

3 – Πολιτικές Ασφάλειας

Εθνική Σχολή Δημόσιας Διοίκησης & Αυτοδιοίκησης
Απρίλιος 2021

Ενότητες

- ▶ Ανάγκη Θέσπισης Πολιτικής Ασφάλειας
- ▶ Οφέλη Πολιτικών Ασφάλειας
- ▶ Ανάπτυξη Πολιτικής Ασφάλειας
- ▶ Κατηγορίες Μέτρων Ασφάλειας
- ▶ Κρίσιμοι Παράγοντες Επιτυχίας

Πολιτικές Ασφάλειας

- ▶ Σε μία σύγχρονη Δημόσια Διοίκηση η επιχειρησιακή λειτουργία των φορέων και η ποιότητα των παρεχόμενων ηλεκτρονικών υπηρεσιών προς τους πολίτες βασίζονται στην **ασφάλεια των πληροφοριακών πόρων** που τις υποστηρίζουν

Πολιτικές Ασφάλειας

- ▶ Η θωράκιση των ψηφιακών συστημάτων του δημόσιου τομέα συμβάλει αποφασιστικά στην **επίτευξη των στόχων** των δημόσιων οργανισμών, **διασφαλίζει το κύρος** τους και επιτρέπει τη **συμμόρφωση** με τις νομικές υποχρεώσεις και τα διεθνή πρότυπα

Πολιτικές Ασφάλειας

- ▶ Η θωράκιση των ψηφιακών συστημάτων του δημόσιου τομέα συμβάλει αποφασιστικά στην **επίτευξη των στόχων** των δημόσιων οργανισμών, **διασφαλίζει το κύρος** τους και επιτρέπει τη **συμμόρφωση** με τις νομικές υποχρεώσεις και τα διεθνή πρότυπα

Πολιτικές Ασφάλειας

**Γιατί χρειαζόμαστε μία
Πολιτική Ασφάλειας;**

Πολιτικές Ασφάλειας

- ▶ Η πολυπλοκότητα των ψηφιακών συστημάτων, το ιδιαίτερα δυναμικό περιβάλλον λειτουργίας των φορέων και η επικινδυνότητα των κυβερνοεπιθέσεων, επιβάλλουν την υιοθέτηση μίας **ολιστικής προσέγγισης** μέσα από την εφαρμογή ενός **ενιαίου σχεδίου ασφάλειας** για την ανάπτυξη, υλοποίηση, λειτουργία, έλεγχο, διαχείριση, παρακολούθηση και βελτίωση των οργανωτικών και τεχνικών μέτρων προστασίας, διασφαλίζοντας την εδραίωση και διατήρηση του **επιθυμητού επιπέδου ασφάλειας**

Πολιτικές Ασφάλειας

- ▶ **Η διαχείριση της ασφάλειας** στοχεύει στην προστασία των ψηφιακών συστημάτων, περιορίζοντας την επικινδυνότητα σε αποδεκτό επίπεδο
 - ▶ Αξιολόγηση της επικινδυνότητας και προσδιορισμό του αποδεκτού επιπέδου ασφάλειας
 - ▶ Ανάπτυξη και εφαρμογή μιας Πολιτικής Ασφάλειας
 - ▶ Δημιουργία κατάλληλου οργανωτικού πλαισίου
 - ▶ Εξασφάλιση των απαιτούμενων πόρων για την εφαρμογή της Πολιτικής Ασφάλειας
 - ▶ Εκπαίδευση, ενημέρωση και ευαισθητοποίηση των χρηστών των ψηφιακών συστημάτων

Πολιτικές Ασφάλειας

- ▶ Η πολιτική ασφάλειας των ψηφιακών συστημάτων αποτυπώνει τη **δέσμευση της Διοίκησης** του Φορέα και τις **βασικές κατευθύνσεις** για τον τρόπο διαχείρισης των θεμάτων ασφάλειας (προστασία εμπιστευτικότητας, ακεραιότητας & διαθεσιμότητας)

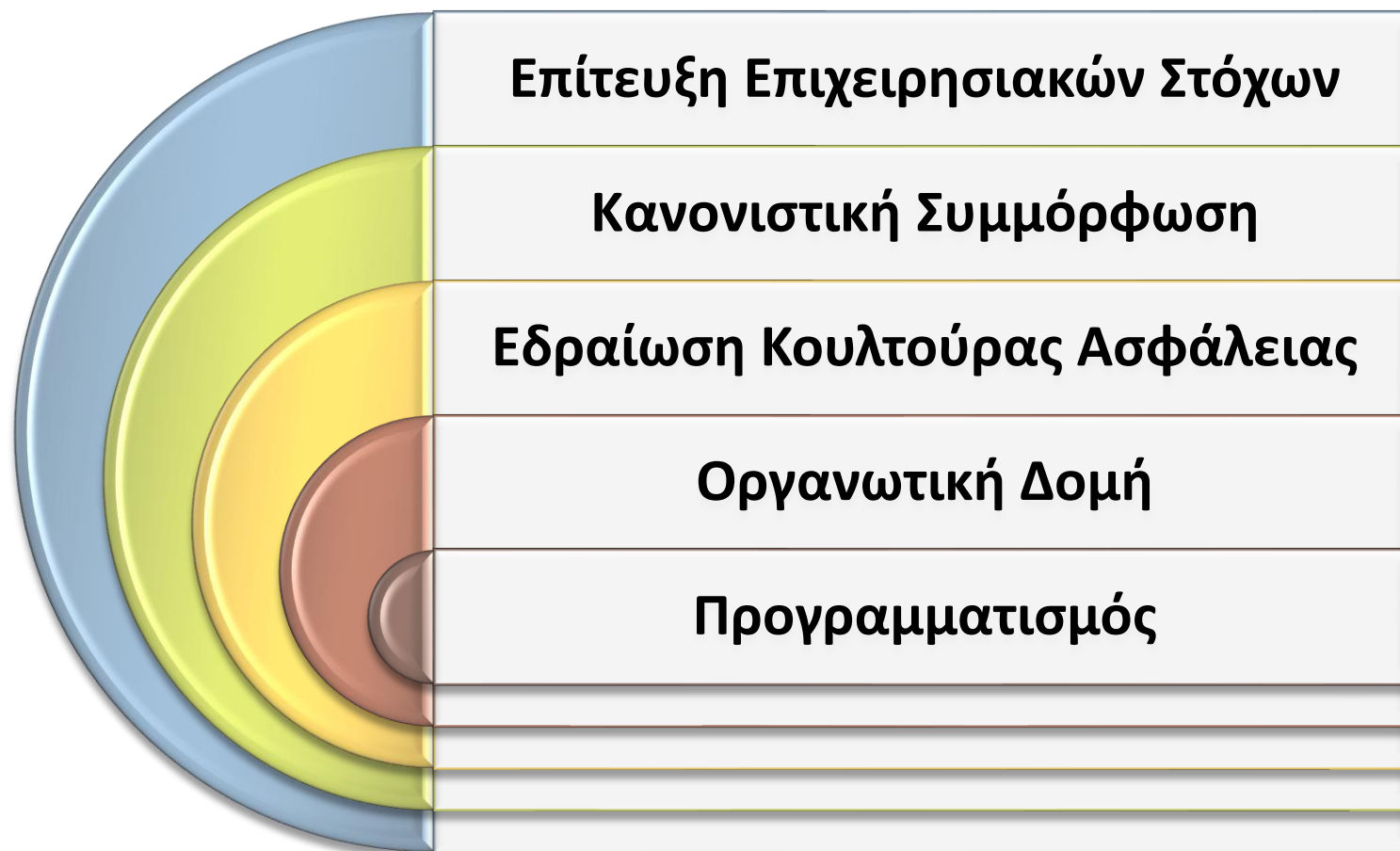
Πολιτικές Ασφάλειας



Πολιτικές Ασφάλειας

- ▶ Οι οδηγίες και οι διαδικασίες υλοποιούνται με την **εφαρμογή των μέτρων ασφάλειας**, τα οποία έχουν προκύψει μέσα από μία αξιολόγηση επικινδυνότητας
- ▶ Η πολιτική ασφάλειας φέρει την **έγκριση της Διοίκησης** του Φορέα, είναι δεσμευτική και κοινοποιείται στο σύνολο του προσωπικού
- ▶ Η **πολιτική ασφάλειας** μαζί με τα **μέτρα προστασίας** ή αντίμετρα ή μέτρα ασφάλειας αποτελούν το **σχέδιο ασφάλειας** του οργανισμού

Οφέλη Πολιτικής Ασφάλειας



Ανάπτυξη Πολιτικής Ασφάλειας

- ▶ Η ασφάλεια ψηφιακών συστημάτων χαρακτηρίζεται από το **πλήθος** και την **ποικιλομορφία** των **παραγόντων** που πρέπει να ληφθούν υπόψη
 - ▶ Τεχνικοί
 - ▶ Διοικητικοί – Οργανωτικοί

Γενικές Διαπιστώσεις

- ▶ Η ασφάλεια ψηφιακών συστημάτων εξαρτάται από **πολλούς παράγοντες** και δεν είναι ούτε αποκλειστικά, ούτε κυρίως τεχνικό ζήτημα
- ▶ Η **επίτευξη απόλυτης ασφάλειας δεν είναι εφικτός στόχος**, σε πραγματικές συνθήκες
- ▶ Για κάθε **επίπεδο** ασφάλειας υπάρχει ένα αντίστοιχο **κόστος** που θα πρέπει να καταβληθεί για την επίτευξή του
- ▶ Στο πλαίσιο της αρχής της αναλογικότητας, τα μέτρα προστασίας που θα ληφθούν θα πρέπει να αντιστοιχούν στο **επίπεδο** και τη **φύση** των κινδύνων που αντιμετωπίζει το ψηφιακό σύστημα

Ανάπτυξη Πολιτικής Ασφάλειας

- ▶ Η πολιτική ασφάλειας καταγράφει τις **βασικές επιλογές** της Διοίκησης και τη **βούλησή** της για τη θωράκιση των ψηφιακών συστημάτων του οργανισμού
- ▶ Περιγράφει τις **γενικές αρχές** πάνω στις οποίες βασίζεται η προστασία των πληροφοριών και προσφέρει μία σειρά από **κατευθυντήριες οδηγίες**
- ▶ Πρέπει να **επικυρώνεται** από τη Διοίκηση του Φορέα

Ανάπτυξη Πολιτικής Ασφάλειας

- ▶ Σχεδιάζοντας μία πολιτική ασφάλειας
 - ▶ Υιοθετούμε **ολιστική προσέγγιση**
 - ▶ Λαμβάνουμε υπόψη τις **τρέχουσες τεχνολογικές εξελίξεις**
 - ▶ Ακολουθούμε μία σειρά διαδοχικών σταδίων, με στόχο την **κάλυψη όλων των διαστάσεων ασφάλειας** των ψηφιακών συστημάτων ενός οργανισμού

Ανάπτυξη Πολιτικής Ασφάλειας

- ▶ Το **αρχικό στάδιο** ανάπτυξης μίας πολιτικής ασφάλειας αφορά την **τεκμηρίωση** των ψηφιακών συστημάτων του φορέα
 - ▶ Σκοπός
 - ▶ Στόχοι
 - ▶ Οριοθέτηση του πεδίου εφαρμογής
 - ▶ Αποτίμηση των αγαθών που κρίζουν προστασίας
 - ▶ Καταγραφή των λειτουργικών στοιχείων που συνθέτουν τα ψηφιακά συστήματα του οργανισμού και του περιβάλλοντος λειτουργίας τους

Ανάπτυξη Πολιτικής Ασφάλειας

- ▶ Ως **αγαθά** ορίζονται τα δεδομένα, οι πληροφορίες και οι υπολογιστικοί πόροι που έχουν αξία (εκφραζόμενη σε χρηματικούς ή άλλους όρους) για το φορέα

Ανάπτυξη Πολιτικής Ασφάλειας

- ▶ Το **επόμενο στάδιο** διαμόρφωσης μίας πολιτικής ασφάλειας αφορά την επιλογή της **μεθόδου ανάλυσης της επικινδυνότητας (risk analysis)** που θα εφαρμοστεί, καθώς και του **προτύπου (standard)** διαχείρισης της πολιτικής

Ανάπτυξη Πολιτικής Ασφάλειας

- ▶ **Ανάλυση και διαχείριση επικινδυνότητας**
 - ▶ Εντοπισμός και την αποτίμηση των **παραμέτρων** που έχουν σχέση με την ασφάλεια των ψηφιακών συστημάτων
 - ▶ Επιλογή και περιγραφή των απαραίτητων **διαδικαστικών** και **τεχνικών μέτρων** για την προστασία τους

Ανάπτυξη Πολιτικής Ασφάλειας

- ▶ Η **αξιολόγηση** των αγαθών και κυρίως η αξιολόγηση των δεδομένων αποτελεί βασική δραστηριότητα της μεθόδου ανάλυσης της επικινδυνότητας
- ▶ Λαμβάνει υπόψη την **εκτίμηση** για τις **πιθανές επιπτώσεις** που ενδέχεται να προκύψουν από την απώλεια των βασικών απαιτήσεων ασφάλειας των δεδομένων, δηλαδή από το **ενδεχόμενο** περιορισμού της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας των δεδομένων

Ανάπτυξη Πολιτικής Ασφάλειας

- ▶ Η **καταγραφή** και **αποτίμηση** τόσο των κινδύνων που υφίστανται τα ψηφιακά συστήματα και οι εγκαταστάσεις τους, όσο και των **πιθανών επιπτώσεων** που είναι δυνατόν να υποστεί ένας φορέας από ενδεχόμενες κακόβουλες ενέργειες, είναι απαραίτητη προϋπόθεση για την επιλογή των κατάλληλων **τεχνολογιών**, καθώς και των αντίστοιχων τεχνολογικών **μέτρων** και των οργανωτικών και διαδικαστικών **πρωτοβουλιών** και **ενεργειών** που είναι απαραίτητες για την ασφάλεια των συστημάτων και των εγκαταστάσεων του φορέα

Ανάπτυξη Πολιτικής Ασφάλειας

- ▶ Η **ανάλυση επικινδυνότητας** παρέχει τη δυνατότητα να εντοπιστούν οι τομείς που απαιτούν τη λήψη μέτρων ασφάλειας (αντιμέτρων) και να προσδιοριστεί το επίπεδο προστασίας που απαιτείται
- ▶ Το σύνολο των μέτρων ασφάλειας, σε συνδυασμό με την πολιτική ασφάλειας αποτελούν το **Σχέδιο Ασφάλειας**

Ανάπτυξη Πολιτικής Ασφάλειας

- ▶ Η **αποτελεσματικότητα** του σχεδίου ασφάλειας προϋποθέτει την πιστή και συνολική εφαρμογή του
- ▶ Τα **αντίμετρα** βρίσκονται σε αλληλεξάρτηση και η αποτελεσματικότητα ενός αντιμέτρου εξαρτάται συχνά από την υλοποίηση ενός άλλου
- ▶ Κανένα τεχνικό αντίμετρο δεν πρόκειται να αποδώσει τα αναμενόμενα αποτελέσματα, χωρίς την παράλληλη εφαρμογή ενός κατάλληλου **οργανωτικού σχήματος** και ενός **προγράμματος ευαισθητοποίησης, ενημέρωσης και εκπαίδευσης**

Κατηγορίες απαιτήσεων ασφάλειας

Ποιες κατηγορίες απαιτήσεων ασφάλειας πρέπει να καλύπτονται από τις διαδικασίες και τα μέτρα προστασίας του σχεδίου ασφάλειας;

Κατηγορίες απαιτήσεων ασφάλειας

Κανονιστική Συμμόρφωση

Οργανωτική Δομή

- Υπεύθυνος Ασφάλειας (Security Officer)
- Επιτροπή Εποπτείας και Ελέγχου (Steering Committee)

Διαχείριση Προσωπικού

Διαχείριση Πολιτικής Ασφάλειας

Έλεγχος Πρόσβασης

Διαχείριση Αλλαγών

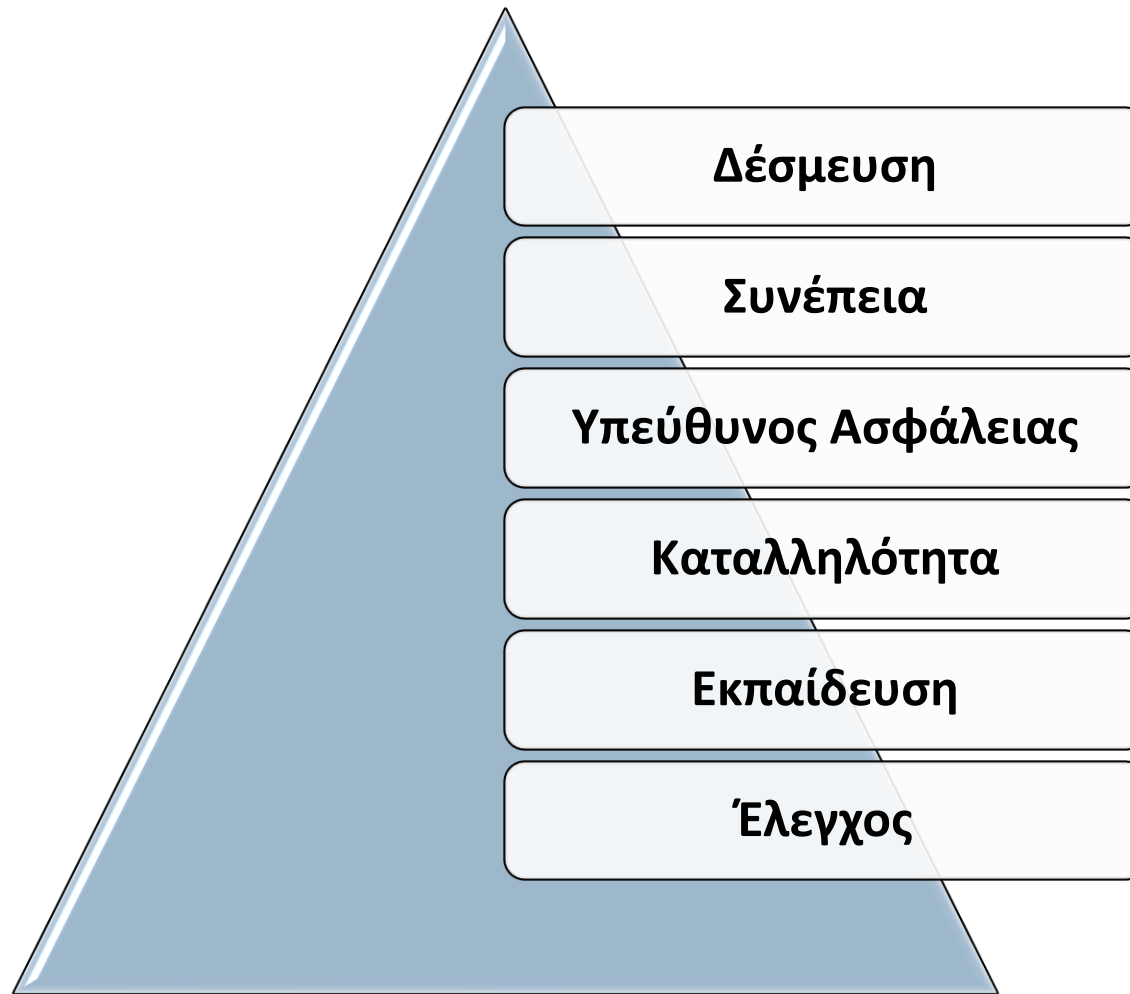
Φυσική Ασφάλεια

Σχέδιο Συνέχισης Λειτουργίας

Κρίσιμοι Παράγοντες Επιτυχίας

- ▶ Η **σχεδίαση**, η **υλοποίηση**, η **διαχείριση** και ο **έλεγχος** μίας πολιτικής ασφάλειας αποτελεί γενικά ένα σύνθετο και πολυδιάστατο ζήτημα

Κρίσιμοι Παράγοντες Επιτυχίας



Ευχαριστώ για την προσοχή σας

Ερωτήσεις

