ΕΦΗΜΕΡΙΔΑ
ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ
ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

3 Δεκεμβρίου 2021 | ΤΕΥΧΟΣ ΔΕΥΤΕΡΟ | Αρ. Φύλλου **5672**

ΑΠΟΦΑΣΕΙΣ

Αρ. απόφ. 195/4/29.11.2021

Υιοθέτηση Κατευθυντήριων Γραμμών της Ευρωπαϊκής Αρχής Ασφαλίσεων και Επαγγελματικών Συντάξεων (EIOPA) σχετικά με την ασφάλεια και τη διακυβέρνηση της Τεχνολογίας Πληροφορικής & Επικοινωνιών (EIOPA-BoS-20-600).

ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ
Η ΕΚΤΕΛΕΣΤΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΣ ΤΡΑΠΕΖΑΣ ΤΗΣ ΕΛΛΑΔΟΣ

Αφού έλαβε υπόψη:

α) τα άρθρα 28 και 55Α του καταστατικού της Τράπεζας της Ελλάδος (Α' 298/1927),

β) τον ν. 4364/2016 «Προσαρμογή της ελληνικής νομοθεσίας στην Οδηγία 2009/138/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009, σχετικά με την ανάληψη και την άσκηση δραστηριοτήτων ασφάλισης και αντασφάλισης (Φερεγγυότητα ΙΙ), στα άρθρα 2 και 8 της Οδηγίας 2014/51/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 16ης Απριλίου 2014 σχετικά με την τροποποίηση των Οδηγιών 2003/71/ΕΚ και 2009/138/ΕΚ, και των Κανονισμών (ΕΚ) υπ' αρ. 1060/2009, (ΕΕ) υπ' αρ. 1094/2010 και (ΕΕ) υπ' αρ. 1095/2010, όσον αφορά τις εξουσίες της Ευρωπαϊκής Αρχής Ασφαλίσεων και Επαγγελματικών Συντάξεων (εφεξής ΕΑΑΕΣ) και της Ευρωπαϊκής Αρχής Κινητών Αξιών και Αγορών, καθώς και στο άρθρο 4 της Οδηγίας 2011/89/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Νοεμβρίου 2011, σχετικά με τη συμπληρωματική εποπτεία των χρηματοπιστωτικών οντοτήτων που ανήκουν σε χρηματοπιστωτικούς ομίλους ετερογενών δραστηριοτήτων και συναφείς διατάξεις της νομοθεσίας περί της ιδιωτικής ασφάλισης και άλλες διατάξεις» (Α' 13) και ιδίως τα άρθρα 30, 32, 34, 35, 46, 104, 201 και 256 αυτού,

γ) την Πράξη Εκτελεστικής Επιτροπής της Τράπεζας της Ελλάδος υπ' αρ. 60/12.2.2016 «Υιοθέτηση Κατευθυντήριων Γραμμών της Ευρωπαϊκής Αρχής Ασφαλίσεων και Επαγγελματικών Συντάξεων (EIOPA) σχετικά με το σύστημα διακυβέρνησης (EIOPA-BoS-14-253/28.1.2015),

δ) την Πράξη Εκτελεστικής Επιτροπής της Τράπεζας της Ελλάδος υπ' αρ. 180/3/17.12.2020 «Υιοθέτηση Κατευθυντήριων Γραμμών της Ευρωπαϊκής Αρχής Ασφαλίσεων και Επαγγελματικών Συντάξεων (EIOPA) σχετικά με την εξωτερική ανάθεση δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους (EIOPA-BoS- 20-002),

ε) τον Κανονισμό υπ' αρ. 1094/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη Σύσταση Ευρωπαϊκής Αρχής Ασφαλίσεων και Επαγγελματικών Συντάξεων (ΕΕ L 331 της 15.12.2010), και ιδίως το άρθρο 16 αυτού,

στ) τον κατ' εξουσιοδότηση Κανονισμό (ΕΕ) 2015/35 της Επιτροπής για τη συμπλήρωση της Οδηγίας 2009/138/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ανάληψη και την άσκηση δραστηριοτήτων ασφάλισης και αντασφάλισης (Φερεγγυότητα ΙΙ) (ΕΕ L 12 της 17.1.2015), και ιδίως τα άρθρα 258, 259, 260, 266, 268, 269, 270, 271 και 274 αυτού,

ζ) τις Κατευθυντήριες Γραμμές της Ευρωπαϊκής Αρχής Ασφαλίσεων και Επαγγελματικών Συντάξεων (EIOPA) σχετικά με την ασφάλεια και τη διακυβέρνηση των Τεχνολογιών των Πληροφοριών και των Επικοινωνιών (EIOPA-BoS-20-600),

η) ότι από τις διατάξεις της παρούσας δεν προκύπτει δαπάνη σε βάρος του κρατικού προϋπολογισμού, αποφασίζει:

Να υιοθετήσει τις Κατευθυντήριες Γραμμές της Ευρωπαϊκής Αρχής Ασφαλίσεων και Επαγγελματικών Συντάξεων σχετικά με την ασφάλεια και τη διακυβέρνηση της τεχνολογίας πληροφορικής και επικοινωνιών (EIOPA-BoS-20-600) ως εξής:

Άρθρο 1
Σκοπός και Ορισμοί

1. Σκοπός της παρούσας είναι να θεσπισθεί πλαίσιο οδηγιών απευθυνόμενο προς τις ασφαλιστικές και αντασφαλιστικές επιχειρήσεις σε σχέση με την ασφάλεια και τη διακυβέρνηση Τεχνολογίας Πληροφορικής και Επικοινωνιών (ΤΠΕ) για την εφαρμογή των απαιτήσεων διακυβέρνησης που προβλέπονται στα άρθρα 30, 32, 34 και 35 του ν. 4364/2016, στις Πράξεις Εκτελεστικής Επιτροπής υπ' αρ. 60/12.2.2016 και 180/3/17.12.2020, καθώς και στα άρθρα 258, 259, 260, 266, 268, 269, 270, 271 και 274 του Κανονισμού (ΕΕ) 2015/35.

2. Οι παρούσες κατευθυντήριες γραμμές εφαρμόζονται κατ' αναλογία και σε επίπεδο ομίλου.

3. Κατά την εφαρμογή της παρούσας, οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις, λαμβάνουν υπόψη την αρχή της αναλογικότητας, ώστε να διασφαλίζεται ότι οι ρυθμίσεις διακυβέρνησης, συμπεριλαμβανομένων αυτών που σχετίζονται με την ασφάλεια και τη διακυβέρνηση των ΤΠΕ, εφαρμόζονται κατά τρόπο αναλογικό προς την φύση, κλίμακα και πολυπλοκότητα των υποκείμενων κινδύνων.

4. Για τις ανάγκες της παρούσας, λαμβάνονται υπόψη οι ορισμοί που δίδονται στις αντίστοιχες έννοιες στις διατάξεις του ν. 4364/2016, της Οδηγίας 2009/138/ΕΚ (Φερεγγυότητα ΙΙ) και των Κανονισμών 1094/2010 και (ΕΕ) 2015/35 που αναφέρονται ανωτέρω. Σε περίπτωση απόκλισης μεταξύ των ορισμών των ιδίων εννοιών στην ελληνική απόδοση των ως άνω νομοθετικών κειμένων, προκρίνεται η ορολογία που υιοθετεί ο ν. 4364/2016.

Ειδικότερα, ισχύουν οι ακόλουθοι ορισμοί:

α. «Ιδιοκτήτης πληροφοριακού πόρου»: Πρόσωπο ή φορέας με υποχρέωση λογοδοσίας και εξουσία επί πληροφοριακού πόρου ή πόρου ΤΠΕ.

β. «Διαθεσιμότητα: Η ιδιότητα του να είναι κάτι διαθέσιμο και έτοιμο προς χρήση κατόπιν παραγγελίας (επικαιρότητα) από εξουσιοδοτημένο φορέα.

γ. «Εμπιστευτικότητα»: Η ιδιότητα της μη δημοσιοποίησης ή γνωστοποίησης πληροφοριών σε μη εξουσιοδοτημένα πρόσωπα, φορείς, διαδικασίες ή συστήματα

δ. «Επίθεση στον κυβερνοχώρο»: Οποιοδήποτε είδος δικτυοπαραβίασης που οδηγεί σε επιθετική/κακόβουλη απόπειρα καταστροφής, έκθεσης, τροποποίησης, απενεργοποίησης, κλοπής ή απόκτησης μη εξουσιοδοτημένης πρόσβασης ή μη εξουσιοδοτημένης χρήσης ενός πληροφοριακού πόρου, που στοχεύει τα συστήματα ΤΠΕ.

ε. «Ασφάλεια στον κυβερνοχώρο»: Προστασία του εμπιστευτικού χαρακτήρα, της ακεραιότητας και της διαθεσιμότητας πληροφοριών ή/και συστημάτων πληροφοριών μέσω του κυβερνοχώρου.

στ. «Πόρος ΤΠΕ»: Πόρος είτε λογισμικού είτε υλισμικού που απαντάται στο επιχειρηματικό περιβάλλον.

ζ. «Έργο ΤΠΕ»: Κάθε έργο, ή μέρος έργου, στο πλαίσιο του οποίου αλλάζουν, αντικαθίστανται, καταργούνται ή υλοποιούνται συστήματα ΤΠΕ.

η. «Κίνδυνος ΤΠΕ και Ασφάλειας»: Κίνδυνος ζημίας λόγω παραβίασης της εμπιστευτικότητας, αστοχίας της ακεραιότητας συστημάτων και δεδομένων, ακαταλληλότητας ή μη διαθεσιμότητας συστημάτων και δεδομένων, ή αδυναμίας αλλαγής Τεχνολογίας Πληροφορικής (ΤΠ) εντός εύλογου χρονικού διαστήματος και με εύλογο κόστος όταν οι απαιτήσεις του περιβάλλοντος ή των επιχειρηματικών δραστηριοτήτων μεταβάλλονται (δηλ. ευελιξία). Στο πλαίσιο αυτό περιλαμβάνονται κίνδυνοι ασφάλειας που προκύπτουν λόγω ανεπάρκειας ή αστοχίας εσωτερικών διεργασιών ή εξωτερικών συμβάντων, μεταξύ των οποίων περιλαμβάνονται και οι επιθέσεις στον κυβερνοχώρο ή η ανεπαρκής φυσική ασφάλεια.

θ. «Ασφάλεια πληροφοριών»: Προστασία του εμπιστευτικού χαρακτήρα, της ακεραιότητας και της διαθεσιμότητας πληροφοριών ή/και συστημάτων πληροφοριών. Επιπλέον, το ίδιο μπορεί επίσης να ισχύει για άλλες ιδιότητες, όπως η αυθεντικότητα, η λογοδοσία, η μη αποποίηση και η αξιοπιστία.

ι. «Υπηρεσίες ΤΠΕ»: Υπηρεσίες παρεχόμενες από συστήματα ΤΠΕ σε έναν ή περισσότερους εσωτερικούς ή εξωτερικούς χρήστες. Περιλαμβάνονται, παραδείγματος χάριν, υπηρεσίες εισαγωγής δεδομένων, αποθήκευσης δεδομένων, επεξεργασίας δεδομένων και υποβολής αναφορών, αλλά και υπηρεσίες παρακολούθησης, υποστήριξης επιχειρηματικών δραστηριοτήτων και υποστήριξης λήψης αποφάσεων.

ια. «Συστήματα ΤΠΕ»: Εγκατάσταση ΤΠΕ ως μέρος ενός μηχανισμού ή ενός δικτύου διασύνδεσης το οποίο υποστηρίζει τις λειτουργίες ασφαλιστικής ή/και αντασφαλιστικής επιχείρησης.

ιβ. «Πληροφοριακός πόρος»: Συλλογή πληροφοριών, είτε υλικών είτε άυλων, που αξίζει να προστατεύονται.

ιγ. «Ακεραιότητα»: Η ιδιότητα ακρίβειας και πληρότητας.

ιδ. «Περιστατικό λειτουργικού κινδύνου ή περιστατικό ασφάλειας»: Μεμονωμένο συμβάν ή σειρά συνδεόμενων μη προγραμματισμένων από την επιχείρηση συμβάντων, τα οποία έχουν ή ενδέχεται να έχουν δυσμενείς επιπτώσεις στην ακεραιότητα, τη διαθεσιμότητα την εμπιστευτικότητα και/ή την αυθεντικότητα των υπηρεσιών.

ιε. «Πάροχος υπηρεσιών»: τρίτη, σε σχέση με την ασφαλιστική ή αντασφαλιστική επιχείρηση, οντότητα, που αναλαμβάνει, εξ ολοκλήρου ή μερικώς, να εκτελέσει διαδικασία, να παράσχει υπηρεσία ή να ασκήσει δραστηριότητα, στο πλαίσιο συμφωνίας εξωτερικής ανάθεσης.

ιστ. «Δοκιμή παρείσδυσης βάσει απειλών»: Μια ελεγχόμενη απόπειρα να τεθεί σε κίνδυνο η ανθεκτικότητα μιας οντότητας όσον αφορά την ασφάλεια στον κυβερνοχώρο, μέσω της προσομοίωσης τακτικών, τεχνικών και διαδικασιών πραγματικών παραγόντων απειλών. Βασίζεται σε στοχευμένες πληροφορίες απειλών και εστιάζει στα άτομα, τις διαδικασίες και την τεχνολογία ενός φορέα, με ελάχιστη γνώση εκ των προτέρων και επιπτώσεις στις επιχειρησιακές λειτουργίες.

ιζ. «Τρωτότητα»: Αδυναμία, ευαισθησία ή ελάττωμα ενός πόρου ή μιας δικλείδας ασφάλειας, που μπορεί να αξιοποιηθεί από μία ή περισσότερες απειλές.

Άρθρο 2
(1η κατευθυντήρια γραμμή)
Αναλογικότητα

1. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις συμμορφώνονται με τις ρυθμίσεις της παρούσας κατά τρόπο ανάλογικό λαμβάνοντας υπόψη τη φύση, την κλίμακα και πολυπλοκότητα των κινδύνων που ενέχουν οι δραστηριότητές τους.

Άρθρο 3
(2η κατευθυντήρια γραμμή)
ΤΠΕ εντός του συστήματος διακυβέρνησης

1. Το Διοικητικό Συμβούλιο διασφαλίζει ότι το σύστημα διακυβέρνησης των επιχειρήσεων, ιδίως το σύστημα διαχείρισης κινδύνων και εσωτερικού ελέγχου, διαχειρίζεται επαρκώς τους κινδύνους ΤΠΕ και ασφάλειας των επιχειρήσεων.

2. Το Διοικητικό Συμβούλιο μεριμνά ώστε ο αριθμός και οι δεξιότητες των μελών του προσωπικού των ασφαλι-

στικών και αντασφαλιστικών επιχειρήσεων να επαρκούν για την υποστήριξη σε διαρκή βάση των λειτουργικών τους αναγκών στον τομέα των ΤΠΕ και των διεργασιών όσον αφορά τη διαχείριση των κινδύνων ΤΠΕ και ασφάλειας, καθώς και για τη διασφάλιση της εφαρμογής της οικείας στρατηγικής ΤΠΕ. Επιπλέον, οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις μεριμνούν ώστε τα μέλη του προσωπικού, συμπεριλαμβανομένων των μελών διοίκησης, να λαμβάνουν κατάλληλη εκπαίδευση σχετικά με τους κινδύνους ΤΠΕ και ασφάλειας, συμπεριλαμβανομένης της ασφάλειας πληροφοριών, σε περιοδική βάση, όπως ορίζεται στο άρθρο 15 της παρούσας.

3. Το Διοικητικό Συμβούλιο διασφαλίζει ότι οι διαθέσιμοι πόροι, ανθρώπινοι, υλικοτεχνικοί και χρηματικοί, είναι επαρκείς και κατάλληλοι για την εκπλήρωση των προαναφερόμενων υποχρεώσεων.

Άρθρο 4
(3η κατευθυντήρια γραμμή)
Στρατηγική ΤΠΕ

1. Το Διοικητικό Συμβούλιο έχει τη συνολική ευθύνη για τον καθορισμό, την έγκριση, και την επίβλεψη της εφαρμογής της γραπτής στρατηγικής ΤΠΕ των ασφαλιστικών και αντασφαλιστικών επιχειρήσεων, η οποία εναρμονίζεται με τη συνολική επιχειρηματική στρατηγική τους. Επίσης, το Διοικητικό Συμβούλιο επιβλέπει την ενημέρωση των κατάλληλων προσώπων εντός της επιχείρησης για την εν λόγω στρατηγική.

2. Η στρατηγική ΤΠΕ καθορίζει τουλάχιστον τα εξής:

α) τον τρόπο με τον οποίο εξελίσσεται η ΤΠΕ ώστε να υποστηρίζει και εφαρμόζει αποτελεσματικά την επιχειρηματική στρατηγική των επιχειρήσεων, συμπεριλαμβανομένης της εξέλιξης της οργανωτικής δομής, των ακολουθούμενων επιχειρηματικών μοντέλων, των συστημάτων ΤΠΕ και των κύριων αλληλεξαρτήσεων με παρόχους υπηρεσιών,

β) την εξέλιξη της αρχιτεκτονικής της ΤΠΕ, συμπεριλαμβανομένων των αλληλεξαρτήσεων με παρόχους υπηρεσιών και

γ) τους σαφείς στόχους ασφάλειας πληροφοριών, με ιδιαίτερη έμφαση στα συστήματα και τις υπηρεσίες ΤΠΕ καθώς και στο προσωπικό και στις διεργασίες ΤΠΕ.

3. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις διασφαλίζουν ότι η στρατηγική ΤΠΕ υλοποιείται, υιοθετείται και κοινοποιείται εγκαίρως σε όλα τα μέλη του αρμόδιου προσωπικού και στους παρόχους υπηρεσιών.

4. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις αναπτύσσουν διαδικασίες με τις οποίες παρακολουθούν και μετρούν την αποτελεσματικότητα της εφαρμογής της στρατηγικής ΤΠΕ. Οι ως άνω διαδικασίες επανεξετάζονται και επικαιροποιούνται σε τακτική βάση.

Άρθρο 5
(25η κατευθυντήρια γραμμή)
Εξωτερική ανάθεση υπηρεσιών ΤΠΕ και συστημάτων ΤΠΕ

1. Με την επιφύλαξη των καθοριζομένων στην ΠΕΕ 180/3/17.12.2020 «Υιοθέτηση Κατευθυντήριων Γραμμών της Ευρωπαϊκής Αρχής Ασφαλίσεων και Επαγγελματικών Συντάξεων (EIOPA) σχετικά με την εξωτερική ανάθεση δραστηριοτήτων σε παρόχους υπηρεσιών υπολογιστικού νέφους (EIOPA-BoS-20-002)», οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις διασφαλίζουν ότι σε περιπτώσεις εξωτερικής ανάθεσης των υπηρεσιών ΤΠΕ και των συστημάτων ΤΠΕ πληρούνται οι σχετικές απαιτήσεις για την υπηρεσία ΤΠΕ ή το σύστημα ΤΠΕ.

2. Σε περίπτωση εξωτερικής ανάθεσης κρίσιμων ή σημαντικών λειτουργιών και προκειμένου να διασφαλίζεται η συνέχεια των υπηρεσιών ΤΠΕ και των συστημάτων ΤΠΕ, οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις διασφαλίζουν ότι οι συμβάσεις και τα συμβόλαια διασφάλισης επιπέδου ποιότητας υπηρεσιών, τόσο υπό κανονικές συνθήκες όσο και σε περίπτωση διαταραχής των υπηρεσιών, που συνάπτονται με παρόχους υπηρεσιών περιλαμβάνουν, τουλάχιστον, τα ακόλουθα:

α) κατάλληλους και αναλογικούς στόχους και μέτρα που αφορούν την ασφάλεια πληροφοριών, συμπεριλαμβανομένων απαιτήσεων, όπως ελάχιστες απαιτήσεις ασφάλειας, προδιαγραφές του κύκλου ζωής των δεδομένων των ασφαλιστικών και αντασφαλιστικών επιχειρήσεων, δικαιώματα ελέγχου και πρόσβασης και τυχόν απαιτήσεις σχετικά με την τοποθεσία των μηχανογραφικών κέντρων και απαιτήσεις σχετικά με την κρυπτογράφηση των δεδομένων, διεργασίες ασφάλειας δικτύου και παρακολούθησης της ασφάλειας,

β) διαδικασίες χειρισμού περιστατικών λειτουργικού κινδύνου και περιστατικών ασφάλειας, συμπεριλαμβανομένης της υποβολής αναφορών και της παραπομπής σε ανώτερη βαθμίδα της ιεραρχικής κλίμακας.

3. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις παρακολουθούν και αναζητούν από τους παρόχους υπηρεσιών διαβεβαίωση για το κατάλληλο επίπεδο συμμόρφωσής τους με τους αντικειμενικούς σκοπούς, τα μέτρα και τους στόχους επιδόσεών τους όσον αφορά την ασφάλεια.

Άρθρο 6
(4η κατευθυντήρια γραμμή)
Κίνδυνοι ΤΠΕ και ασφάλειας εντός του συστήματος διαχείρισης κινδύνων

1. Το Διοικητικό Συμβούλιο έχει τη συνολική ευθύνη να θεσπίζει αποτελεσματικό σύστημα διαχείρισης των κινδύνων ΤΠΕ και ασφάλειας στο πλαίσιο του συστήματος διαχείρισης κινδύνων των ασφαλιστικών και αντασφαλιστικών επιχειρήσεων. Το πλαίσιο αυτό περιλαμβάνει τον προσδιορισμό του επιπέδου ανοχής (risk tolerance) των εν λόγω κινδύνων, σύμφωνα με τη συνολική στρατηγική κινδύνων της ασφαλιστικής ή αντασφαλιστικής επιχείρησης, καθώς και την υποβολή τακτικής γραπτής αναφοράς σχετικά με το αποτέλεσμα της διαδικασίας διαχείρισης κινδύνων προς το Διοικητικό Συμβούλιο.

2. Στο πλαίσιο του συνολικού συστήματος διαχείρισης κινδύνων, οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις προβαίνουν, όσον αφορά στους κινδύνους ΤΠΕ και ασφάλειας (και ενώ καθορίζουν τις απαιτήσεις προστασίας ΤΠΕ, όπως περιγράφονται κατωτέρω), τουλάχιστον στα ακόλουθα:

α) καταρτίζουν και επικαιροποιούν τακτικά τη χαρτογράφηση των επιχειρηματικών τους διεργασιών και δραστηριοτήτων, επιχειρηματικών λειτουργιών, ρόλων και πόρων (π.χ. πληροφοριακών πόρων και πόρων ΤΠΕ) ώστε να προσδιορίζεται η σημασία κάθε επιμέρους επιχειρηματικής λειτουργίας, ρόλου και διεργασίας, καθώς και των αλληλεξαρτήσεών τους, σε σχέση με τους κινδύνους ΤΠΕ και ασφάλειας,

β) αναγνωρίζουν και μετρούν όλους τους συναφείς κινδύνους ΤΠΕ και ασφάλειας στους οποίους εκτίθενται και κατηγοριοποιούν τις ως άνω επιχειρηματικές διεργασίες και δραστηριότητες, λειτουργίες, ρόλους και πόρους (π.χ. πληροφοριακούς πόρους και πόρους ΤΠΕ) βάσει της κρισιμότητάς τους. Για τον καθορισμό της κρισιμότητας των εν λόγω προσδιοριζόμενων επιχειρηματικών διεργασιών και δραστηριοτήτων, λειτουργιών, ρόλων και πόρων (π.χ. των πληροφοριακών πόρων και των πόρων ΤΠΕ), οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις λαμβάνουν υπόψη, κατ’ ελάχιστον, τις απαιτήσεις προστασίας, της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Οι κάτοχοι πόρων, οι οποίοι φέρουν ευθύνη και λογοδοτούν για την κατηγοριοποίηση των πόρων, πρέπει να προσδιορίζονται,

γ) χρησιμοποιούν μεθόδους για τον καθορισμό του επιπέδου κρισιμότητας, καθώς και του απαιτούμενου επιπέδου προστασίας, ιδίως όσον αφορά τους στόχους προστασίας της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας, οι οποίες διασφαλίζουν ότι οι προκύπτουσες απαιτήσεις προστασίας είναι συνεκτικές και περιλαμβάνουν κάθε πιθανή πτυχή,

δ) διενεργούν μέτρηση των κινδύνων ΤΠΕ και ασφάλειας βάσει καθορισμένων κριτηρίων κινδύνων ΤΠΕ και ασφάλειας, λαμβάνοντας υπόψη το επίπεδο κρισιμότητας των επιχειρηματικών τους διεργασιών και δραστηριοτήτων, επιχειρηματικών λειτουργιών, ρόλων και πόρων (π.χ. πληροφοριακών πόρων και πόρων ΤΠΕ), την έκταση των γνωστών τρωτών σημείων και προηγούμενων συμβάντων που επηρέασαν την επιχείρηση,

ε) διενεργούν και τεκμηριώνουν αξιολόγηση των κινδύνων ΤΠΕ και ασφάλειας σε τουλάχιστον ετήσια βάση. Η εν λόγω αξιολόγηση κινδύνων διενεργείται πριν από οποιαδήποτε σημαντική αλλαγή στην υποδομή, τις διεργασίες ή τις διαδικασίες που επηρεάζουν τις επιχειρηματικές διεργασίες και δραστηριότητες, λειτουργίες, ρόλους και πόρους (π.χ. πληροφοριακούς πόρους και πόρους ΤΠΕ),

στ) καθορίζουν και εφαρμόζουν, βάσει της αξιολόγησης κινδύνων, μέτρα για τη διαχείριση των προσδιοριζόμενων κινδύνων ΤΠΕ και ασφάλειας και για την προστασία των πληροφοριακών πόρων βάσει της κατηγοριοποίησής τους. Αυτό περιλαμβάνει τον ορισμό μέτρων για τη διαχείριση των υπολειπόμενων κινδύνων.

3. Τα αποτελέσματα της διαδικασίας διαχείρισης κινδύνων ΤΠΕ και ασφάλειας εγκρίνονται από το Διοικητικό Συμβούλιο και συμπεριλαμβάνονται στη διαδικασία διαχείρισης λειτουργικού κινδύνου στο πλαίσιο της συνολικής διαχείρισης κινδύνων των ασφαλιστικών και αντασφαλιστικών επιχειρήσεων.

Άρθρο 7
Εσωτερικός Έλεγχος
(5η κατευθυντήρια γραμμή)

Η διακυβέρνηση, τα συστήματα και οι διεργασίες των ασφαλιστικών και αντασφαλιστικών επιχειρήσεων ως προς τους κινδύνους ΤΠΕ και ασφάλειας υπόκεινται σε διαδικασία εσωτερικού ελέγχου σε περιοδική βάση σύμφωνα με το πρόγραμμα ελέγχων των επιχειρήσεων από ελεγκτές με επαρκείς γνώσεις, δεξιότητες και εξειδίκευση σε θέματα κινδύνων ΤΠΕ και ασφάλειας, ώστε να παρέχεται στο Διοικητικό Συμβούλιο ανεξάρτητη διαβεβαίωση όσον αφορά την αποτελεσματικότητά τους. Η συχνότητα και το σημείο εστίασης των εν λόγω ελέγχων είναι ανάλογα προς τους αντίστοιχους κινδύνους ΤΠΕ και ασφάλειας.

Άρθρο 8
Πολιτική και μέτρα ασφάλειας πληροφοριών
(6η κατευθυντήρια γραμμή)

1. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις αναπτύσσουν και τεκμηριώνουν πολιτική ασφάλειας πληροφοριών, στην οποία καθορίζονται γενικές αρχές και κανόνες για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των πληροφοριών που διαθέτουν οι επιχειρήσεις για την υποστήριξη της υλοποίησης της στρατηγικής ΤΠΕ. Η πολιτική εγκρίνεται από το Διοικητικό Συμβούλιο.

2. Η πολιτική περιλαμβάνει περιγραφή των κύριων ρόλων και αρμοδιοτήτων της διαχείρισης ασφάλειας πληροφοριών και καθορίζει τις απαιτήσεις για το προσωπικό, τις διεργασίες και την τεχνολογία σε σχέση με την ασφάλεια πληροφοριών, αναγνωρίζοντας ότι το προσωπικό σε όλα τα επίπεδα έχει ευθύνες όσον αφορά τη διασφάλιση της ασφάλειας πληροφοριών των επιχειρήσεων.

3. Η πολιτική κοινοποιείται εντός της επιχείρησης και ισχύει για όλο το προσωπικό. Η πολιτική ασφάλειας πληροφοριών ή τμήματα αυτής κοινοποιούνται και ισχύουν, κατά περίπτωση, για τους παρόχους υπηρεσιών.

4. Βάσει της πολιτικής ασφάλειας πληροφοριών, οι επιχειρήσεις θεσπίζουν και εφαρμόζουν πιο συγκεκριμένες διαδικασίες ασφάλειας πληροφοριών καθώς και μέτρα ασφάλειας πληροφοριών, μεταξύ άλλων για τη μείωση των κινδύνων ΤΠΕ και ασφάλειας στους οποίους εκτίθενται. Οι εν λόγω διαδικασίες και τα μέτρα ασφάλειας πληροφοριών περιλαμβάνουν κάθε διαδικασία που περιγράφεται στην παρούσα πράξη κατά περίπτωση.

Άρθρο 9
Λειτουργία ασφάλειας πληροφοριών
(7η κατευθυντήρια γραμμή)

1. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις διαθέτουν στο σύστημα διακυβέρνησής τους λειτουργία ασφάλειας πληροφοριών, η οποία λειτουργεί στη βάση της αρχής της αναλογικότητας, και αναθέτουν την ευθύνη των εργασιών που περιλαμβάνονται στην εν λόγω λειτουργία σε ένα πρόσωπο. Η επιχείρηση διασφαλίζει την ανεξαρτησία και την αντικειμενικότητα της λειτουργίας ασφάλειας πληροφοριών, διαχωρίζοντάς την δεόντως

από τις διεργασίες ανάπτυξης και λειτουργιών των ΤΠΕ. Το πρόσωπο που είναι υπεύθυνο για τις εργασίες που περιλαμβάνονται στην εν λόγω λειτουργία αναφέρεται και λογοδοτεί στο Διοικητικό Συμβούλιο.

2. Η λειτουργία ασφάλειας πληροφοριών περιλαμβάνει τουλάχιστον τις ακόλουθες εργασίες:

α) υποστήριξη του Διοικητικού Συμβουλίου κατά τον καθορισμό και τη διατήρηση της πολιτικής ασφάλειας πληροφοριών για τις επιχειρήσεις και έλεγχο της εφαρμογής της,

β) ενημέρωση και παροχή συμβουλών στο Διοικητικό Συμβούλιο σε τακτική και έκτακτη βάση όσον αφορά την κατάσταση της ασφάλειας πληροφοριών καθώς και τις εξελίξεις στον τομέα αυτό,

γ) παρακολούθηση και έλεγχο των μέτρων για την ασφάλεια πληροφοριών,

δ) διασφάλιση της τήρησης των απαιτήσεων ασφάλειας πληροφοριών κατά τη χρήση παρόχων υπηρεσιών,

ε) διασφάλιση ότι όλοι οι υπάλληλοι και οι πάροχοι υπηρεσιών που έχουν πρόσβαση σε πληροφορίες και συστήματα είναι επαρκώς ενημερωμένοι για την πολιτική ασφάλειας πληροφοριών, για παράδειγμα μέσω συνεδριών κατάρτισης και ενημέρωσης σχετικά με την ασφάλεια πληροφοριών,

στ) συντονισμός της αξιολόγησης περιστατικών λειτουργίας ή ασφαλείας και σχετική υποβολή αναφορών στο Διοικητικό Συμβούλιο.

Άρθρο 10
(8η κατευθυντήρια γραμμή)
Λογική ασφάλεια

1. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις καθορίζουν, τεκμηριώνουν και εφαρμόζουν διαδικασίες για τον έλεγχο της λογικής πρόσβασης ή της λογικής ασφάλειας (διαχείριση στοιχείων ταυτότητας και πρόσβασης) σύμφωνα με τις απαιτήσεις προστασίας, λαμβάνοντας υπόψη τα αποτελέσματα της αξιολόγησης κινδύνων σύμφωνα με όσα ορίζονται στο άρθρο 6 της παρούσας. Οι διαδικασίες αυτές εφαρμόζονται, επιβάλλονται και παρακολουθούνται, ενώ επανεξετάζονται σε τακτική βάση. Οι διαδικασίες περιλαμβάνουν επίσης ελέγχους για την παρακολούθηση ασυνήθιστων ενεργειών. Στο πλαίσιο των εν λόγω διαδικασιών πρέπει κατ’ ελάχιστον να εφαρμόζονται τα ακόλουθα στοιχεία, λαμβάνοντας υπόψη ότι ο όρος «χρήστης» περιλαμβάνει επίσης τεχνικούς χρήστες:

α) ελάχιστη απαιτούμενη πληροφόρηση, ελάχιστα προνόμια και διαχωρισμός καθηκόντων: οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις διαχειρίζονται τα δικαιώματα πρόσβασης σε πληροφοριακούς πόρους και τα υποστηρικτικά συστήματά τους, συμπεριλαμβανομένης της απομακρυσμένης πρόσβασης, βάσει της αρχής της «ελάχιστης απαιτούμενης πληροφόρησης». Στους χρήστες χορηγούνται ελάχιστα δικαιώματα πρόσβασης τα οποία είναι απολύτως απαραίτητα για την εκτέλεση των καθηκόντων τους (αρχή των «ελάχιστων προνομίων»), δηλαδή αποτρέπεται η αδικαιολόγητη πρόσβαση σε μεγάλο εύρος δεδομένων ή η χορήγηση συνδυασμένων δικαιωμάτων πρόσβασης που θα μπορούσαν να χρησιμοποιηθούν για την παράκαμψη δικλείδων ασφαλείας (αρχή του «διαχωρισμού των καθηκόντων»),

β) ευθύνη και λογοδοσία χρήστη: οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις περιορίζουν/στο μέγιστο δυνατό βαθμό τη χρήση γενικών και κοινών λογαριασμών χρηστών και διασφαλίζουν τη δυνατότητα ταυτοποίησης των χρηστών για τις ενέργειες που πραγματοποιούνται στα συστήματα ΤΠΕ ανά πάσα στιγμή,

γ) δικαιώματα διαβαθμισμένης πρόσβασης: οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις εφαρμόζουν ισχυρές δικλείδες ασφαλείας για τη διαβαθμισμένη πρόσβαση στα συστήματά τους, περιορίζοντας αυστηρά την πρόσβαση και παρακολουθώντας επισταμένως τους λογαριασμούς με αυξημένα δικαιώματα πρόσβασης στα εν λόγω συστήματα (π.χ. λογαριασμούς διαχειριστών),

δ) απομακρυσμένη πρόσβαση: για την εξασφάλιση ασφαλούς επικοινωνίας και τη μείωση του κινδύνου, η απομακρυσμένη διαχειριστική πρόσβαση σε κρίσιμα συστήματα ΤΠΕ επιτρέπεται μόνο με βάση την αρχή της «ελάχιστης απαιτούμενης πληροφόρησης» και εφόσον χρησιμοποιούνται διαδικασίες αυστηρής αυθεντικοποίησης,

ε) καταγραφή της δραστηριότητας των χρηστών: κατ’ ελάχιστον καταγράφονται και παρακολουθούνται όλες οι δραστηριότητες των προνομιούχων χρηστών. Τα αρχεία καταγραφής πρόσβασης προστατεύονται από μη εξουσιοδοτημένη τροποποίηση ή διαγραφή και διατηρούνται για χρονικό διάστημα ανάλογο της κρισιμότητας των επιχειρηματικών διεργασιών και δραστηριοτήτων, των επιχειρηματικών λειτουργιών και των πληροφοριακών πόρων, με την επιφύλαξη των απαιτήσεων διατήρησης που προβλέπονται στο ευρωπαϊκό και εθνικό δίκαιο. Οι επιχειρήσεις χρησιμοποιούν τις εν λόγω πληροφορίες για να διευκολύνουν την αναγνώριση και τη διερεύνηση ασυνήθιστων δραστηριοτήτων που έχουν εντοπιστεί κατά την παροχή υπηρεσιών,

στ) διαχείριση πρόσβασης: τα δικαιώματα πρόσβασης χορηγούνται, ανακαλούνται ή τροποποιούνται εγκαίρως, σύμφωνα με προκαθορισμένες εγκριτικές ροές εργασίας, στις οποίες συμμετέχει ο ιδιοκτήτης του πληροφοριακού πόρου. Σε περίπτωση που δεν απαιτείται πλέον πρόσβαση, τα δικαιώματα πρόσβασης ανακαλούνται άμεσα,

ζ) επανεξέταση πρόσβασης: τα δικαιώματα πρόσβασης επανεξετάζονται σε περιοδική βάση ώστε να διασφαλίζεται ότι οι χρήστες δεν διαθέτουν υπερβολικά προνόμια και ότι τα δικαιώματα πρόσβασης ανακαλούνται όταν δεν είναι πλέον απαραίτητα,

η) η χορήγηση, τροποποίηση και ανάκληση δικαιωμάτων πρόσβασης τεκμηριώνονται κατά τρόπο που διευκολύνει την κατανόηση και την ανάλυση αυτών, και

θ) μέθοδοι αυθεντικοποίησης: οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις επιβάλλουν μεθόδους αυθεντικοποίησης επαρκώς αξιόπιστες ώστε να διασφαλίζεται με κατάλληλο και αποτελεσματικό τρόπο η συμμόρφωση προς τις πολιτικές και τις διαδικασίες ελέγχου της πρόσβασης. Οι μέθοδοι αυθεντικοποίησης είναι ανάλογες προς τον βαθμό κρισιμότητας των συστημάτων ΤΠΕ, των πληροφοριών ή των διεργασιών

που αποτελούν αντικείμενο πρόσβασης. Στο πλαίσιο αυτό περιλαμβάνονται, κατ’ ελάχιστον, σύνθετοι κωδικοί πρόσβασης ή ισχυρότερες μέθοδοι αυθεντικοποίησης (όπως η αυθεντικοποίηση δύο παραγόντων), βάσει του αντίστοιχου κινδύνου.

2. Η ηλεκτρονική πρόσβαση από εφαρμογές σε δεδομένα και συστήματα ΤΠΕ περιορίζεται στο ελάχιστο επίπεδο που απαιτείται για την παροχή της αντίστοιχης υπηρεσίας.

Άρθρο 11
(9η κατευθυντήρια γραμμή)
Φυσική ασφάλεια

1. Τα μέτρα φυσικής ασφάλειας των ασφαλιστικών και αντασφαλιστικών επιχειρήσεων (ενδεικτικά προστασία έναντι διακοπής ρεύματος, πυρκαγιάς, πλημμύρας και μη εξουσιοδοτημένης φυσικής πρόσβασης), καθορίζονται, τεκμηριώνονται και εφαρμόζονται με σκοπό την προστασία των εγκαταστάσεων, των μηχανογραφικών κέντρων και των ευαίσθητων χώρων από μη εξουσιοδοτημένη πρόσβαση και από περιβαλλοντικούς κινδύνους.

2. Η φυσική πρόσβαση σε συστήματα ΤΠΕ επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα. Η εξουσιοδότηση παρέχεται ανάλογα με τα καθήκοντα και τις αρμοδιότητες του ατόμου και περιορίζεται σε άτομα που υποβάλλονται σε κατάλληλη εκπαίδευση και παρακολούθηση. Η φυσική πρόσβαση επανεξετάζεται σε τακτική βάση ώστε να διασφαλίζεται η άμεση ανάκληση μη αναγκαίων δικαιωμάτων πρόσβασης όταν αυτά δεν είναι απαραίτητα.

3. Τα ενδεδειγμένα μέτρα για την προστασία από περιβαλλοντικούς κινδύνους και κακόβουλες ενέργειες είναι ανάλογα προς τη σημασία των κτιρίων και την κρισιμότητα των επιχειρηματικών λειτουργιών ή των συστημάτων ΤΠΕ που βρίσκονται στα εν λόγω κτίρια.

Άρθρο 12
(10η κατευθυντήρια γραμμή)
Ασφάλεια λειτουργιών ΤΠΕ

Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις εφαρμόζουν διαδικασίες για την διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των συστημάτων ΤΠΕ και των υπηρεσιών ΤΠΕ, προκειμένου να ελαχιστοποιούνται αντίστοιχα οι επιπτώσεις των ζητημάτων ασφάλειας στην παροχή υπηρεσιών ΤΠΕ. Στις διαδικασίες αυτές περιλαμβάνονται δεόντως τα ακόλουθα μέτρα:

α) εντοπισμός πιθανών ευπαθειών, οι οποίες αξιολογούνται και αποκαθίστανται διασφαλίζοντας ότι το λογισμικό και το υλικολογισμικό των συστημάτων, καθώς και το λογισμικό που παρέχουν οι επιχειρήσεις στους εσωτερικούς και τους εξωτερικούς χρήστες τους, είναι ενημερωμένα, εγκαθιστώντας κρίσιμες ενημερώσεις ασφάλειας, περιλαμβανομένων ενημερώσεων για αντιϊκή προστασία ή εφαρμόζοντας αντισταθμιστικούς ελέγχους,

β) εφαρμογή βασικών γραμμών (baseline) ασφαλούς παραμετροποίησης των δικτυακών στοιχείων,

γ) υλοποίηση κατάτμησης δικτύου (network segmentation), συστημάτων πρόληψης απώλειας δεδομένων (data loss prevention) και κρυπτογράφηση της κίνησης του δικτύου (σύμφωνα με την κατηγοριοποίηση του πληροφοριακού πόρου),

δ) εφαρμογή της προστασίας των τελικών σημείων (endpoint), συμπεριλαμβανομένων διακομιστών, σταθμών εργασίας και φορητών συσκευών. Οι ασφαλιστικές και αντασφαλιστικές αξιολογούν αν τα τελικά σημεία πληρούν τα πρότυπα ασφάλειας τα οποία έχουν ορισθεί από τις ίδιες τις επιχειρήσεις πριν χορηγηθεί σε αυτά πρόσβαση στο εταιρικό δίκτυο,

ε) εξασφάλιση της εφαρμογής μηχανισμών για την επαλήθευση της ακεραιότητας των ΤΠΕ συστημάτων,

στ) κρυπτογράφηση των δεδομένων όταν αποθηκεύονται και όταν διαβιβάζονται (σύμφωνα με την κατηγοριοποίηση των πληροφοριακών πόρων).

Άρθρο 13
(11η κατευθυντήρια γραμμή)
Παρακολούθηση ασφάλειας

1. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις θεσπίζουν και εφαρμόζουν λειτουργίες και διαδικασίες με αντικείμενο την συνεχή παρακολούθηση των ενεργειών που επηρεάζουν την ασφάλεια των πληροφοριών τους. Οι διεργασίες συνεχούς παρακολούθησης καλύπτουν τουλάχιστον:

α) συναφείς εσωτερικούς και εξωτερικούς παράγοντες, συμπεριλαμβανομένων διαχειριστικών λειτουργιών τόσο επιχειρηματικών όσο και ΤΠΕ,

β) συναλλαγές ή κινήσεις τόσο από παρόχους υπηρεσιών/τρίτους ή άλλες οντότητες όσο και από εσωτερικούς χρήστες, και

γ) πιθανές εσωτερικές και εξωτερικές απειλές.

2. Βάσει της παρακολούθησης, οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις εφαρμόζουν κατάλληλες και αποτελεσματικές διαδικασίες εντοπισμού, αναφοράς και ανταπόκρισης σε ασυνήθιστες δραστηριότητες και απειλές, όπως φυσική ή λογική εισβολή, παραβιάσεις της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας πληροφοριακών πόρων, κακόβουλο κώδικα και ευρέως γνωστές ευπάθειες λογισμικού και υλικού.

3. Η διαδικασία παρακολούθησης της ασφάλειας πρέπει να είναι τέτοιας μορφής ώστε να βοηθά τις επιχειρήσεις να κατανοούν τη φύση των περιστατικών λειτουργικού κινδύνου ή των περιστατικών ασφαλείας, να αναγνωρίζουν τάσεις και να στηρίζουν τις έρευνες των επιχειρήσεων και να τους επιτρέπει να λαμβάνουν τις κατάλληλες αποφάσεις.

Άρθρο 14
(12η κατευθυντήρια γραμμή)
Επανεξετάσεις, αξιολογήσεις και δοκιμές της ασφάλειας πληροφοριών

1. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις διενεργούν ποικίλων ειδών επανεξετάσεις, αξιολογήσεις και δοκιμές της ασφάλειας πληροφοριών, ώστε να διασφαλίζεται η αποτελεσματική αναγνώριση ευπαθειών στα συστήματα ΤΠΕ και στις υπηρεσίες ΤΠΕ των επιχειρήσεων. Για παράδειγμα, οι επιχειρήσεις μπορούν να διενεργούν ανάλυση ελλείψεων (gap analysis) με βάση

τα πρότυπα ασφάλειας πληροφοριών, ελέγχους συμμόρφωσης, εσωτερικούς και εξωτερικούς ελέγχους των συστημάτων ΤΠΕ ή ελέγχους φυσικής ασφάλειας.

2. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις θεσπίζουν και εφαρμόζουν πλαίσιο δοκιμών ασφάλειας πληροφοριών, το οποίο επικυρώνει την αξιοπιστία και την αποτελεσματικότητα των οικείων μέτρων ασφάλειας πληροφοριών και διασφαλίζουν ότι στο εν λόγω πλαίσιο λαμβάνονται υπόψη απειλές και ευπάθειες, οι οποίες έχουν προσδιοριστεί μέσω της παρακολούθησης απειλών και της διαδικασίας αξιολόγησης κινδύνων ΤΠΕ και ασφάλειας.

3. Το πλαίσιο δοκιμών ασφάλειας πληροφοριών διασφαλίζει ότι οι δοκιμές διενεργούνται από ανεξάρτητους φορείς διεξαγωγής δοκιμών που διαθέτουν επαρκείς γνώσεις, δεξιότητες και εξειδίκευση στη διενέργεια δοκιμών όσον αφορά μέτρα ασφάλειας πληροφοριών και οι οποίοι δεν εμπλέκονται στην ανάπτυξη των μέτρων ασφάλειας πληροφοριών.

4. Οι επιχειρήσεις διενεργούν δοκιμές σε τακτική βάση. Το εύρος, η συχνότητα και η μέθοδος δοκιμών (μεταξύ των οποίων και δοκιμές παρείσδυσης βάσει απειλών όπου κρίνεται αναγκαίο και σκόπιμο) είναι ανάλογα με το επίπεδο του κινδύνου που προσδιορίζεται σε σχέση με τις επιχειρηματικές διεργασίες και τα συστήματα. Οι δοκιμές παρείσδυσης για το σύνολο των κρίσιμων συστημάτων ΤΠΕ και οι έλεγχοι ευπαθειών διενεργούνται τουλάχιστον σε ετήσια βάση.

5. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις διασφαλίζουν ότι οι δοκιμές των μέτρων ασφάλειας διενεργούνται σε περίπτωση αλλαγών στην υποδομή, στις διεργασίες ή στις διαδικασίες, καθώς και σε περίπτωση αλλαγών λόγω μειζόνων περιστατικών λειτουργικού κινδύνου ή μειζόνων περιστατικών ασφάλειας ή λόγω της έκδοσης νέων ή σημαντικά τροποποιημένων κρίσιμων εφαρμογών διαδικτύου. Οι επιχειρήσεις παρακολουθούν και αξιολογούν τα αποτελέσματα των δοκιμών ασφάλειας και επικαιροποιούν αναλόγως και χωρίς αδικαιολόγητες καθυστερήσεις τα μέτρα ασφάλειάς τους στην περίπτωση των κρίσιμων συστημάτων ΤΠΕ.

Άρθρο 15
(13η κατευθυντήρια γραμμή)
Κατάρτιση και ευαισθητοποίηση σε θέματα ασφάλειας πληροφοριών

1. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις εφαρμόζουν εκπαιδευτικό πρόγραμμα σε θέματα ασφάλειας πληροφοριών για όλο το προσωπικό, συμπεριλαμβανομένων των μελών του Διοικητικού Συμβουλίου καθώς και για τους αναδόχους έργων, προκειμένου να διασφαλίζεται η επαρκής κατάρτισή τους για την άσκηση των καθηκόντων και των αρμοδιοτήτων τους, σύμφωνα με τις σχετικές πολιτικές και διαδικασίες ασφάλειας για τη μείωση των φαινομένων ανθρώπινου σφάλματος, κλοπής, απάτης, κατάχρησης ή απώλειας. Οι επιχειρήσεις διασφαλίζουν ότι το εκπαιδευτικό πρόγραμμα παρέχει κατάρτιση για το σύνολο των μελών του προσωπικού σε τακτική βάση.

2. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις εφαρμόζουν περιοδικά προγράμματα ευαισθητοποίησης σε θέματα ασφάλειας για την εκπαίδευση του προσωπικού τους, συμπεριλαμβανομένων των μελών του Διοικητικού Συμβουλίου, σχετικά με τον τρόπο αντιμετώπισης κινδύνων που σχετίζονται με την ασφάλεια πληροφοριών.

Άρθρο 16
(14η κατευθυντήρια γραμμή)
Διαχείριση λειτουργιών ΤΠΕ

1. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις διαχειρίζονται τις σχετικές με τις ΤΠΕ δραστηριότητές τους βάσει της στρατηγικής ΤΠΕ και καθορίζουν σε σχετικά έγγραφα τον τρόπο με τον οποίο διασφαλίζουν την λειτουργία, την παρακολούθηση και τον έλεγχο των συστημάτων και των υπηρεσιών ΤΠΕ, συμπεριλαμβανομένων των κρίσιμων διεργασιών, διαδικασιών και λειτουργιών ΤΠΕ.

2. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις εφαρμόζουν διαδικασίες καταγραφής και παρακολούθησης για τις κρίσιμες λειτουργίες ΤΠΕ, ώστε να είναι εφικτή η ανίχνευση, η ανάλυση και η διόρθωση σφαλμάτων.

3. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις τηρούν πλήρη και ενήμερο κατάλογο των ΤΠΕ πόρων τους. Ο κατάλογος πόρων ΤΠΕ είναι επαρκώς λεπτομερής ώστε να παρέχεται η δυνατότητα άμεσου προσδιορισμού του πόρου ΤΠΕ, της θέσης του, της κατηγοριοποίησης ασφάλειας του καθεστώτος ιδιοκτησίας του καθώς και των αλληλεξαρτήσεων με άλλους πόρους ΤΠΕ.

4. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις παρακολουθούν και διαχειρίζονται τον κύκλο ζωής των πόρων ΤΠΕ ώστε να διασφαλίζεται ότι εξακολουθούν να πληρούν και να υποστηρίζουν τις απαιτήσεις διαχείρισης των επιχειρηματικών δραστηριοτήτων και των κινδύνων τους. Οι επιχειρήσεις παρακολουθούν κατά πόσο οι ΤΠΕ πόροι τους υποστηρίζονται από τους εξωτερικούς ή εσωτερικούς προμηθευτές και σχεδιαστές εφαρμογών, καθώς και αν όλες οι σχετικές ενημερώσεις και αναβαθμίσεις εφαρμόζονται βάσει τεκμηριωμένων διαδικασιών. Οι κίνδυνοι που απορρέουν από παρωχημένους ή μη υποστηριζόμενους πόρους ΤΠΕ αξιολογούνται και περιορίζονται. Οι αποσυρθέντες πόροι ΤΠΕ υποβάλλονται σε ασφαλή επεξεργασία και διαγραφή.

5. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις εφαρμόζουν διαδικασίες σχεδιασμού και παρακολούθησης των επιδόσεων και της χωρητικότητας με σκοπό την έγκαιρη πρόληψη, ανίχνευση και αντιμετώπιση σημαντικών ζητημάτων όσον αφορά τις επιδόσεις των συστημάτων και τις ελλείψεις χωρητικότητας των συστημάτων ΤΠΕ.

6. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις καθορίζουν και εφαρμόζουν διαδικασίες δημιουργίας εφεδρικών αντιγράφων και αποκατάστασης δεδομένων και συστημάτων ΤΠΕ, ώστε να διασφαλίζεται η δυνατότητα ανάκτησής τους σύμφωνα με τις απαιτήσεις. Το πεδίο εφαρμογής και η συχνότητα της δημιουργίας εφεδρικών αντιγράφων καθορίζονται σύμφωνα με τις απαιτήσεις επιχειρησιακής ανάκαμψης και την κρισιμότητα των δε-

δομένων και των συστημάτων ΤΠΕ και αξιολογούνται με βάση τη διενεργηθείσα αξιολόγηση κινδύνων. Οι δοκιμές των διαδικασιών δημιουργίας εφεδρικών αντιγράφων και αποκατάστασης διενεργούνται σε περιοδική βάση.

7. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις διασφαλίζουν ότι τα εφεδρικά αντίγραφα δεδομένων και συστημάτων ΤΠΕ αποθηκεύονται με ασφάλεια και σε αρκετά απομακρυσμένη τοποθεσία από τον κύριο χώρο, ώστε να μην εκτίθενται στους ίδιους κινδύνους.

Άρθρο 17
(15η κατευθυντήρια γραμμή)
Διαχείριση περιστατικών και προβλημάτων ΤΠΕ

1. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις δημιουργούν και εφαρμόζουν διαδικασία διαχείρισης περιστατικών και προβλημάτων για την παρακολούθηση και την καταγραφή περιστατικών λειτουργικού κινδύνου και περιστατικών ασφάλειας ΤΠΕ, καθώς και για να εξασφαλίζεται η δυνατότητά τους να συνεχίζουν ή να επανεκκινούν εγκαίρως τις κρίσιμες επιχειρηματικές λειτουργίες και διεργασίες σε περίπτωση εμφάνισης δυσλειτουργιών.

2. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις καθορίζουν κατάλληλα κριτήρια και κατώτατα όρια για την κατηγοριοποίηση συμβάντων ως περιστατικών λειτουργικού κινδύνου ή περιστατικών ασφάλειας, καθώς και δείκτες έγκαιρης προειδοποίησης που θα χρησιμεύουν ως ειδοποιήσεις, ώστε να καθίσταται δυνατός ο έγκαιρος εντοπισμός των εν λόγω περιστατικών.

3. Για την ελαχιστοποίηση των επιπτώσεων δυσμενών συμβάντων και την εξασφάλιση της δυνατότητας έγκαιρης ανάκαμψης, οι επιχειρήσεις εφαρμόζουν κατάλληλες διεργασίες και οργανωτικές δομές για τη διασφάλιση συνεκτικής και ολοκληρωμένης παρακολούθησης, διαχείρισης και επανεξέτασης των περιστατικών λειτουργικού κινδύνου και των περιστατικών ασφάλειας, για τη διασφάλιση του προσδιορισμού και της αντιμετώπισης των βασικών αιτιών με σκοπό την αποτροπή επαναλαμβανόμενων περιστατικών και για τη λήψη διορθωτικών μέτρων με σκοπό την αποφυγή παρόμοιων συμβάντων στο μέλλον. Στη διαδικασία διαχείρισης περιστατικών και προβλημάτων καθορίζονται τουλάχιστον τα ακόλουθα:

α) οι διαδικασίες για τον προσδιορισμό, την ανίχνευση, την καταγραφή, την κατηγοριοποίηση και την ταξινόμηση των περιστατικών βάσει προτεραιοποίησης ανάλογα με την κρισιμότητα των επιχειρησιακών λειτουργιών και των συμβάσεων παροχής υπηρεσιών,

β) οι ρόλοι και οι αρμοδιότητες για τα διάφορα σενάρια περιστατικών (π.χ. σφάλματα, δυσλειτουργίες, κυβερνο-επιθέσεις),

γ) διαδικασίες διαχείρισης προβλημάτων για την αναγνώριση, την ανάλυση και την επίλυση των βασικών αιτιών ενός ή περισσότερων περιστατικών: οι επιχειρήσεις αναλύουν τα περιστατικά λειτουργικού κινδύνου ή τα περιστατικά ασφάλειας που έχουν αναγνωριστεί ή έχουν ήδη εμφανιστεί εντός και/ή εκτός του οργανισμού, ενώ επίσης λαμβάνουν υπόψη τα κύρια διδάγματα που αντλούνται από τις εν λόγω αναλύσεις και επικαιροποιούν αναλόγως τα μέτρα ασφάλειας,

δ) αποτελεσματικά σχέδια εσωτερικής επικοινωνίας, συμπεριλαμβανομένων διαδικασιών γνωστοποίησης περιστατικών και παραπομπής σε ανώτερη βαθμίδα της ιεραρχικής κλίμακας - οι οποίες καλύπτουν επίσης καταγγελίες πελατών σχετικά με θέματα ασφάλειας - ώστε να διασφαλίζεται ότι:

i. τα περιστατικά με δυνητικά σοβαρές δυσμενείς επιπτώσεις σε συστήματα ΤΠΕ και υπηρεσίες ΤΠΕ κρίσιμης σημασίας αναφέρονται στα αρμόδια μέλη της διοίκησης,

ii. το Διοικητικό Συμβούλιο ενημερώνεται σε έκτακτη βάση σε περίπτωση σημαντικών περιστατικών και επίσης, κατ’ ελάχιστον, για τις επιπτώσεις, την αντιμετώπιση και τους πρόσθετους ελέγχους που πρέπει να καθοριστούν συνεπεία των περιστατικών,

ε) διαδικασίες αντιμετώπισης περιστατικών για τη μείωση των επιπτώσεων που συνδέονται με αυτά και για την εξασφάλιση της δυνατότητας έγκαιρης και ασφαλούς επαναλειτουργίας της υπηρεσίας,

στ) συγκεκριμένα σχέδια εξωτερικής επικοινωνίας για τις κρίσιμες επιχειρηματικές λειτουργίες και διεργασίες, με στόχο:

i. τη συνεργασία με τους σχετικούς ενδιαφερομένους για την αποτελεσματική αντιμετώπιση του περιστατικού και την ανάκαμψη μετά από αυτό,

ii. την έγκαιρη παροχή πληροφοριών, συμπεριλαμβανομένης της αναφοράς περιστατικών, σε εξωτερικά μέρη (π.χ. πελάτες, άλλους συμμετέχοντες στην αγορά, αρμόδιες εποπτικές αρχές), κατά περίπτωση και σύμφωνα με τις ισχύουσες κανονιστικές διατάξεις.

Άρθρο 18
(16η κατευθυντήρια γραμμή)
Διαχείριση έργων ΤΠΕ

1. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις εφαρμόζουν μεθοδολογία διακυβέρνησης έργων ΤΠΕ (συμπεριλαμβανομένων προδιαγραφών για θέματα ασφάλειας από ανεξάρτητη πηγή που θα πρέπει να ληφθούν υπόψη) για τον καθορισμό ρόλων, αρμοδιοτήτων και υποχρεώσεων λογοδοσίας με σκοπό την αποτελεσματική υποστήριξη της υλοποίησης της στρατηγικής ΤΠΕ μέσω των ΤΠΕ έργων.

2. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις μεριμνούν δεόντως για την παρακολούθηση και τον μετριασμό των κινδύνων που απορρέουν από το οικείο χαρτοφυλάκιο έργων ΤΠΕ, λαμβάνοντας επίσης υπόψη τους κινδύνους που ενδέχεται να προκύπτουν από αλληλεξαρτήσεις μεταξύ διαφόρων έργων και από την εξάρτηση πολλαπλών έργων από τους ίδιους ή/και ίδιας εξειδίκευσης πόρους.

Άρθρο 19
(17η κατευθυντήρια γραμμή)
Απόκτηση και ανάπτυξη συστημάτων ΤΠΕ

1. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις αναπτύσσουν και εφαρμόζουν διαδικασία η οποία διέπει την απόκτηση, την ανάπτυξη και τη συντήρηση των συστημάτων ΤΠΕ προκειμένου να διασφαλίζεται ότι η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα των προς επεξεργασία δεδομένων διασφαλίζονται με

αναλυτικό τρόπο και ότι πληρούνται οι καθορισμένες απαιτήσεις προστασίας. Η διαδικασία αυτή σχεδιάζεται χρησιμοποιώντας προσέγγιση βάσει κινδύνου.

2. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις διασφαλίζουν ότι πριν από οποιαδήποτε απόκτηση ή ανάπτυξη συστημάτων ΤΠΕ, ορίζονται με σαφήνεια οι λειτουργικές και μη λειτουργικές απαιτήσεις (συμπεριλαμβανομένων των απαιτήσεων ασφάλειας πληροφοριών) καθώς και οι τεχνικοί στόχοι.

3. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις διασφαλίζουν ότι εφαρμόζονται μέτρα για τη μείωση του κινδύνου ακούσιας τροποποίησης ή εσκεμμένης παραποίησης των συστημάτων ΤΠΕ κατά τη διάρκεια της ανάπτυξης και υλοποίησης του περιβάλλοντος παραγωγής.

4. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις διαθέτουν μεθοδολογία για τις δοκιμές και την αποδοχή των συστημάτων ΤΠΕ πριν από την πρώτη χρήση τους, των υπηρεσιών ΤΠΕ και των μέτρων ασφάλειας των πληροφοριών.

5. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις υποβάλλουν σε δοκιμές τα συστήματα ΤΠΕ, τις υπηρεσίες ΤΠΕ και τα μέτρα ασφάλειας πληροφοριών για τον προσδιορισμό πιθανών αδυναμιών, παραβιάσεων και περιστατικών ασφάλειας.

6. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις μεριμνούν για τον διαχωρισμό των περιβαλλόντων παραγωγής από τα περιβάλλοντα ανάπτυξης, δοκιμών και άλλα μη παραγωγικά περιβάλλοντα.

7. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις εφαρμόζουν μέτρα για την προστασία της ακεραιότητας του πηγαίου κώδικα (όπου υπάρχει) των συστημάτων ΤΠΕ. Επίσης, τεκμηριώνουν την ανάπτυξη, την εφαρμογή, τη λειτουργία και/ή την παραμετροποίηση των συστημάτων ΤΠΕ κατά τρόπο ολοκληρωμένο, ώστε να περιορίζεται τυχόν αδικαιολόγητη εξάρτηση από ειδικούς επί του αντικειμένου αυτού. Η τεκμηρίωση του συστήματος ΤΠΕ περιλαμβάνει, κατά περίπτωση, τουλάχιστον την τεκμηρίωση για τον χρήστη, την τεχνική τεκμηρίωση του συστήματος και τις διαδικασίες λειτουργίας.

8. Οι διεργασίες των επιχειρήσεων για την απόκτηση και την ανάπτυξη συστημάτων ΤΠΕ εφαρμόζονται επίσης σε συστήματα ΤΠΕ των οποίων η ανάπτυξη ή η διαχείριση πραγματοποιείται από τους τελικούς χρήστες της επιχειρηματικής λειτουργίας εκτός της οργανωτικής δομής ΤΠΕ (π.χ. υπολογιστικές εφαρμογές τελικού χρήστη) σύμφωνα με μια προσέγγιση βάσει κινδύνου. Οι επιχειρήσεις τηρούν μητρώο των εν λόγω εφαρμογών που υποστηρίζουν κρίσιμες επιχειρηματικές λειτουργίες ή διεργασίες.

Άρθρο 20
(18η κατευθυντήρια γραμμή)
Διαχείριση αλλαγών ΤΠΕ

1. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις θεσπίζουν και εφαρμόζουν διαδικασία διαχείρισης αλλαγών ΤΠΕ ώστε να διασφαλίζεται ότι όλες οι αλλαγές στα συστήματα ΤΠΕ καταγράφονται, υποβάλλονται σε δοκιμές, αξιολογούνται, εγκρίνονται, υλοποιούνται και επαληθεύονται με ελεγχόμενο τρόπο. Οι επιχειρήσεις χειρίζονται τις αλλαγές κατά τη διάρκεια περιπτώσεων έκτακτης ανάγκης (δηλαδή αλλαγές που πρέπει να εφαρμοσθούν το συντομότερο δυνατόν) σύμφωνα με διαδικασίες που παρέχουν επαρκείς διασφαλίσεις.

2. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις προσδιορίζουν αν οι αλλαγές στο υφιστάμενο λειτουργικό περιβάλλον επηρεάζουν τα ισχύοντα μέτρα ασφάλειας ή απαιτούν τη λήψη πρόσθετων μέτρων για τον μετριασμό των αντίστοιχων κινδύνων. Οι αλλαγές αυτές πραγματοποιούνται σύμφωνα με την επίσημη διαδικασία διαχείρισης αλλαγών που εφαρμόζουν οι επιχειρήσεις.

Άρθρο 21
(19η κατευθυντήρια γραμμή)
Διαχείριση της επιχειρησιακής συνέχειας

Στο πλαίσιο της πολιτικής επιχειρησιακής συνέχειας της παρ. 3 του άρθρου 258 του Κανονισμού (ΕΕ) 2015/35 των ασφαλιστικών και αντασφαλιστικών επιχειρήσεων, το Διοικητικό Συμβούλιο έχει την ευθύνη για τον καθορισμό και την έγκριση της πολιτικής επιχειρησιακής συνέχειας ΤΠΕ των επιχειρήσεων. Η πολιτική επιχειρησιακής συνέχειας των ΤΠΕ κοινοποιείται δεόντως εντός των επιχειρήσεων και εφαρμόζεται από τα αρμόδια μέλη του προσωπικού και, κατά περίπτωση, από τους παρόχους υπηρεσιών.

Άρθρο 22
(20η κατευθυντήρια γραμμή)
Ανάλυση επιπτώσεων για τις επιχειρήσεις

1. Στο πλαίσιο της χρηστής διαχείρισης της επιχειρησιακής συνέχειας, οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις διενεργούν ανάλυση των επιχειρηματικών επιπτώσεων, αναλύοντας την έκθεσή τους σε σοβαρές διαταραχές της επιχειρηματικής δραστηριότητάς τους και αξιολογώντας τις πιθανές επιπτώσεις τους βάσει ποσοτικών και ποιοτικών κριτηρίων, χρησιμοποιώντας εσωτερικά ή/και εξωτερικά δεδομένα και ανάλυση σεναρίων. Στην ανάλυση των επιχειρηματικών επιπτώσεων λαμβάνεται επίσης υπόψη η κρισιμότητα των επιχειρηματικών διεργασιών και δραστηριοτήτων, επιχειρηματικών λειτουργιών, των ρόλων και των πόρων (π.χ. πληροφοριακών πόρων και πόρων ΤΠΕ), καθώς και των αλληλεξαρτήσεών τους σύμφωνα με το άρθρο 6 της παρούσας, περιλαμβανομένων τυχόν υπηρεσιών που έχουν ανατεθεί εξωτερικά.

2. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις διασφαλίζουν ότι τα συστήματα ΤΠΕ και οι υπηρεσίες ΤΠΕ τους σχεδιάζονται και συνάδουν με την ανάλυση των επιχειρηματικών επιπτώσεων που διενεργούν, για παράδειγμα εξασφαλίζοντας την εφεδρεία ορισμένων κρίσιμων στοιχείων για την πρόληψη δυσλειτουργιών ή διαταραχών λόγω συμβάντων που μπορεί να προκαλέσουν επιπτώσεις στα εν λόγω στοιχεία.

Άρθρο 23
(21η κατευθυντήρια γραμμή)
Σχεδιασμός επιχειρησιακής συνέχειας

1. Στα Σχέδια Επιχειρησιακής Συνέχειας (ΣΕΣ) που καταρτίζονται στο πλαίσιο της πολιτικής επιχειρησιακής

συνέχειας της παρ. 3 του άρθρου 258 του Κανονισμού (ΕΕ) 2015/35, λαμβάνονται υπόψη οι κίνδυνοι που θα μπορούσαν να έχουν δυσμενείς επιπτώσεις στα συστήματα ΤΠΕ και στις υπηρεσίες ΤΠΕ. Τα σχέδια υποστηρίζουν στόχους για την προστασία και, εφόσον απαιτείται, την αποκατάσταση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των επιχειρηματικών διεργασιών και δραστηριοτήτων, λειτουργιών, των ρόλων και των πληροφοριακών πόρων τους. Κατά την κατάρτιση των εν λόγω σχεδίων, οι επιχειρήσεις συντονίζονται με τους σχετικούς εσωτερικούς και εξωτερικούς ενδιαφερομένους, κατά περίπτωση.

2. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις θέτουν σε εφαρμογή σχέδια επιχειρησιακής συνέχειας (ΣΕΣ), ώστε να διασφαλίζεται ότι μπορούν να αντιδράσουν κατάλληλα σε πιθανά σενάρια αστοχίας και ότι είναι σε θέση να ανακτήσουν, έπειτα από διαταραχές, τις λειτουργίες των κρίσιμων επιχειρηματικών δραστηριοτήτων τους στο πλαίσιο ενός στόχου χρόνου ανάκτησης (ΣΧΑ, στόχος χρόνου ανάκαμψης: ο μέγιστος χρόνος εντός του οποίου ένα σύστημα ή μία διεργασία πρέπει να αποκατασταθεί έπειτα από κάποιο περιστατικό) και ενός στόχου σημείου ανάκτησης (ΣΣΑ, στόχος σημείου ανάκαμψης: η μέγιστη χρονική περίοδος κατά τη διάρκεια της οποίας είναι αποδεκτή η απώλεια δεδομένων σε περίπτωση συμβάντος ή περιστατικού).

3. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις εξετάζουν στα σχέδια επιχειρησιακής συνέχειας πληθώρα διαφορετικών σεναρίων, συμπεριλαμβανομένων ακραίων αλλά πιθανών σεναρίων, καθώς και σεναρίων επιθέσεων στον κυβερνοχώρο, και αξιολογούν τις δυνητικές επιπτώσεις των εν λόγω σεναρίων. Με βάση τα σενάρια αυτά, οι επιχειρήσεις περιγράφουν τον τρόπο διασφάλισης της συνέχειας των συστημάτων και των υπηρεσιών ΤΠΕ, καθώς και της ασφάλειας πληροφοριών των επιχειρήσεων.

Άρθρο 24
(22η κατευθυντήρια γραμμή)
Σχέδια αντιμετώπισης και ανάκαμψης

1. Βάσει των αναλύσεων των επιχειρηματικών επιπτώσεων του άρθρου 22 και των εύλογων σεναρίων της παρ. 2 του άρθρου 23, οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις καταρτίζουν σχέδια αντιμετώπισης και ανάκαμψης. Στα σχέδια αυτά προσδιορίζονται οι συνθήκες οι οποίες ενδέχεται να προκαλέσουν την άμεση ενεργοποίηση των σχεδίων, καθώς και τα μέτρα που λαμβάνονται για τη διασφάλιση της ακεραιότητας, της διαθεσιμότητας, της συνέχειας και της ανάκαμψης, τουλάχιστον, των κρίσιμων συστημάτων ΤΠΕ και υπηρεσιών ΤΠΕ των επιχειρήσεων. Τα σχέδια αντιμετώπισης και ανάκαμψης αποσκοπούν στην επίτευξη των στόχων ανάκαμψης των λειτουργιών των επιχειρήσεων.

2. Στα σχέδια αντιμετώπισης και ανάκαμψης λαμβάνονται υπόψη τόσο βραχυπρόθεσμες όσο και μακροπρόθεσμες επιλογές ανάκαμψης. Τα σχέδια:

α) εστιάζουν στην ανάκαμψη της λειτουργίας των κρίσιμων επιχειρηματικών λειτουργιών, των υποστηρικτικών διεργασιών, των πληροφοριακών πόρων, καθώς και των αλληλεξαρτήσεών τους, ώστε να αποφεύγονται δυσμενείς επιπτώσεις στη λειτουργία των επιχειρήσεων,

β) είναι τεκμηριωμένα, τίθενται στη διάθεση των επιχειρηματικών και υποστηρικτικών μονάδων και είναι εύκολα προσβάσιμα σε περίπτωση έκτακτης ανάγκης, συμπεριλαμβανομένου ενός σαφούς ορισμού ρόλων και αρμοδιοτήτων, και

γ) επικαιροποιούνται αμελλητί με βάση τα διδάγματα που αντλούνται από τα περιστατικά, τις δοκιμές, τους νέους κινδύνους και τις απειλές που εντοπίζονται, καθώς και τους μεταβαλλόμενους στόχους και τις προτεραιότητες ανάκαμψης.

3. Στα σχέδια λαμβάνονται επίσης υπόψη εναλλακτικές επιλογές σε περίπτωση που η ανάκαμψη μπορεί να μην είναι εφικτή σε βραχυπρόθεσμο ορίζοντα λόγω κόστους, κινδύνων, υλικοτεχνικής υποστήριξης ή απρόβλεπτων περιστάσεων.

4. Στο πλαίσιο των σχεδίων αντιμετώπισης και ανάκαμψης, οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις εξετάζουν και εφαρμόζουν μέτρα συνέχειας για την άμβλυνση των αστοχιών παρόχων υπηρεσιών, που είναι καίριας σημασίας για τη συνέχεια των υπηρεσιών ΤΠΕ των επιχειρήσεων (σύμφωνα με τις διατάξεις της ΠΕΕ 60/12.2.2016 και της ΠΕΕ 180/3/17.12.2020).

Άρθρο 25
(23η κατευθυντήρια γραμμή)
Δοκιμές των σχεδίων

1. Οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις υποβάλλουν σε δοκιμή τα σχέδια επιχειρησιακής συνέχειας σε περιοδική βάση και διασφαλίζουν ότι διενεργείται δοκιμή σε τουλάχιστον ετήσια βάση των εν λόγω σχεδίων των κρίσιμων επιχειρηματικών διεργασιών και δραστηριοτήτων, επιχειρηματικών λειτουργιών, των ρόλων και των πληροφοριακών πόρων, καθώς και των αλληλεξαρτήσεών τους (συμπεριλαμβανομένων των αλληλεξαρτήσεων με παρόχους υπηρεσιών) με βάση τα χαρακτηριστικά του προφίλ κινδύνου των επιχειρήσεων.

2. Τα σχέδια επιχειρησιακής συνέχειας επανεξετάζονται σε τουλάχιστον ετήσια βάση και επικαιροποιούνται με βάση τα αποτελέσματα των δοκιμών της παραγράφου 1, τις τρέχουσες πληροφορίες σχετικά με απειλές και τα διδάγματα που αντλούνται από προηγούμενα συμβάντα. Κάθε αλλαγή στους στόχους ανάκαμψης (συμπεριλαμβανομένων των στόχων χρόνου ανάκαμψης και των στόχων σημείου ανάκαμψης) ή/και αλλαγή στις επιχειρηματικές λειτουργίες, τις υποστηρικτικές διεργασίες και στους πληροφοριακούς πόρους λαμβάνεται επίσης υπόψη, κατά περίπτωση, για την επικαιροποίηση των σχεδίων επιχειρησιακής συνέχειας.

3. Στο πλαίσιο της δοκιμής των σχεδίων επιχειρησιακής συνέχειάς τους, οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις καταδεικνύουν ότι είναι σε θέση να διατηρήσουν τη βιωσιμότητα της επιχειρηματικής δραστηριότητάς τους έως ότου αποκατασταθούν οι κρίσιμες λειτουργίες.

4. Τα αποτελέσματα της δοκιμής τεκμηριώνονται από τους εκάστοτε υπεύθυνους και επιβεβαιώνονται από τη λειτουργία εσωτερικού ελέγχου, ενώ επίσης τυχόν δια-

πιστωθείσες ελλείψεις που προκύπτουν από τις δοκιμές αναλύονται, αντιμετωπίζονται και αναφέρονται στο Διοικητικό Συμβούλιο.

Άρθρο 26
(24η κατευθυντήρια γραμμή)
Επικοινωνία σε καταστάσεις κρίσεων

Σε περίπτωση διακοπής λειτουργίας, σημαντικού περιστατικού ασφάλειας ή έκτακτης ανάγκης, και κατά τη διάρκεια της εφαρμογής των σχεδίων επιχειρησιακής συνέχειας, οι ασφαλιστικές και αντασφαλιστικές επιχειρήσεις διασφαλίζουν την εφαρμογή αποτελεσματικών μέτρων επικοινωνίας σε καταστάσεις κρίσεων, ούτως ώστε όλοι οι σχετικοί εσωτερικοί και εξωτερικοί ενδιαφερόμενοι, συμπεριλαμβανομένων των αρμόδιων εποπτικών αρχών, κατά περίπτωση και σύμφωνα με τις ισχύουσες κανονιστικές διατάξεις, καθώς και οι σχετικοί πάροχοι υπηρεσιών, να ενημερώνονται έγκαιρα και με κατάλληλο τρόπο.

Άρθρο 27
Τελικές διατάξεις

1. Για παραβάσεις της παρούσας η Τράπεζα της Ελλάδος δύναται να επιβάλλει τις κυρώσεις του άρθρου 256 του ν. 4364/2016 σε συνδυασμό κατά περίπτωση με το άρθρο 55Α του Καταστατικού της.

2. Η παρούσα πράξη τίθεται σε ισχύ από την ημερομηνία δημοσίευσής της στην Εφημερίδα της Κυβερνήσεως.

3. Εξουσιοδοτείται η Διεύθυνση Εποπτείας Ιδιωτικής Ασφάλισης της Τράπεζας της Ελλάδος να παρέχει οδηγίες και διευκρινίσεις για την εφαρμογή της παρούσας.

4. Η παρούσα πράξη να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως και να αναρτηθεί στον ιστότοπο της Τράπεζας της Ελλάδος.

Ο Πρόεδρος

ΙΩΑΝΝΗΣ ΣΤΟΥΡΝΑΡΑΣ

ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ

Το Εθνικό Τυπογραφείο αποτελεί δημόσια υπηρεσία υπαγόμενη στην Προεδρία της Κυβέρνησης και έχει την ευθύνη τόσο για τη σύνταξη, διαχείριση, εκτύπωση και κυκλοφορία των Φύλλων της Εφημερίδας της Κυβερνήσεως (ΦΕΚ), όσο και για την κάλυψη των εκτυπωτικών - εκδοτικών αναγκών του δημοσίου και του ευρύτερου δημόσιου τομέα (ν. 3469/2006/Α΄ 131 και π.δ. 29/2018/Α΄58).

1. ΦΥΛΛΟ ΤΗΣ ΕΦΗΜΕΡΙΔΑΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ (ΦΕΚ)

• Τα **ΦΕΚ σε ηλεκτρονική μορφή** διατίθενται δωρεάν στο **www.et.gr**, την επίσημη ιστοσελίδα του Εθνικού Τυπογραφείου. Όσα ΦΕΚ δεν έχουν ψηφιοποιηθεί και καταχωριστεί στην ανωτέρω ιστοσελίδα, ψηφιοποιούνται και αποστέλλονται επίσης δωρεάν με την υποβολή αίτησης, για την οποία αρκεί η συμπλήρωση των αναγκαίων στοιχείων σε ειδική φόρμα στον ιστότοπο www.et.gr.

• Τα **ΦΕΚ σε έντυπη μορφή** διατίθενται σε μεμονωμένα φύλλα είτε απευθείας από το Τμήμα Πωλήσεων και Συνδρομητών, είτε ταχυδρομικά με την αποστολή αιτήματος παραγγελίας μέσω των ΚΕΠ, είτε με ετήσια συνδρομή μέσω του Τμήματος Πωλήσεων και Συνδρομητών. Το κόστος ενός ασπρόμαυρου ΦΕΚ από 1 έως 16 σελίδες είναι 1,00 €, αλλά για κάθε επιπλέον οκτασέλιδο (ή μέρος αυτού) προσαυξάνεται κατά 0,20 €. Το κόστος ενός έγχρωμου ΦΕΚ από 1 έως 16 σελίδες είναι 1,50 €, αλλά για κάθε επιπλέον οκτασέλιδο (ή μέρος αυτού) προσαυξάνεται κατά 0,30 €. Το τεύχος Α.Σ.Ε.Π. διατίθεται δωρεάν.

• **Τρόποι αποστολής κειμένων προς δημοσίευση:**

Α. Τα κείμενα προς δημοσίευση στο ΦΕΚ, από τις υπηρεσίες και τους φορείς του δημοσίου, αποστέλλονται ηλεκτρονικά στη διεύθυνση **webmaster.et@et.gr** με χρήση προηγμένης ψηφιακής υπογραφής και χρονοσήμανσης.

Β. Κατ’ εξαίρεση, όσοι πολίτες δεν διαθέτουν προηγμένη ψηφιακή υπογραφή μπορούν είτε να αποστέλλουν ταχυδρομικά, είτε να καταθέτουν με εκπρόσωπό τους κείμενα προς δημοσίευση εκτυπωμένα σε χαρτί στο Τμήμα Παραλαβής και Καταχώρισης Δημοσιευμάτων.

• Πληροφορίες, σχετικά με την αποστολή/κατάθεση εγγράφων προς δημοσίευση, την ημερήσια κυκλοφορία των Φ.Ε.Κ., με την πώληση των τευχών και με τους ισχύοντες τιμοκαταλόγους για όλες τις υπηρεσίες μας, περιλαμβάνονται στον ιστότοπο (www.et.gr). Επίσης μέσω του ιστότοπου δίδονται πληροφορίες σχετικά με την πορεία δημοσίευσης των εγγράφων, με βάση τον Κωδικό Αριθμό Δημοσιεύματος (ΚΑΔ). Πρόκειται για τον αριθμό που εκδίδει το Εθνικό Τυπογραφείο για όλα τα κείμενα που πληρούν τις προϋποθέσεις δημοσίευσης.

2. ΕΚΤΥΠΩΤΙΚΕΣ - ΕΚΔΟΤΙΚΕΣ ΑΝΑΓΚΕΣ ΤΟΥ ΔΗΜΟΣΙΟΥ

Το Εθνικό Τυπογραφείο ανταποκρινόμενο σε αιτήματα υπηρεσιών και φορέων του δημοσίου αναλαμβάνει να σχεδιάσει και να εκτυπώσει έντυπα, φυλλάδια, βιβλία, αφίσες, μπλοκ, μηχανογραφικά έντυπα, φακέλους για κάθε χρήση, κ.ά.

Επίσης σχεδιάζει ψηφιακές εκδόσεις, λογότυπα και παράγει οπτικοακουστικό υλικό.

Ταχυδρομική Διεύθυνση: Καποδιστρίου 34, τ.κ. 10432, Αθήνα	Ιστότοπος: **www.et.gr**
ΤΗΛΕΦΩΝΙΚΟ ΚΕΝΤΡΟ: 210 5279000 - fax: 210 5279054	Πληροφορίες σχετικά με την λειτουργία του ιστότοπου: **helpdesk.et@et.gr**
ΕΞΥΠΗΡΕΤΗΣΗ ΚΟΙΝΟΥ **Πωλήσεις - Συνδρομές:** (Ισόγειο, τηλ. 210 5279178 - 180) **Πληροφορίες:** (Ισόγειο, Γρ. 3 και τηλεφ. κέντρο 210 5279000) **Παραλαβή Δημ. Ύλης:** (Ισόγειο, τηλ. 210 5279167, 210 5279139)	Αποστολή ψηφιακά υπογεγραμμένων εγγράφων προς δημοσίευση στο ΦΕΚ: **webmaster.et@et.gr**
Ωράριο για το κοινό: Δευτέρα ως Παρασκευή: 8:00 - 13:30	Πληροφορίες για γενικό πρωτόκολλο και αλληλογραφία: **grammateia@et.gr**

Πείτε μας τη γνώμη σας,

για να βελτιώσουμε τις υπηρεσίες μας, συμπληρώνοντας την ειδική φόρμα στον ιστότοπό μας.

02056720312210012