτυχών προσπαθειών για είσοδο (log in) σε λογαριασμό, πέραν των οποίων ο λογαριασμός θα κλειδώνει για ένα προκαθορισμένο χρονικό διάστημα. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 2 | 0 | |
| 6.7 | Ο Οργανισμός διασφαλίζει ότι οι κωδικοί πρόσβασης αποθηκεύονται σε κρυπτογραφημένη μορφή. Η κρυπτογράφηση γίνεται με τη χρήση one-way hash αλγορίθμων με την επιπλέον προσθήκη στον υπολογισμό μίας ακολουθίας τυχαίων δεδομένων (salt). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 6.8 | Ο Οργανισμός έχει ρυθμίσει στους σταθμούς εργασίας να ενεργοποιείται κλείδωμα της οθόνης μετά από μέγιστο χρονικό διάστημα 15 λεπτών αδράνειας του χρήστη, με σκοπό την αποφυγή μη εξουσιοδοτημένης πρόσβασης. Προκειμένου να ξεκλειδωθεί η οθόνη, απαιτείται η εκ νέου αυθεντικοποίηση του χρήστη. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |
| 6.9 | Ο Οργανισμός εφαρμόζει πολυπαραγοντική αυθεντικοποίηση (multi-factor authentication) με αποστολή one-time password με χρήση mobile εφαρμογής αντί για SMS. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |
| 6.10 | Ο Οργανισμός υλοποιεί υποδομή δημοσίου κλειδιού (public key infrastructure) για τη διενέργεια αυθεντικοποίησης χρηστών με τη χρήση ψηφιακού πιστοποιητικού. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |

| 7. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ | | | | | |
|---|---|---|---|---|---|
| Α/Α | ΕΡΩΤΗΜΑΤΑ | ΑΠΑΝΤΗΣΕΙΣ | ΒΑΡΥΤΗΤΑ | SCORE | ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ |
| 7.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στην ασφαλή αρχιτεκτονική των δικτύων του. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 7.2 | Ο Οργανισμός τηρεί επικαιροποιημένο διάγραμμα δικτύου και ροής δεδομένων (network and data flow diagram), στο οποίο απεικονίζονται όλες οι δικτυακές συνδέσεις, συμπεριλαμβανομένων των ασύρματων δικτύων, καθώς και οι ροές μετάδοσης των ευαίσθητων δεδομένων μεταξύ όλων των συστημάτων του Οργανισμού. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 7.3 | Ο Οργανισμός τηρεί σε προστατευμένο αρχείο όλους τους κανόνες δρομολόγησης, καθώς και τους κανόνες ελέγχου πρόσβασης (access control lists) των firewalls. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 7.4 | Οι servers του Οργανισμού που έχουν δημόσια IP διεύθυνση (π.χ. web servers, mail servers, VPN servers κ.λπ.) ανήκουν σε διακριτή δικτυακή ζώνη (υποδίκτυο) που είναι διαχωρισμένη με φυσικό ή λογικό τρόπο από το εσωτερικό δίκτυο του Οργανισμού. Η υλοποίηση αυτή ονομάζεται αποστρατικοποιημένη ζώνη (de-militirized zone - DMZ). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 7.5 | Ο Οργανισμός έχει εγκαταστήσει firewall στην εξωτερική περίμετρο του δικτύου, το οποίο επιτρέπει μόνο την εισερχόμενη και εξερχόμενη ροή της πληροφορίας (inbound και outbound traffic) που είναι απαραίτητη για την εκτέλεση των επιχειρησιακών λειτουργιών του. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 7.6 | Ο Οργανισμός έχει διαχωρίσει το εσωτερικό του δίκτυο σε διακριτά υποδίκτυα με βάση το επίπεδο ευαισθησίας των επιχειρησιακών τομέων του (network segmentation). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |

| 7. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ | | | | | |
|---|---|---|---|---|---|
| Α/Α | ΕΡΩΤΗΜΑΤΑ | ΑΠΑΝΤΗΣΕΙΣ | ΒΑΡΥΤΗΤΑ | SCORE | ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ |
| 7.7 | Ο Οργανισμός εφαρμόζει φιλτράρισμα της δικτυακής κίνησης (traffic filtering) μεταξύ των υποδικτύων με σκοπό να περιορίσει τη ροή της πληροφορίας στην απολύτως απαραίτητη για τις επιχειρησιακές ανάγκες του. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 7.8 | Ο Οργανισμός διασφαλίζει ότι η απομακρυσμένη πρόσβαση χρηστών στο εσωτερικό δίκτυό του γίνεται μέσω VPN (Virtual Private Network), με χρήση αυθεντικοποίησης δύο παραγόντων (2-factor authentication) και των πιο πρόσφατων αλγόριθμων κρυπτογράφησης. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 7.9 | Ο Οργανισμός υλοποιεί firewall επιπέδου εφαρμογής (application firewall) μπροστά από κάθε κρίσιμης σημασίας server, με σκοπό τον αποκλεισμό της κακόβουλης κίνησης. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 3 | 0 | |
| 7.10 | Ο Οργανισμός υλοποιεί δικτυακά συστήματα ανίχνευσης και πρόληψης εισβολών (network intrusion detection / prevention systems), με σκοπό την ανίχνευση και πρόληψη επιθέσεων σε κάθε υποδίκτυο του Οργανισμού. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 7.11 | Ο Οργανισμός έχει κατανοήσει τους τρόπους με τους οποίους η υπηρεσία που παρέχει μπορεί να υπερφορτωθεί, καθώς και τα όρια (σε bandwidth, επεξεργαστική ισχύ και αποθηκευτικό χώρο) πέρα από τα οποία η διαθεσιμότητα της υπηρεσίας κινδυνεύει με διακοπή. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 7.12 | Ο Οργανισμός εφαρμόζει τη χρήση του domain registrar locking, προκειμένου να εμποδίσει συμβάν άρνησης παροχής υπηρεσιών λόγω μη εξουσιοδοτημένης διαγραφής, μεταφοράς ή αλλοίωσης της εγγραφής του domain του. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 7.13 | Ο Οργανισμός έχει διασφαλίσει ότι η υποδομή του διαθέτει πλεονασμό σε πόρους που της επιτρέπουν να ανθίσταται σε επίθεση άρνησης παροχής υπηρεσιών. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |

| 7. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ | | | | | |
|---|---|---|---|---|---|
| Α/Α | ΕΡΩΤΗΜΑΤΑ | ΑΠΑΝΤΗΣΕΙΣ | ΒΑΡΥΤΗΤΑ | SCORE | ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ |
| 7.14 | Ο Οργανισμός έχει διαχωρίσει δικτυακά τις κρίσιμες υπηρεσίες του από άλλες υπηρεσίες που είναι πιθανότερο να στοχοποιηθούν (π.χ. web υπηρεσίες). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 7.15 | Ο Οργανισμός υλοποιεί συστήματα παρακολούθησης της διαθεσιμότητας των κρίσιμων υπηρεσιών του, που ανιχνεύουν επιθέσεις άρνησης παροχής υπηρεσιών και στέλνουν ειδοποίηση σε πραγματικό χρόνο. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 7.16 | Ο Οργανισμός έχει αναθέσει σε ειδικευμένο πάροχο cloud υπηρεσιών ασφάλειας (security as a service) την παροχή υπηρεσιών προστασίας των δημόσιας πρόσβασης εφαρμογών του από κατανεμημένες επιθέσεις άρνησης παροχής υπηρεσιών (distributed denial of service attacks). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 7.17 | Ο Οργανισμός έχει διασφαλίσει ότι τυχόν ασύρματα δίκτυα δημόσιας πρόσβασης που διαθέτει είναι διαχωρισμένα από το υπόλοιπο δίκτυό του. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 7.18 | Ο Οργανισμός υλοποιεί συστήματα δικτυακού ελέγχου πρόσβασης (network access control), με σκοπό τον αποκλεισμό της σύνδεσης μη εξουσιοδοτημένων συσκευών στο δίκτυό του. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 7.19 | Ο Οργανισμός υλοποιεί ασύρματο σύστημα ανίχνευσης εισβολών (wireless intrusion detection system - WIDS), με σκοπό την ανίχνευση μη εγκεκριμένων ασύρματων σημείων πρόσβασης (wireless access points) συνδεδεμένων στο δίκτυό του. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 7.20 | Ο Οργανισμός υλοποιεί δίοδο δεδομένων (data diode) σε μορφή hardware, το οποίο επιβάλλει τη ροή δεδομένων μόνο προς μία κατεύθυνση με σκοπό την προστασία κρίσιμης πληροφορίας σε υποδίκτυα υψηλών απαιτήσεων ασφάλειας. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |

| 8. ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ | | | | | |
|---|---|---|---|---|---|
| Α/Α | ΕΡΩΤΗΜΑΤΑ | ΑΠΑΝΤΗΣΕΙΣ | ΒΑΡΥΤΗΤΑ | SCORE | ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ |
| 8.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στην προστασία των πληροφοριακών συστημάτων του από μόλυνση με κακόβουλο λογισμικό. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 8.2 | Ο Οργανισμός εφαρμόζει λογισμικό προστασίας από κακόβουλα προγράμματα (anti-malware software) σε κάθε σταθμό εργασίας και server, το οποίο υλοποιείται μέσω κεντρικής διαχείρισης και ενημερώνεται σε τακτική βάση με αυτοματοποιημένο τρόπο. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 3 | 0 | |
| 8.3 | Ο Οργανισμός υλοποιεί την υπηρεσία DNS filtering, με σκοπό τον αποκλεισμό πρόσβασης σε γνωστά κακόβουλα domains. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 8.4 | Ο Οργανισμός έχει κατοχυρώσει domain names που είναι παραπλήσια με το domain name του, έτσι ώστε να αποτρέψει επιτιθέμενους από το να τα κατοχυρώσουν εκείνοι για κακόβουλο σκοπό. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |
| 8.5 | Ο Οργανισμός έχει διασφαλίσει ότι διενεργείται αυτόματα σάρωση για κακόβουλο λογισμικό (anti-malware scanning) σε φορητά μέσα αποθήκευσης (USB, εξωτερικούς σκληρούς δίσκους, CD, DVD), όταν αυτά συνδέονται σε συσκευές. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |

| 8. ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ | | | | | |
|---|---|---|---|---|---|
| Α/Α | ΕΡΩΤΗΜΑΤΑ | ΑΠΑΝΤΗΣΕΙΣ | ΒΑΡΥΤΗΤΑ | SCORE | ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ |
| 8.6 | Ο Οργανισμός υλοποιεί τεχνολογίες προστασίας από spam emails σε όλα τα σημεία εισόδου και εξόδου της υποδομής του (firewalls, email / web / proxy / remote access servers, σταθμούς εργασίας, laptops, κινητές συσκευές), με σκοπό τον αποκλεισμό κακόβουλου περιεχομένου. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 3 | 0 | |
| 8.7 | Ο Οργανισμός υλοποιεί και επιβάλλει δικτυακά URL filters, με σκοπό τον περιορισμό της δυνατότητας σύνδεσης σε ιστοσελίδες όχι εγκεκριμένες από την πολιτική ασφάλειας του Οργανισμού. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 8.8 | Ο Οργανισμός έχει διασφαλίσει ότι το σύνολο της δικτυακής κυκλοφορίας από και προς το διαδίκτυο περνά από αυθεντικοποιημένο διακομιστή μεσολάβησης επιπέδου εφαρμογής (application layer (web) proxy server), ο οποίος έχει ρυθμιστεί να απαγορεύει μη εξουσιοδοτημένες συνδέσεις και να μπλοκάρει κακόβουλο περιεχόμενο. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 8.9 | Ο Οργανισμός έχει διασφαλίσει ότι έχει απενεργοποιηθεί ή απεγκατασταθεί κάθε μη εγκεκριμένο plug-in ή add-on σε web browsers και e-mail clients. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 1 | 0 | |
| 8.10 | Ο Οργανισμός έχει υλοποιήσει σύστημα πρόληψης εισβολών στις τελικές συσκευές του (host-based intrusion prevention system). Παράδειγμα αποτελεί η χρήση εργαλείων EDR (Endpoint Detection and Response). | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 2 | 0 | |

| 9. ΤΗΡΗΣΗ ΚΑΙ ΑΝΑΛΥΣΗ ΑΡΧΕΙΩΝ ΚΑΤΑΓΡΑΦΗΣ ΣΥΜΒΑΝΤΩΝ (EVENT LOGS) | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 9.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στην καταγραφή, παρακολούθηση και ανάλυση συμβάντων στα πληροφοριακά του συστήματα. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 9.2 | Ο Οργανισμός έχει ενεργοποιήσει τη λειτουργία καταγραφής συμβάντων (event logs) σε όλους τους σταθμούς εργασίας, servers και δικτυακές συσκευές. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 3 | 0 | |
| 9.3 | Ο Οργανισμός έχει διασφαλίσει τον συγχρονισμό ανάμεσα στα ρολόγια όλων των συσκευών, έτσι ώστε να επιτυγχάνεται ακρίβεια στη συσχέτιση συμβάντων μεταξύ διαφορετικών συστημάτων. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 9.4 | Ο Οργανισμός έχει ενεργοποιήσει την καταγραφή επιτυχούς και ανεπιτυχούς εισόδου (login) και εξόδου (logout) για όλα τα συστήματα που απαιτούν αυθεντικοποίηση. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 2 | 0 | |
| 9.5 | Ο Οργανισμός έχει ενεργοποιήσει την καταγραφή όλων των δραστηριοτήτων που αφορούν σε διαχειριστικούς λογαριασμούς. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |

| 9. ΤΗΡΗΣΗ ΚΑΙ ΑΝΑΛΥΣΗ ΑΡΧΕΙΩΝ ΚΑΤΑΓΡΑΦΗΣ ΣΥΜΒΑΝΤΩΝ (EVENT LOGS) | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 9.6 | Ο Οργανισμός έχει διασφαλίσει ότι καταγράφονται τα παρακάτω συμβάντα: | | | | |
| 9.6.1 | • Πρόσβασης σε αρχεία και διεργασίες διακομιστών (servers). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 9.6.2 | • Αποτυχημένων προσπαθειών εκτέλεσης αρχείων. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 2 | 0 | |
| 9.6.3 | • Χρήσης και απόπειρας χρήσης ειδικών προνομίων. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 2 | 0 | |
| 9.6.4 | • Χρήσης των εφαρμογών συστήματος. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 2 | 0 | |
| 9.6.5 | • Αλλαγών σε λογαριασμούς και στην πολιτική ασφάλειας. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 2 | 0 | |

| 9. ΤΗΡΗΣΗ ΚΑΙ ΑΝΑΛΥΣΗ ΑΡΧΕΙΩΝ ΚΑΤΑΓΡΑΦΗΣ ΣΥΜΒΑΝΤΩΝ (EVENT LOGS) | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 9.6.6 | • Αιτημάτων HTTP και DNS. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 2 | 0 | |
| 9.6.7 | • Μεταφοράς δεδομένων από και προς φορητά μέσα αποθήκευσης. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 2 | 0 | |
| 9.7 | Ο Οργανισμός έχει ρυθμίσει τα αρχεία καταγραφής συμβάντων να περιλαμβάνουν λεπτομερή metadata όπως πηγή γεγονότος, ημερομηνία, χρήστης, χρονοσήμανση, IP διεύθυνση πηγής, IP διεύθυνση προορισμού κ.λπ. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 9.8 | Ο Οργανισμός έχει διασφαλίσει ότι τα αρχεία καταγραφής συμβάντων τηρούνται για χρονική περίοδο κατ' ελάχιστον ενός (1) έτους. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |
| 9.9 | Ο Οργανισμός έχει διασφαλίσει ότι τα αρχεία καταγραφής συμβάντων προστατεύονται επαρκώς από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση και διαγραφή. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 9.10 | Ο Οργανισμός έχει διασφαλίσει ότι η διαχείριση της λειτουργίας καταγραφής συμβάντων έχει ανατεθεί σε ένα υποσύνολο χρηστών με λογαριασμούς αυξημένων προνομίων. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |
| 9.11 | Ο Οργανισμός έχει εγκαταστήσει σύστημα ασφάλειας πληροφοριών και διαχείρισης συμβάντων (Security Information and Event Management - SIEM), με σκοπό τη συγκέντρωση των αρχείων καταγραφής συμβάντων σε κεντρικό σημείο και την ανάλυση και συσχέτισή τους για τον εντοπισμό ύποπτης δραστηριότητας. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |

| 10. ΑΣΦΑΛΕΙΑ ΔΙΑΔΙΚΤΥΑΚΩΝ ΕΦΑΡΜΟΓΩΝ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 10.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στην ασφάλεια των διαδικτυακών εφαρμογών του. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 10.2 | Ο Οργανισμός ορίζει τις απαιτήσεις ασφάλειας για κάθε εφαρμογή που πρόκειται να αναπτυχθεί, είτε in-house είτε outsourced. Οι απαιτήσεις ανταποκρίνονται στο βαθμό κρισιμότητας των λειτουργιών της εφαρμογής και της ευαισθησίας των δεδομένων που επεξεργάζεται. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 10.3 | Ο Οργανισμός διασφαλίζει ότι χρησιμοποιούνται αξιόπιστες και πλήρως ενημερωμένες πλατφόρμες ανάπτυξης εφαρμογών, καθώς και βιβλιοθήκες λογισμικού που προέρχονται από έμπιστες πηγές και συντηρούνται ενεργά. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 10.4 | Ο Οργανισμός διασφαλίζει ότι εφαρμόζονται τεχνικές ασφαλούς ανάπτυξης λογισμικού (secure development lifecycle) καθ' όλη τη διάρκεια του κύκλου ζωής των διαδικτυακών εφαρμογών του (σχεδιασμός, ανάπτυξη, δοκιμές, παραγωγική λειτουργία, συντήρηση), είτε αυτές έχουν αναπτυχθεί in-house είτε outscourced. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 10.5 | Ο Οργανισμός διασφαλίζει ότι κατά την ανάπτυξη διαδικτυακών εφαρμογών λαμβάνονται υπόψη κοινοί τύποι ευπαθειών, όπως είναι το OWASP Top-10. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 2 | 0 | |

| 10. ΑΣΦΑΛΕΙΑ ΔΙΑΔΙΚΤΥΑΚΩΝ ΕΦΑΡΜΟΓΩΝ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 10.6 | Ο Οργανισμός διασφαλίζει ότι κατά την ανάπτυξη διαδικτυακών εφαρμογών όλα τα δεδομένα εισόδου (πεδία φορμών HTML, αιτήματα REST, παράμετροι URL, κεφαλίδες (headers) HTTP, cookies, αρχεία batch, RSS feeds κ.α.) επικυρώνονται συντακτικά και σημασιολογικά (input validation) με τη χρήση white-list filtering στην πλευρά του server. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 2 | | |
| 10.7 | Ο Οργανισμός διασφαλίζει ότι κάθε επικοινωνία του web server (με browsers χρηστών, κλήσεις άλλων web υπηρεσιών, βάσεις δεδομένων, cloud κ.α.) υλοποιείται με κρυπτογράφηση της σύνδεσης με χρήση της πλέον πρόσφατης έκδοσης του πρωτοκόλλου TLS (encryption in transit). | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 3 | 0 | |
| 10.8 | Ο Οργανισμός διασφαλίζει ότι κατά την ανάπτυξη των εφαρμογών υλοποιούνται τεχνικές ελέγχου και διαχείρισης λαθών και εξαιρέσεων (errors and exceptions) για κάθε είδος εισερχόμενων δεδομένων, λαμβάνοντας υπόψη τον τύπο, το μέγεθος, τη μορφή και το αποδεκτό εύρος τιμών. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 2 | 0 | |
| 10.9 | Ο Οργανισμός διασφαλίζει ότι οι διαδικτυακές εφαρμογές του, ανεπτυγμένες είτε in-house είτε outsourced, υλοποιούν τα παρακάτω γνωρίσματα: | | | | |
| 10.9.1 | • Επιτρέπουν μόνο ισχυρούς κωδικούς πρόσβασης. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 3 | 0 | |

| 10. ΑΣΦΑΛΕΙΑ ΔΙΑΔΙΚΤΥΑΚΩΝ ΕΦΑΡΜΟΓΩΝ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 10.9.2 | • Εφαρμόζουν αυθεντικοποίηση δύο παραγόντων (2-factor authentication), όπου ορίζουν οι απαιτήσεις ασφάλειας της εφαρμογής. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 3 | 0 | |
| 10.9.3 | • Υλοποιούν την αρχή των ελάχιστων προνομίων (least privilege). | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 2 | 0 | |
| 10.9.4 | • Υλοποιούν τεχνικές παραμετροποίησης ερωτημάτων (query parameterization) σε κάθε στοιχείο που εισάγεται στο σύστημα διαχείρισης βάσεων δεδομένων της εφαρμογής. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 2 | 0 | |
| 10.9.5 | • Υλοποιούν τεχνικές κωδικοποίησης χαρακτήρων (output encoding και character escaping) ακριβώς πριν τα δεδομένα εισόδου εισέλθουν στο διερμηνευτή (interpreter) της εφαρμογής. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 2 | 0 | |

| 10. ΑΣΦΑΛΕΙΑ ΔΙΑΔΙΚΤΥΑΚΩΝ ΕΦΑΡΜΟΓΩΝ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 10.9.6 | • Οι κεφαλίδες απάντησης (response headers) του πρωτοκόλλου HTTP έχουν ρυθμιστεί ώστε να υλοποιούν τα Content-Security-Policy, HSTS και X-Frame-Options. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 2 | 0 | |
| 10.9.7 | • Σε κάθε αυθεντικοποίηση χρήστη η εφαρμογή δημιουργεί ένα νέο token συνόδου (session token) με τη χρήση εγκεκριμένων κρυπτογραφικών αλγορίθμων. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 2 | 0 | |
| 10.9.8 | • Κατά την αποσύνδεση του χρήστη (logout) και τη λήξη της συνόδου το token συνόδου ακυρώνεται, έτσι ώστε η χρήση του back button δεν επαναφέρει μία αυθεντικοποιημένη σύνοδο. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 2 | 0 | |
| 10.9.9 | • Τα δεδομένα της εφαρμογής που έχουν ταξινομηθεί ως κρίσιμα / ευαίσθητα αποθηκεύονται σε κρυπτογραφημένη μορφή (encryption at rest). | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 2 | 0 | |

| 10. ΑΣΦΑΛΕΙΑ ΔΙΑΔΙΚΤΥΑΚΩΝ ΕΦΑΡΜΟΓΩΝ | | | | | |
|---|---|---|---|---|---|
| Α/Α | ΕΡΩΤΗΜΑΤΑ | ΑΠΑΝΤΗΣΕΙΣ | ΒΑΡΥΤΗΤΑ | SCORE | ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ |
| 10.9.10 | • Τα tokens συνόδου που βασίζονται σε cookies έχουν ενεργοποιημένες τις ιδιότητες (attributes) "Secure", "HttpOnly", "SameSite" και το prefix "__Host-". | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 2 | 0 | |
| 10.10 | Ο Οργανισμός διασφαλίζει ότι διενεργείται έλεγχος ευπαθειών (vulnerability test) για κάθε νέα λειτουργικότητα που προστίθεται στην εφαρμογή κατά τα διαδοχικά στάδια ανάπτυξής της. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 2 | 0 | |
| 10.11 | Ο Οργανισμός διασφαλίζει ότι διενεργείται έλεγχος παρείσδυσης (penetration test) πριν η τελική έκδοση της εφαρμογής τεθεί σε παραγωγική λειτουργία. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 2 | 0 | |
| 10.12 | Ο Οργανισμός εφαρμόζει την τεχνική TLS inspection, με την οποία η διαδικτυακή κίνηση που μεταφέρεται μέσω HTTPS συνδέσεων αποκρυπτογραφείται και επιθεωρείται με σκοπό την ανίχνευση κακόβουλου περιεχομένου. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 10.13 | Ο Οργανισμός υλοποιεί firewall επιπέδου web εφαρμογής (web application firewall), είτε στην υποδομή του είτε ως ανατιθέμενη cloud υπηρεσία (security as a service), το οποίο ελέγχει την HTTP κίνηση προς τις διαδικτυακές εφαρμογές του για γνωστούς τύπους επιθέσεων. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποιες εφαρμογές<br>Υλοποιείται στις περισσότερες εφαρμογές<br>Υλοποιείται σε όλες τις εφαρμογές | 3 | 0 | |

| 11. ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΕΡΓΑΣΙΑ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 11.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στην υλοποίηση απομακρυσμένης εργασίας του προσωπικού με ασφαλή τρόπο. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 11.2 | Ο Οργανισμός διασφαλίζει ότι τα VPNs και firewalls διαθέτουν την τελευταία έκδοση λειτουργικών συστημάτων (up to date) και ότι λαμβάνουν ενημερώσεις ασφάλειας και αναβαθμίσεις λογισμικού σε τακτά χρονικά διαστήματα με αυτοματοποιημένο τρόπο. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 11.3 | Ο Οργανισμός διασφαλίζει ότι εφαρμόζεται αυθεντικοποίηση δύο παραγόντων (2-factor authentication), καθώς και ισχυροί κωδικοί πρόσβασης, για όλες τις VPN συνδέσεις προς το εσωτερικό δίκτυό του. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 11.4 | Ο Οργανισμός εφαρμόζει διεθνώς αποδεκτές ρυθμίσεις ασφάλειας για τη χρήση του πρωτοκόλλου RDP (Remote Desktop Protocol). | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 11.5 | Ο Οργανισμός έχει χορηγήσει φορητό υπολογιστή στους εργαζόμενους για τις ανάγκες της απομακρυσμένης εργασίας, ο οποίος έχει διαμορφωθεί κατάλληλα από τις υπηρεσίες πληροφορικής του Οργανισμού στο να πληροί τις απαιτούμενες ρυθμίσεις ασφάλειας. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 11.6 | Ο Οργανισμός έχει χορηγήσει στο προσωπικό που τηλεργάζεται κατάλληλες οδηγίες που αφορούν στην υλοποίηση βασικών παραμέτρων ασφάλειας για το οικιακό του δίκτυο, τον προσωπικό του υπολογιστή και την online συμπεριφορά του στο διαδίκτυο. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | | |

| 12. ΧΡΗΣΗ ΚΡΥΠΤΟΓΡΑΦΙΑΣ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 12.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στη χρήση της κρυπτογραφίας στα πληροφοριακά του συστήματα. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 12.2 | Ο Οργανισμός διασφαλίζει ότι τα δεδομένα που έχουν ταξινομηθεί ως κρίσιμα / ευαίσθητα κρυπτογραφούνται κατά τη μετάδοσή τους (encryption in transit). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 12.3 | Ο Οργανισμός διασφαλίζει ότι τα δεδομένα που έχουν ταξινομηθεί ως κρίσιμα / ευαίσθητα κρυπτογραφούνται κατά την αποθήκευσή τους (encryption at rest). Τα εν λόγω δεδομένα μπορεί να βρίσκονται σε διακομιστές, εφαρμογές και βάσεις δεδομένων. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 3 | 0 | |
| 12.4 | Ο Οργανισμός διασφαλίζει ότι κατά την κρυπτογράφηση χρησιμοποιούνται μόνο τελευταίες εκδόσεις εγκεκριμένων κρυπτογραφικών πρωτοκόλλων και λογισμικού, καθώς επίσης και το κατάλληλο μήκος κλειδιών. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 12.5 | Κατά τη χρήση της κρυπτογραφίας, ο Οργανισμός χρησιμοποιεί τους παρακάτω κρυπτογραφικούς αλγόριθμους: | | | | |
| 12.5.1 | • Για την υλοποίηση συμμετρικής κρυπτογράφησης χρησιμοποιείται ο αλγόριθμος AES, με μήκος κλειδιού 128, 192 ή 256 bits. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |

| 12. ΧΡΗΣΗ ΚΡΥΠΤΟΓΡΑΦΙΑΣ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 12.5.2 | • Για την υλοποίηση ψηφιακών υπογραφών χρησιμοποιείται ο αλγόριθμος RSA με μήκος κλειδιού τουλάχιστον 2048 bits ή ο αλγόριθμος ECDSA με μήκος κλειδιού τουλάχιστον 224 bits. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 12.5.3 | • Για την υλοποίηση αλγορίθμων κατακερματισμού (π.χ. ψηφιακές υπογραφές κ.α.) χρησιμοποιείται ο Secure Hash Algorithm 2 (SHA-2), με επιλογή μεταξύ των SHA-256, SHA-384 ή SHA-512. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 12.6 | Ο Οργανισμός υλοποιεί συνολική διαχείριση (δημιουργία, αποθήκευση, έλεγχος, διανομή) συμμετρικών και ασύμμετρων κλειδιών κρυπτογράφησης χρησιμοποιώντας διεθνώς αποδεκτά πρότυπα και διαδικασίες, συμπεριλαμβανομένων αυστηρών κανόνων πρόσβασης στην πλατφόρμα διαχείρισης. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |
| 12.7 | Ο Οργανισμός χρησιμοποιεί αυθεντικοποίηση δημοσίου κλειδιού (public key-based authentication) για την υλοποίηση SSH (Secure Shell) συνδέσεων. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 1 | 0 | |

| 13. ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΣΕ ΘΕΜΑΤΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 13.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στην εκπαίδευση και ευαισθητοποίηση του προσωπικού σε θέματα κυβερνοασφάλειας. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 13.2 | Ο Οργανισμός διενεργεί σε περιοδική βάση εκπαιδευτικό πρόγραμμα με σκοπό την ευαισθητοποίηση και ανάπτυξη δεξιοτήτων του προσωπικού σε θέματα κυβερνοασφάλειας.<br>Η ύλη των εκπαιδεύσεων περιλαμβάνει: | | | | |
| 13.2.1 | • Τους τρόπους αλληλεπίδρασης του χρήστη με τα συστήματα, το δίκτυο και τα δεδομένα του Οργανισμού με ασφαλή τρόπο. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 13.2.2 | • Τους τρόπους αναγνώρισης των επιθέσεων κοινωνικής μηχανικής, όπως είναι τα email εξαπάτησης (phishing), οι τηλεφωνικές κλήσεις πλαστοπροσωπίας κ.α. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 13.2.3 | • Τις καλές πρακτικές αυθεντικοποίησης, όπως είναι η δημιουργία ισχυρών κωδικών πρόσβασης και η πολυπαραγοντική αυθεντικοποίηση (multi-factor authentication). | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 13.2.4 | • Την αναγνώριση ενδείξεων παραβίασης συστημάτων και περιστατικών που προέρχονται από απειλές εκ των έσω (insider threats). | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |

| 13. ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΣΕ ΘΕΜΑΤΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 13.3 | Ο Οργανισμός διενεργεί σε περιοδική βάση εκπαιδευτικό πρόγραμμα ευαισθητοποίησης του προσωπικού για θέματα κυβερνοασφάλειας βασισμένο σε διακριτούς ρόλους και στοχευμένο σε διαφορετικές κατηγορίες εργαζομένων με βάση το επιχειρησιακό αντικείμενο και το επίπεδο τεχνικής εξειδίκευσης. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 13.4 | Ο Οργανισμός έχει διενεργήσει ανάλυση γνωσιακών κενών του προσωπικού (knowledge gap analysis), με σκοπό τη σύνταξη ενός πλάνου δημιουργίας διαδοχικών εκπαιδεύσεων. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 1 | 0 | |
| 13.5 | Ο Οργανισμός διενεργεί σε περιοδική βάση ασκήσεις προσομοίωσης περιστατικών κυβερνοασφάλειας και των επιπτώσεών τους, όπως π.χ. το άνοιγμα ενός κακόβουλου αρχείου συνημμένου σε email ή την επίσκεψη σε κακόβουλη ιστοσελίδα. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |

| 14. ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΣΤΗΝ ΕΦΟΔΙΑΣΤΙΚΗ ΑΛΥΣΙΔΑ (SUPPLY CHAIN RISK MANAGEMENT) | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 14.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στη διαχείριση κινδύνων στην εφοδιαστική του αλυσίδα, με σκοπό τη διασφάλιση της προστασίας των πληροφοριακών συστημάτων του από τη χρήση προϊόντων και υπηρεσιών πληροφορικής και επικοινωνιών από τρίτους προμηθευτές και παρόχους υπηρεσιών. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |

| 14. ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΣΤΗΝ ΕΦΟΔΙΑΣΤΙΚΗ ΑΛΥΣΙΔΑ (SUPPLY CHAIN RISK MANAGEMENT) | | | | | |
|---|---|---|---|---|---|
| Α/Α | ΕΡΩΤΗΜΑΤΑ | ΑΠΑΝΤΗΣΕΙΣ | ΒΑΡΥΤΗΤΑ | SCORE | ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ |
| 14.2 | Ο Οργανισμός διενεργεί σε περιοδική βάση ενδελεχή έρευνα και αξιολόγηση κινδύνων (supply chain risk management) για τους προμηθευτές και παρόχους υπηρεσιών πληροφορικής, συμπεριλαμβανομένων και των υπεργολάβων τους, λαμβάνοντας υπόψη παραμέτρους όπως εταιρικές συνεργασίες, ανταγωνιστές και χώρες προέλευσης, προκειμένου να συγκεντρώσει ολοκληρωμένη γνώση για την εφοδιαστική του αλυσίδα και το επίπεδο κινδύνων που αυτή αντιμετωπίζει. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 14.3 | Ο Οργανισμός διασφαλίζει ότι στις συμβάσεις παροχής υπηρεσιών πληροφορικής καταγράφεται με λεπτομέρεια το είδος των συστημάτων και δεδομένων στα οποία ο πάροχος αποκτά πρόσβαση κατά τη διάρκεια εκτέλεσης της σύμβασης. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 14.4 | Ο Οργανισμός έχει αναπτύξει και επικοινωνήσει ένα σύνολο ελάχιστων απαιτήσεων κυβερνοασφάλειας στους προμηθευτές και παρόχους υπηρεσιών, οι οποίες αντανακλούν την αξιολόγηση των κινδύνων που έχει διενεργήσει και απαιτεί τόσο από εκείνους όσο και από τους υπεργολάβους τους να παρέχουν εμφανή πειστήρια (evidence) συμμόρφωσής τους με τις ανωτέρω απαιτήσεις. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 14.5 | Ο Οργανισμός έχει αναπτύξει και επικοινωνήσει διαφορετικά σύνολα απαιτήσεων ασφάλειας για διαφορετικές κατηγορίες συμβάσεων, ανάλογα με το ύψος του κινδύνου για κάθε κατηγορία. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 14.6 | Ο Οργανισμός διασφαλίζει ότι οι ενέργειες που ακολουθούνται κατά τη διακοπή ή λήξη σύμβασης παροχής υπηρεσιών περιλαμβάνουν την απενεργοποίηση λογαριασμών χρηστών και υπηρεσιών, τον τερματισμό των ροών δεδομένων και την ασφαλή διαγραφή δεδομένων του Οργανισμού που βρίσκονται σε συστήματα του αναδόχου. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 14.7 | Ο Οργανισμός έχει υλοποιήσει απαιτήσεις διασφάλισης για τους προμηθευτές και παρόχους υπηρεσιών του, όπως ελέγχους παρείσδυσης (penetration tests), εξωτερικούς ελέγχους (external audits) ή/και διεθνώς αποδεκτές πιστοποιήσεις ασφάλειας. Παράλληλα, εφαρμόζει βασικούς δείκτες απόδοσης (key performance indicators) για να μετρήσει την απόδοση του συνόλου της εφοδιαστικής αλυσίδας όσον αφορά στις πρακτικές τους για τη διαχείριση της κυβερνοασφάλειας. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |

| 15. ΥΛΟΠΟΙΗΣΗ ΤΕΧΝΙΚΩΝ ΕΛΕΓΧΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ | | | | | |
|---|---|---|---|---|---|
| Α/Α | ΕΡΩΤΗΜΑΤΑ | ΑΠΑΝΤΗΣΕΙΣ | ΒΑΡΥΤΗΤΑ | SCORE | ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ |
| 15.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στη διενέργεια περιοδικών τεχνικών ελέγχων κυβερνοασφάλειας στα πληροφοριακά του συστήματα. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 15.2 | Ο Οργανισμός διενεργεί σε τακτική βάση (π.χ. μία φορά το μήνα) αυτοματοποιημένη σάρωση ευπαθειών στα πληροφοριακά του συστήματα, προκειμένου να εντοπιστούν δυνητικές ευπάθειες στο δίκτυο, στα συστήματα και στις εφαρμογές του. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 3 | 0 | |
| 15.3 | Ο Οργανισμός υλοποιεί εγκεκριμένη διαδικασία επιδιόρθωσης των ευπαθειών που έχουν ανιχνευθεί στα αγαθά του σε μηνιαία βάση. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 15.4 | Ο Οργανισμός διενεργεί σε περιοδική βάση (π.χ. μία φορά ετησίως) πλήρη αξιολόγηση των ευπαθειών στα πληροφοριακά του συστήματα (vulnerability assessment). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 15.5 | Ο Οργανισμός διενεργεί σε περιοδική βάση (π.χ. μία φορά ετησίως) εξωτερικό έλεγχο παρείσδυσης (external penetration test), με σκοπό την προσομοίωση κυβερνοεπίθεσης που εκκινεί έξω από τη δικτυακή περίμετρο του Οργανισμού. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 15.6 | Ο Οργανισμός διενεργεί σε περιοδική βάση (π.χ. μία φορά ετησίως) εσωτερικό έλεγχο παρείσδυσης (internal penetration test), με σκοπό την προσομοίωση κυβερνοεπίθεσης στο εσωτερικό δίκτυο του Οργανισμού. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |

| 15. ΥΛΟΠΟΙΗΣΗ ΤΕΧΝΙΚΩΝ ΕΛΕΓΧΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 15.7 | Ο Οργανισμός διενεργεί σε περιοδική βάση (π.χ. μία φορά ετησίως) ασκήσεις «κόκκινης / μπλε ομάδας» ("red team / blue team" exercises), με σκοπό την προσομοίωση κυβερνοεπιθέσεων από γνωστές υψηλού προφίλ ομάδες κυβερνοεγκληματιών. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 15.8 | Ο Οργανισμός υλοποιεί εγκεκριμένη διαδικασία επιδιόρθωσης των ευρημάτων που εντοπίζονται στους ελέγχους παρείσδυσης ή στις ασκήσεις «κόκκινης / μπλε ομάδας» με βάση σαφές πλάνο προτεραιοποίησης. Επίσης, υλοποιεί διαδικασία επικύρωσης των πρόσθετων μέτρων ασφάλειας που απαιτούνται για την επιδιόρθωση. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |

| 16. ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΕΓΚΑΤΑΣΤΑΣΕΩΝ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 16.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στη φυσική ασφάλεια των εγκαταστάσεων που φιλοξενούν τα πληροφοριακά του συστήματα. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 16.2 | Ο Οργανισμός έχει διασφαλίσει ότι οι κτηριακές εγκαταστάσεις που φιλοξενούν τους servers του (computer room) διαθέτουν στην εξωτερική περίμετρο μηχανισμούς ελέγχου (ενδεικτικά: μπάρες, κλειδαριές, συναγερμό) για την προστασία από μη εξουσιοδοτημένη φυσική πρόσβαση. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 16.3 | Ο Οργανισμός έχει διασφαλίσει ότι οι κτηριακές εγκαταστάσεις που φιλοξενούν τους servers του (computer room) διαθέτουν έναν επαρκώς στελεχωμένο χώρο υποδοχής που καταγράφει τους επισκέπτες κατά την είσοδό τους στο κτήριο. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |

| 16. ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΕΓΚΑΤΑΣΤΑΣΕΩΝ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 16.4 | Ο Οργανισμός τηρεί κατάλογο των ατόμων με εξουσιοδότηση πρόσβασης στο computer room. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 16.5 | Η είσοδος στο χώρο του computer room του Οργανισμού από τα εξουσιοδοτημένα άτομα γίνεται μόνο με χρήση έξυπνης κάρτας (smartcard). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 16.6 | Ο Οργανισμός υλοποιεί τους παρακάτω μηχανισμούς στο computer room: | | | | |
| 16.6.1 | • Σύστημα συναγερμού. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 16.6.2 | • Πλεονασμό (redundancy) σε συστήματα και κυκλώματα δικτύωσης. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 16.6.3 | • UPS, για την αδιάλειπτη παροχή ρεύματος και τη δυνατότητα ελεγχόμενου κλεισίματος μηχανημάτων και συσκευών (controlled shutdown). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 16.6.4 | • Συστήματα πυρανίχνευσης και πυρόσβεσης. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 16.6.5 | • Αυτοματοποιημένους ελεγκτές θερμοκρασίας, υγρασίας και πίεσης. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 16.6.6 | • Συστήματα προστασίας από διαρροή νερού. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 16.7 | Ο Οργανισμός έχει εγκαταστήσει κλειστό κύκλωμα τηλεόρασης (CCTV) με σκοπό την παρακολούθηση του εξωτερικού και εσωτερικού χώρου του computer room. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |

| 17. ΛΗΨΗ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ (BACKUP) | | | | | |
|---|---|---|---|---|---|
| Α/Α | ΕΡΩΤΗΜΑΤΑ | ΑΠΑΝΤΗΣΕΙΣ | ΒΑΡΥΤΗΤΑ | SCORE | ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ |
| 17.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στη λήψη αντιγράφων ασφαλείας από τα πληροφοριακά του συστήματα. Στις εν λόγω διαδικασίες περιλαμβάνονται θέματα όπως η προτεραιοποίηση, αξία και κρισιμότητα των δεδομένων καθώς και οι απαιτήσεις διατήρησης των ληφθέντων αντιγράφων. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 17.2 | Ο Οργανισμός έχει διασφαλίσει ότι λαμβάνονται αντίγραφα ασφαλείας με αυτοματοποιημένο τρόπο από όλα τα σημαντικά πληροφοριακά του συστήματα σε ημερήσια βάση, συνδυάζοντας με τον κατάλληλο τρόπο τις διαθέσιμες τεχνολογίες (full, incremental, differential). | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 17.3 | Ο Οργανισμός έχει διασφαλίσει ότι τα ληφθέντα αντίγραφα ασφαλείας προστατεύονται με κρυπτογράφηση κατά τη μεταφορά τους (encryption in transit). | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 2 | 0 | |
| 17.4 | Ο Οργανισμός έχει διασφαλίσει ότι τα ληφθέντα αντίγραφα ασφαλείας προστατεύονται με επαρκή μέτρα ασφάλειας κατά την αποθήκευσή τους. Παραδείγματα αποτελούν η κρυπτογράφηση, η πολυπαραγοντική αυθεντικοποίηση, ο έλεγχος πρόσβασης κ.α. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 17.5 | Ο Οργανισμός έχει διασφαλίσει ότι τα αντίγραφα ασφαλείας αποθηκεύονται σε τουλάχιστον έναν (1) offline προορισμό που δεν είναι συνδεδεμένος σε κάποιο δίκτυο. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 3 | 0 | |

| 17. ΛΗΨΗ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ (BACKUP) | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 17.6 | Ο Οργανισμός διενεργεί έλεγχο ακεραιότητας των αντιγράφων ασφαλείας σε περιοδική βάση. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 2 | 0 | |
| 17.7 | Ο Οργανισμός διενεργεί δοκιμή επαναφοράς δεδομένων (restoration) σε περιοδική βάση, με σκοπό την επικύρωση ότι η λήψη αντιγράφων ασφαλείας λειτουργεί με σωστό τρόπο. | Δεν απαντήθηκε<br>Δεν υλοποιείται<br>Υλοποιείται σε κάποια συστήματα<br>Υλοποιείται στα περισσότερα συστήμα<br>Υλοποιείται σε όλα τα συστήματα | 3 | 0 | |
| 17.8 | Ο Οργανισμός αποθηκεύει τα ληφθέντα αντίγραφα ασφαλείας σε διαφορετικές γεωγραφικά διεσπαρμένες τοποθεσίες. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |

| 18. ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 18.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στην αντιμετώπιση περιστατικών κυβερνοασφάλειας στα πληροφοριακά του συστήματα. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 18.2 | Ο Οργανισμός έχει αναπτύξει λεπτομερές πλάνο αντιμετώπισης περιστατικών κυβερνοασφάλειας (incident response plan). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |
| 18.3 | Το πλάνο αντιμετώπισης περιστατικών κυβερνοασφάλειας του Οργανισμού περιλαμβάνει τις παρακάτω φάσεις: | | | | |
| 18.3.1 | • Προετοιμασίας για ενδεχόμενο περιστατικό. Η φάση αυτή περιλαμβάνει την αξιολόγηση των κρίσιμων συστημάτων, την ανάλυση απειλών, την εφαρμογή μέτρων ασφάλειας και την οργάνωση του ανθρώπινου δυναμικού στην όλη διαδικασία. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 18.3.2 | • Ανίχνευσης και ανάλυσης του περιστατικού. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 18.3.3 | • Περιορισμού της μόλυνσης και εξάλειψης του συνόλου των στοιχείων που προκάλεσαν το περιστατικό. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 18.3.4 | • Ανάκτησης δεδομένων και λειτουργικότητας. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |

| 18. ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 18.3.5 | • Συλλογής του συνόλου των πειστηρίων του περιστατικού, σύνταξης λεπτομερούς αναφοράς και ενημέρωσης των εμπλεκόμενων μερών και των αρμόδιων Αρχών. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 18.3.6 | • Ανασκόπησης και ανάπτυξης γνώσης από τα στοιχεία του περιστατικού, με σκοπό την ισχυροποίηση του Οργανισμού από μελλοντικές επιθέσεις. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 18.4 | Ο Οργανισμός έχει συγκροτήσει ομάδα αντιμετώπισης περιστατικών κυβερνοασφάλειας από το προσωπικό του και έχει αναθέσει συγκεκριμένους ρόλους και αρμοδιότητες. Εφόσον η ανάπτυξη της ομάδας δεν είναι εφικτή in-house, έχει αναθέσει το έργο σε εξειδικευμένο πάροχο αντίστοιχων υπηρεσιών. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 18.5 | Ο Οργανισμός έχει διασφαλίσει ότι η ομάδα αντιμετώπισης περιστατικών κυβερνοασφάλειας, είτε η δική του είτε του τρίτου παρόχου, έχει πρόσβαση σε επαρκείς πηγές δεδομένων και εργαλεία που παρακολουθούν τα πληροφοριακά συστήματα για την ανίχνευση βασικών δεικτών παραβίασης. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 18.6 | Ο Οργανισμός διενεργεί, σε τακτές χρονικές περιόδους, εκπαίδευση αντιμετώπισης περιστατικών κυβερνοασφάλειας στο προσωπικό με την αντίστοιχη αρμοδιότητα. Η εκπαίδευση περιλαμβάνει τεχνικές και μη τεχνικές θεματικές ενότητες και διαφοροποιείται ανάλογα με τους ρόλους που έχουν ανατεθεί. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |
| 18.7 | Ο Οργανισμός έχει σχεδιάσει και διενεργεί σε περιοδική βάση ασκήσεις προσομοίωσης περιστατικών κυβερνοασφάλειας, με σκοπό η αρμόδια ομάδα απόκρισης να αναπτύξει επίγνωση και ικανότητα διαχείρισης έναντι πραγματικών απειλών. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 1 | 0 | |
| 18.8 | Ο Οργανισμός έχει υλοποιήσει Κέντρο Επιχειρήσεων Ασφάλειας (Security Operations Center, SOC), εξοπλισμένο με τα κατάλληλα εξειδικευμένα εργαλεία (monitoring, scanning and forensic tools) και στελεχωμένο με το αναγκαίο εξειδικευμένο προσωπικό, με σκοπό την έγκαιρη ανίχνευση και αντιμετώπιση περιστατικών κυβερνοασφάλειας. Το SOC μπορεί να έχει υλοποιηθεί είτε in-house είτε να έχει ανατεθεί ως υπηρεσία σε εξειδικευμένο πάροχο αντίστοιχων υπηρεσιών. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |

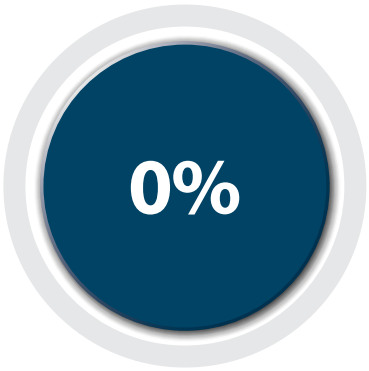
| 19. ΔΙΑΣΦΑΛΙΣΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ ΚΑΙ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΗ | | | | | |
|---|---|---|---|---|---|
| Α/Α | ΕΡΩΤΗΜΑΤΑ | ΑΠΑΝΤΗΣΕΙΣ | ΒΑΡΥΤΗΤΑ | SCORE | ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ |
| 19.1 | Ο Οργανισμός έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στη διασφάλιση της επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή των κρίσιμων πληροφοριακών συστημάτων του μετά από ανεπιθύμητο συμβάν. | Δεν απαντήθηκε<br>Δεν υπάρχει πολιτική και διαδικασίες<br>Πολιτική και διαδικασίες ασκούνται εμπειρικά<br>Υπάρχει μερικώς γραπτή πολιτική και διαδικασίες<br>Υπάρχει γραπτή πολιτική και διαδικασίες<br>Υπάρχει εγκεκριμένη γραπτή πολιτική και διαδικασίες | 3 | 0 | |
| 19.2 | Ο Οργανισμός έχει εντοπίσει τα κρίσιμα συστήματα και λειτουργίες του και έχει διενεργήσει αξιολόγηση των επιπτώσεων από την επέλευση ανεπιθύμητων συμβάντων (κυβερνοεπίθεση, φυσική καταστροφή κ.α.). | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 3 | 0 | |
| 19.3 | Ο Οργανισμός έχει αναπτύξει και καταγράψει λεπτομερές σχέδιο επιχειρησιακής συνέχειας, με σκοπό την άμεση αποκατάσταση και συνέχεια της διαθεσιμότητας των κρίσιμων λειτουργιών και υπηρεσιών του έπειτα από ανεπιθύμητο συμβάν. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | | |
| 19.4 | Ο Οργανισμός έχει συγκροτήσει συγκεκριμένη ομάδα του προσωπικού, η οποία κατέχει πλήρη γνώση των σχεδίων επιχειρησιακής συνέχειας και αντίστοιχη ικανότητα υλοποίησης των απαραίτητων ενεργειών για την αποκατάσταση των επιχειρησιακών λειτουργιών του Οργανισμού σε περίπτωση ανεπιθύμητου συμβάντος. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |
| 19.5 | Ο Οργανισμός διενεργεί σε τακτική βάση ασκήσεις δοκιμής των μέτρων διασφάλισης της επιχειρησιακής συνέχειας και αποκατάστασης από καταστροφή και ιδίως όταν έχουν επέλθει σοβαρές τεχνικές και διαδικαστικές αλλαγές στην επιχειρησιακή λειτουργία. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 19.6 | Ο Οργανισμός έχει υλοποιήσει πλεονάζοντες πόρους στην υπάρχουσα αρχιτεκτονική των συστημάτων του, με σκοπό την κάλυψη των απαιτήσεων διαθεσιμότητας. | Δεν απαντήθηκε<br>Όχι<br>Εν μέρει<br>Σε μεγάλο βαθμό<br>Πλήρως | 2 | 0 | |

| 19. ΔΙΑΣΦΑΛΙΣΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ ΚΑΙ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΗ | | | | | |
|---|---|---|---|---|---|
| **Α/Α** | **ΕΡΩΤΗΜΑΤΑ** | **ΑΠΑΝΤΗΣΕΙΣ** | **ΒΑΡΥΤΗΤΑ** | **SCORE** | **ΠΑΡΑΤΗΡΗΣΕΙΣ ΟΡΓΑΝΙΣΜΟΥ** |
| 19.7 | Ο Οργανισμός έχει υλοποιήσει έναν εναλλακτικό χώρο αποθήκευσης δεδομένων (backup site) που βρίσκεται σε επαρκή χιλιομετρική απόσταση από τον πρωταρχικό χώρο αποθήκευσης, με σκοπό τη μείωση της ευπάθειάς του έναντι της ίδιας κατηγορίας απειλών. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 19.8 | Ο Οργανισμός έχει αναθέσει σε εξειδικευμένο πάροχο cloud υπηρεσιών την παροχή υπηρεσίας ανάκαμψης από καταστροφή (disaster recovery as a service), με σκοπό την άμεση μεταφορά των επιχειρησιακών λειτουργιών του Οργανισμού σε άλλο περιβάλλον με χρήση των τεχνολογιών εικονικοποίησης (virtualization). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 19.9 | Ο Οργανισμός έχει υλοποιήσει έναν εναλλακτικό χώρο επεξεργασίας (disaster recovery site) που βρίσκεται σε επαρκή χιλιομετρική απόσταση από τον πρωταρχικό χώρο επεξεργασίας (primary site), με σκοπό τη μείωση της ευπάθειάς του έναντι της ίδιας κατηγορίας απειλών. | Δεν απαντήθηκε<br>Όχι<br>Ναι | 2 | 0 | |
| 19.10 | Ο Οργανισμός έχει πιστοποιηθεί ότι εφαρμόζει, συντηρεί και βελτιώνει ένα σύστημα διαχείρισης με βάση το οποίο προετοιμάζεται, ανταποκρίνεται και ανακτά κρίσιμες λειτουργίες και συνεχίζει να παρέχει προϊόντα και υπηρεσίες σε ένα αποδεκτό επίπεδο σε περίπτωση ανεπιθύμητου συμβάντος (π.χ. ISO 22301). | Δεν απαντήθηκε<br>Όχι<br>Ναι | 3 | 0 | |

# ΑΠΟΤΕΛΕΣΜΑΤΑ

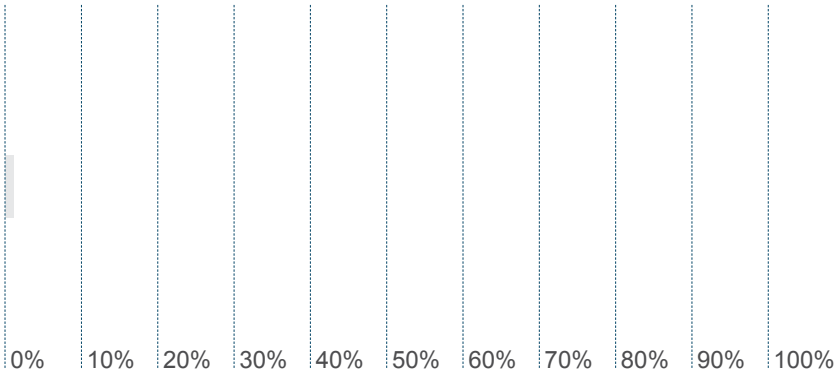
## ΣΥΓΚΕΝΤΡΩΤΙΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

### ΣΥΝΟΛΙΚΗ ΒΑΘΜΟΛΟΓΙΑ



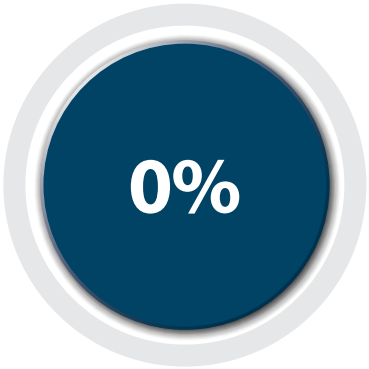

Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

### ΒΑΘΜΟΣ ΩΡΙΜΟΤΗΤΑΣ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΑΔΙΚΑΣΙΩΝ



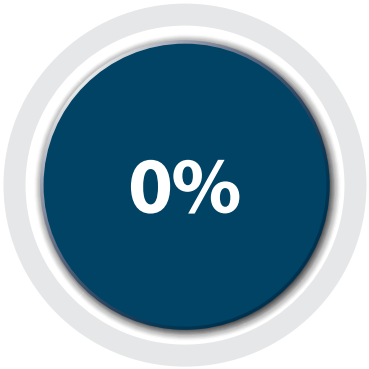

## ΑΠΟΤΕΛΕΣΜΑΤΑ ΑΝΑ ΘΕΜΑΤΙΚΗ ΕΝΟΤΗΤΑ

### 1. ΔΙΟΙΚΗΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ



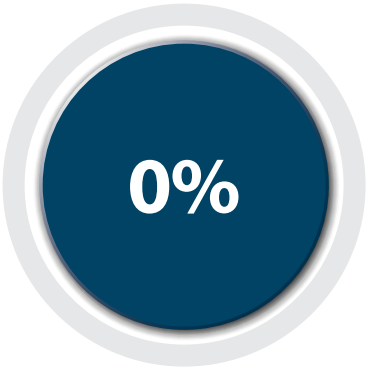

Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

### 2. ΚΑΤΑΓΡΑΦΗ ΥΛΙΚΟΥ ΚΑΙ ΛΟΓΙΣΜΙΚΟΥ




Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

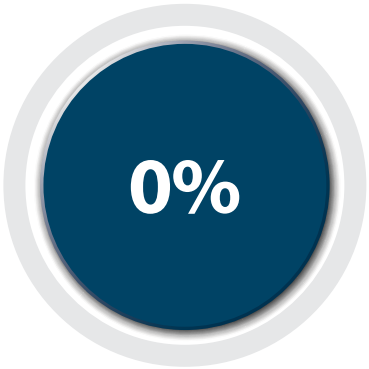
### 3. ΑΣΦΑΛΗΣ ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ ΕΞΟΠΛΙΣΜΟΥ ΚΑΙ ΕΦΑΡΜΟΓΩΝ




Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

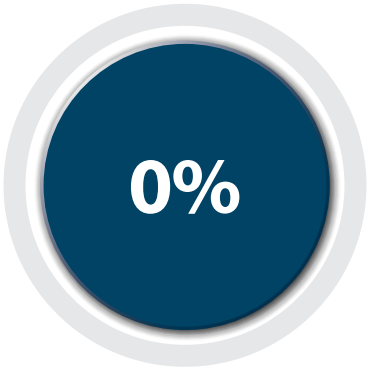
## ΑΠΟΤΕΛΕΣΜΑΤΑ ΑΝΑ ΘΕΜΑΤΙΚΗ ΕΝΟΤΗΤΑ

### 4. ΕΛΕΓΧΟΣ ΕΚΤΕΛΕΣΗΣ ΠΡΟΓΡΑΜΜΑΤΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ



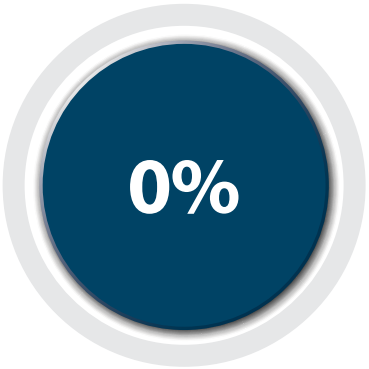

Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

### 5. ΔΙΑΧΕΙΡΙΣΗ ΛΟΓΑΡΙΑΣΜΩΝ ΚΑΙ ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ



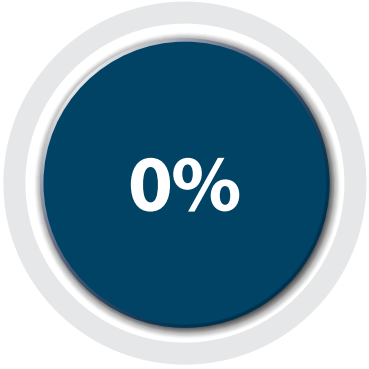

Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

### 6. ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΧΡΗΣΤΩΝ



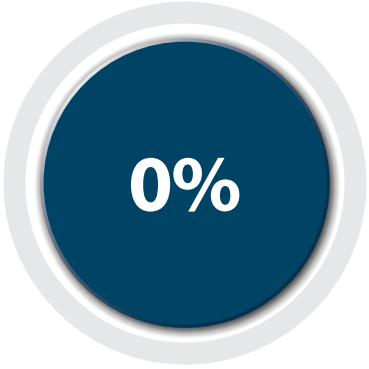

Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

### 7. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ




Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

### 8. ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ




Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

### 9. ΤΗΡΗΣΗ ΚΑΙ ΑΝΑΛΥΣΗ ΑΡΧΕΙΩΝ ΚΑΤΑΓΡΑΦΗΣ ΣΥΜΒΑΝΤΩΝ (EVENT LOGS)

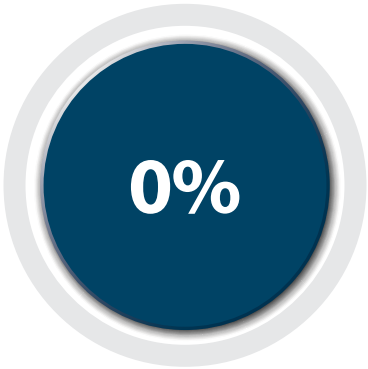

Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

## ΑΠΟΤΕΛΕΣΜΑΤΑ ΑΝΑ ΘΕΜΑΤΙΚΗ ΕΝΟΤΗΤΑ

### 10. ΑΣΦΑΛΕΙΑ ΔΙΑΔΙΚΤΥΑΚΩΝ ΕΦΑΡΜΟΓΩΝ

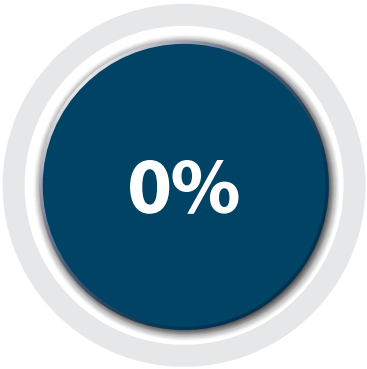

Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

### 11. ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΕΡΓΑΣΙΑ




Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

### 12. ΧΡΗΣΗ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

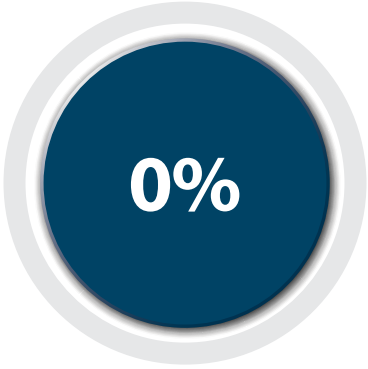



Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

### 13. ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΣΕ ΘΕΜΑΤΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ


Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

### 14. ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΣΤΗΝ ΕΦΟΔΙΑΣΤΙΚΗ ΑΛΥΣΙΔΑ (SUPPLY CHAIN RISK MANAGEMENT)




Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

### 15. ΥΛΟΠΟΙΗΣΗ ΤΕΧΝΙΚΩΝ ΕΛΕΓΧΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

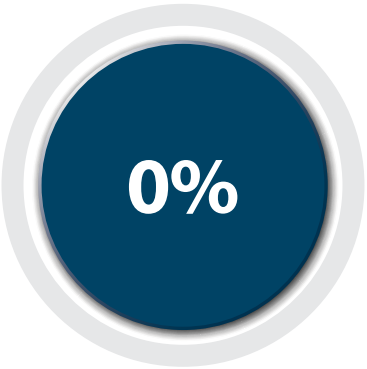

Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

## ΑΠΟΤΕΛΕΣΜΑΤΑ ΑΝΑ ΘΕΜΑΤΙΚΗ ΕΝΟΤΗΤΑ

### 16. ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΕΓΚΑΤΑΣΤΑΣΕΩΝ

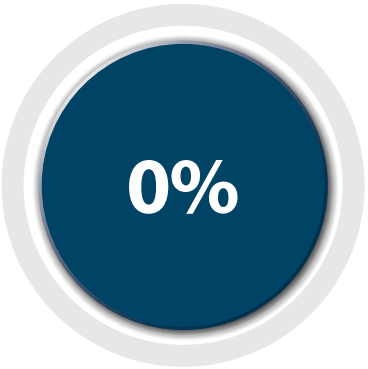

Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

### 17. ΛΗΨΗ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ (BACKUP)




Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

### 18. ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ




Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

### 19. ΔΙΑΣΦΑΛΙΣΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ ΚΑΙ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΗ


Βαθμολογία: **0%**
Επικινδυνότητα: **100%**
Κατάσταση: **CRITICAL RISK**

**ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ**
**ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ**
**ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ**

**ΙΟΥΛΙΟΣ 2022**