Π Α Ν Ε Π Ι Σ Τ Η Μ Ι Ο Π Ε Ι Ρ Α Ι Ω Σ

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ. ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ & ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κατεύθυνση: ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Διπλωματική Εργασία

ΣΧΕΔΙΑΣΜΟΣ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΕΣ (DISASTER RECOVERY PLANNING)

Γιώργος Δρίβας

Α.Μ.: MTE1047

Επιβλέπων Καθηγητής: Χρήστος Ξενάκης

Πειραιάς, Οκτώβριος 2012

ΠΕΡΙΛΗΨΗ

Τα Πληροφοριακά Συστήματα αποτελούν πλέον βασικό πυλώνα της καθημερινότητας της ανθρώπινης δραστηριότητας. Το γεγονός αυτό τα έχει καταστήσει πολύτιμο και ελκυστικό στόχο για κάθε είδους επιθέσεις. Για να αντιμετωπιστούν αυτές οι απειλές έχει δημιουργηθεί πληθώρα προστατευτικών μέτρων, τα οποία, όταν εφαρμόζονται με τον ενδεδειγμένο τρόπο, εκπληρώνουν με επιτυχία το σκοπό τους. Πάραυτα, πάντα υπάρχει ένα ποσοστό απειλών που καταφέρνουν να πλήξουν με καταστροφικές συνέπειες τα Πληροφοριακά Συστήματα. Σε αυτές τις περιπτώσεις μόνη λύση αποτελεί η εφαρμογή μέτρων ταχείας ανάκαμψης με τη μορφή ενός οργανωμένου Σχεδίου Ανάκαμψης από Καταστροφές.

Η παρούσα εργασία αποτελεί μια προσπάθεια να παρουσιαστεί, με ολοκληρωμένο τρόπο, το θεματικό πεδίο του Σχεδιασμού Ανάκαμψης από Καταστροφές (ΣΑΚ) των Πληροφοριακών Συστημάτων ενός οργανισμού. Επιχειρείται να περιγραφεί και να αναλυθεί ο τρόπος που εφαρμόζεται ένας τέτοιος σχεδιασμός σε διοικητικό, οργανωτικό και τεχνολογικό επίπεδο μέσα από τη μελέτη κατάλληλων προτύπων και βέλτιστων πρακτικών. Παράλληλα, δίδεται έμφαση σε ιδιαίτερα ζητήματα, κυρίως οικονομικής και νομικής φύσης, στα οποία μέχρι σήμερα μοιάζει να μην υπάρχουν ικανοποιητικές απαντήσεις. Χαρακτηριστικά, διερευνάται κατά πόσο υπάρχουν νομικές/κανονιστικές δεσμεύσεις που να επιβάλλουν το ΣΑΚ, αλλά και προσδιορίζεται ο τρόπος προϋπολογισμού του κόστους του, ώστε να επιτυγχάνεται η βέλτιστη επένδυση. Συγκρίνονται οι σύγχρονες τάσεις και μέτρα ανάκαμψης και αναλύεται ο τρόπος που πρέπει να επιλέγονται. Τέλος, μέσα από μια μελέτη περίπτωσης, γίνεται προσπάθεια να δημιουργηθεί ένα πλαίσιο που να παρέχει τη δυνατότητα εφαρμογής του ΣΑΚ, με γρήγορο και αποδοτικό τρόπο, σε μικρούς /μικρομεσαίους οργανισμούς.

Abstract

Information Systems are already a key pillar of everyday human activity. This fact has made them valuable and attractive target for any kind of attack. To meet these threats many protective measures have been created, that are successfully fulfilling their purpose, when applied properly. Nevertheless, there is always a percentage of threats that finally manage to hit Information Systems, with devastating consequences. In these cases the only solution is the implementation of rapid recovery measures in the form of an organized Disaster Recovery Plan.

This paper is an attempt to present, in an integrated way, the thematic area of Disaster Recovery Planning (DRP) of Information Systems in an organization. It describes and analyzes the manner to apply such a planning on administrative, organizational and technological level through the study of appropriate standards and best practices. Alongside, emphasis is given on particular issues, mainly financial and legal, where, as of today, there seems to be no satisfactory answers. Indicative, it is investigated whether there are legal/regulatory constraints that enforce a DRP and specified how the budget on DRP is estimated, in order to bring the best return on investment. It compares the latest trends and recovery measures and analyzes the way they should be selected. Finally, there is an effort, through a case study, to create a framework that allows the application of DRP in a fast and efficient way on small and medium size organizations.

Περιεχόμενα

Ευρετήριο Σχημάτων

Ευρετήριο Πινάκων

1 Εισαγωγή

Η διείσδυση των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) στην καθημερινότητα της ανθρώπινης δραστηριότητας εκτός από δεδομένη τείνει πλέον να γίνει και καθολική σε κάθε έκφανσή της, είτε σε οικονομικό, είτε σε κοινωνικό, είτε σε πολιτικό, είτε ακόμα και σε πολιτισμικό επίπεδο. Η εξέλιξη αυτή καθιστά τις ΤΠΕ αναγκαίες και απαραίτητες μετατρέποντάς τες σε πολύτιμο αγαθό και ταυτόχρονα ελκυστικό στόχο για κάθε είδους επιθέσεις.

Το γεγονός αυτό ώθησε στη δημιουργία απαραίτητων προστατευτικών μέτρων (διοικητικών, οργανωτικών, τεχνολογικών), τα οποία σήμερα φέρονται ικανά να εκπληρώσουν με επιτυχία το σκοπό τους, όταν εφαρμόζονται με τον ενδεδειγμένο τρόπο. Πάραυτα όσο επαρκή και ολοκληρωμένα και αν είναι αυτά, πάντα θα υπάρχει ένα ποσοστό εναπομείναντα κινδύνου. Αυτό συνήθως οφείλεται στις απειλές, των οποίων οι επιπτώσεις θεωρείται πολλές φορές αδύνατο να αποφευχθούν. Χαρακτηριστικό παράδειγμα τέτοιων απειλών αποτελούν οι κάθε είδους καταστροφές, με συνηθέστερες τις φυσικές καταστροφές, των οποίων οι επιπτώσεις μπορεί να είναι και ολέθριες. Από τις απειλές αυτές, η συχνότητα των οποίων παρουσιάζει αύξηση τα τελευταία χρόνια, δε μπορούν να εξαιρεθούν ούτε οι οργανισμοί ούτε τα πληροφοριακά συστήματα που τους υποστηρίζουν. Αξίζει να σημειωθεί χαρακτηριστικά, ότι στα κέντρα δεδομένων (data centers) των ΗΠΑ παρουσιάζονται κατά μέσο όρο 2,5 καταστροφικά περιστατικά το χρόνο, μέσης διάρκειας 134 λεπτών [1].

Οι σύγχρονοι οργανισμοί φροντίζουν για τη λήψη όλων των πρόσφορων μέτρων για τον περιορισμό ή ακόμα και την εξάλειψη των επιπτώσεων, μιας ενδεχόμενης καταστροφής, στα Πληροφοριακά τους Συστήματα. Βασικό εργαλείο για την λήψη αυτών των μέτρων αποτελούν τα διάφορα σχέδια τα οποία μπορεί να αφορούν είτε στην πρόληψη, είτε στην αντιμετώπιση-ανάκαμψη ή ακόμα και στην αποφυγή των επιπτώσεων. Βασικός στόχος των σχεδίων αυτών είναι να διατηρηθεί η ικανότητα του οργανισμού, που πλήχθηκε από κάποια καταστροφή, να συνεχίσει να παρέχει, στο συντομότερο χρονικό διάστημα, τις κρίσιμες λειτουργίες του. Αυτή η απαίτηση γίνεται ακόμα πιο έντονη όταν οι οργανισμοί χρησιμοποιούν κεντρικές δομές ή/και παρέχουν υπηρεσίες κοινής ωφέλειας.

1.1 Το αντικείμενο της διπλωματικής εργασίας

Αντικείμενο της παρούσας εργασίας αποτελεί ο σχεδιασμός που απαιτείται, καθώς και τα μέτρα που μπορούν να υιοθετηθούν από αυτόν, ώστε να επιτευχτεί η ταχύτερη δυνατή ανάκαμψη των Πληροφοριακών Συστημάτων ενός οργανισμού έπειτα από μια καταστροφή. Η διαδικασία αυτή, η οποία εντάσσεται στο ευρύτερο πεδίο της επιχειρησιακής συνέχειας, είναι γνωστή ως «Σχεδιασμός Ανάκαμψης από Καταστροφές (ΣΑΚ)» (Disaster Recovery Planning-DRP).

1.2 Σκοπός της παρούσας εργασίας

Σκοπός της παρούσας εργασίας αποτελεί η μελέτη και ανάλυση του σχεδιασμού ανάκαμψης από καταστροφές, οι οποίες προσβάλλουν τα Πληροφοριακά Συστήματα των οργανισμών. Έμφαση δίδεται στα Πληροφοριακά Συστήματα που υποστηρίζουν τη λειτουργία μικρών και μικρομεσαίων οργανισμών. Ειδικότερα θα επιχειρηθεί να διερευνηθούν και να δοθούν απαντήσεις, όπου καθίσταται εφικτό, στα παρακάτω ερωτήματα:

- Πόσο σημαντικό είναι το ΣΑΚ για έναν οργανισμό;
- Η ύπαρξη ενός τέτοιου σχεδίου θα πρέπει να θεωρείται υποχρεωτική ή προαιρετική; Υπάρχουν υποχρεώσεις νομικού χαρακτήρα που να το επιβάλλουν;
- Υπάρχουν κατάλληλα πρότυπα ή/και βέλτιστες πρακτικές για την αποτελεσματική εφαρμογή ενός ΣΑΚ;
- Ποιό πρέπει να είναι το κόστος ενός ΣΑΚ ώστε να μπορεί να θεωρηθεί αποδοτικό με οικονομικούς όρους;
- Ποιά μέτρα ανάκαμψης υπάρχουν σήμερα και με ποια κριτήρια πρέπει να επιλέγονται;
- Πως μπορεί να εφαρμοστεί γρήγορα και αποδοτικά σε μικρούς/μικρομεσαίους οργανισμούς;

1.3 Η δομή της διπλωματικής εργασίας

Η εργασία είναι δομημένη με τέτοιο τρόπο ώστε από μια αρχικά θεωρητική προσέγγιση του θέματος να οδηγηθούμε σε πρακτική εφαρμογή και περαιτέρω επέκτασή του, μέσα από μια μελέτη περίπτωσης. Επιγραμματικά σε κάθε κεφάλαιο περιλαμβάνεται:

Κεφάλαιο 1: Στο 1ο κεφάλαιο παρουσιάζεται το αντικείμενο και ο σκοπός της παρούσας εργασίας.

Κεφάλαιο 2: Στο 2ο κεφάλαιο γίνεται αναφορά στο πλαίσιο της διπλωματικής εργασίας. Καταγράφονται τα είδη των καταστροφών και οι επιπτώσεις τους στα Πληροφοριακά Συστήματα και κατ' επέκταση στους οργανισμούς που τα χρησιμοποιούν. Δίδονται τα είδη σχεδίων αντιμετώπισης που υπάρχουν και περιγράφεται ο κύκλος ζωής τους.

Κεφάλαιο 3: Στο 3ο κεφάλαιο αναλύονται τα ειδικότερα ζητήματα που αφορούν στο Σχεδιασμό Ανάκαμψης από Καταστροφές. Αναλύεται η σημασία του για έναν οργανισμό, η σχέση του με την επιχειρησιακή συνέχεια και το κόστος που πρέπει να έχει για να θεωρείται αποδοτικός. Ταυτόχρονα εξετάζεται η ύπαρξη νομικών υποχρεώσεων που τον επιβάλλουν και η ύπαρξη προτύπων σχετικά με τον τρόπο που πρέπει να εφαρμόζεται.

Κεφάλαιο 4: Στο 4ο κεφάλαιο περιγράφεται μια τυπική διαδικασία Σχεδιασμού Ανάκαμψης από Καταστροφές και αναλύονται τα επιμέρους βήματα που πρέπει να ακολουθούνται.

Κεφάλαιο 5: Στο 5ο κεφάλαιο παρουσιάζονται οι σύγχρονες τάσεις αντιμετώπισης και τα μέτρα ανάκαμψης που προσφέρονται σήμερα. Γίνεται μια προσπάθεια συγκριτικής αξιολόγησής τους και παρουσίασης των κριτηρίων με τα οποία μπορούν να επιλέγονται.

Κεφάλαιο 6: Στο 6ο κεφάλαιο επιχειρείται να παρουσιαστεί η εφαρμογή όσων περιγράφονται παραπάνω, μέσω της μελέτης μιας περίπτωσης ενός υποθετικού φορέα υγείας. Από τη μελέτη αυτή προκύπτει ένα Σχέδιο Ανάκαμψης από Καταστροφές (ΣΑΚ) το οποίο μπορεί να χρησιμοποιηθεί ως πρότυπο, για τη γρήγορη και αποδοτική προσαρμογή του, σε αντίστοιχους μικρούς/μικρομεσαίους οργανισμούς.

Κεφάλαιο 7: Στο 7ο κεφάλαιο συνοψίζονται τα συμπεράσματα που προέκυψαν από την παρούσα εργασία καθώς και από τη μελέτη περίπτωσης που πραγματοποιήθηκε.

2 Το πλαίσιο της διπλωματικής εργασίας

2.1 Είδη καταστροφών

Οι καταστροφές που μπορεί να πλήξουν έναν οργανισμό, και ειδικότερα τα πληροφοριακά συστήματα που τον υποστηρίζουν λειτουργικά, συνήθως αποτελούν συνεπακόλουθο είτε κάποιου φυσικού φαινομένου, είτε αποτέλεσμα ανθρώπινης ενέργειας, είτε ακόμα και τεχνολογικού σφάλματος.

Οι φυσικές καταστροφές συνήθως αφορούν σε ξαφνικά γεγονότα τα οποία οφείλονται σε περιβαλλοντικούς παράγοντες και συνήθως είναι:

- σεισμοί
- πυρκαγιές
- πλημμύρες
- τυφώνες
- κατολισθήσεις
- ηφαίστεια
- ακραία καιρικά φαινόμενα

Οι καταστροφές από ανθρώπινη ενέργεια συνήθως αφορούν είτε λάθη, παραλείψεις, άγνοια είτε δόλο και ενδεικτικά μπορεί να είναι:

Ανθρώπινα λάθη:

- ατυχήματα
- διαρροή επικίνδυνων ουσιών/μόλυνση

Ανθρώπινος δόλος:

- τρομοκρατικές ενέργειες
- hacking
- κλοπή υλικού/δεδομένων
- εξεγέρσεις/κοινωνικές αναταραχές

Τα τεχνολογικά σφάλματα μπορεί να αφορούν σε:

- δυσλειτουργία εξοπλισμού

- λάθη συστήματος
- πτώση/απώλεια ενέργειας
- απώλεια επικοινωνιών

Τέλος υπάρχουν και καταστροφές ειδικότερου τύπου όπως:

- πανδημίες
- οικονομική κατάρρευση

2.2 Επιπτώσεις καταστροφών σε Πληροφοριακά Συστήματα

Οι επιπτώσεις των καταστροφών μπορούν να αφορούν από την αποδιοργάνωση κάποιων καθημερινών λειτουργιών έως και την ακραία περίπτωση της απώλειας ανθρώπινων ζωών.

Δεδομένης της ευρείας εισαγωγής των πληροφοριακών συστημάτων στη καθημερινή λειτουργία των οργανισμών, μια ενδεχόμενη καταστροφή τους μπορεί να έχει πολυδιάστατες συνέπειες. Προσπαθώντας να εξετάσουμε αυτές τις συνέπειες, μπορούμε να τις κατηγοριοποιήσουμε στα παρακάτω πεδία [2] [3]:

2.2.1 Νομικές-κανονιστικές

Χαρακτηριστικό της εποχής που ζούμε είναι η ολοένα και αυξανόμενη μετάβαση των δεδομένων σε ηλεκτρονική μορφή είτε αυτά αποτελούν δεδομένα σε κίνηση ή σε αποθήκευση, έτοιμα προς επεξεργασία. Η διείσδυση των νέων τεχνολογιών και ιδίως του κλάδου των ΤΠΕ στη διαχείριση αυτών των ηλεκτρονικών δεδομένων κληροδοτεί όλες τις νομικές υποχρεώσεις που υπάρχουν σχετικά με την ασφάλεια τους και την προστασία της ιδιωτικότητας. Ως αποτέλεσμα, κάθε καταστροφικό περιστατικό που μπορεί να επηρεάσει τα ηλεκτρονικά δεδομένα, ιδίως όταν αυτά αφορούν προσωπικά δεδομένα τρίτων η πολύ περισσότερο ευαίσθητα, μπορεί να οδηγήσει σε πρόστιμα και νομικές κυρώσεις βάσει νομικών και κανονιστικών υποχρεώσεων του οργανισμού. Όμως ακόμα και η καταστροφή ή μη διαθεσιμότητα απλών δεδομένων μπορεί να αποτελέσει αντικείμενο νομικών διεκδικήσεων, στην περίπτωση που αυτά συνδέονται με υποχρεώσεις διασφαλισμένου επιπέδου παροχής υπηρεσιών (SLA) από τον οργανισμό προς τρίτους.

2.2.2 Οικονομικές

Η μη διαθεσιμότητας των ΠΣ μπορούν να οδηγήσουν είτε σε άμεσες οικονομικές απώλειες είτε σε έμμεσες και μπορεί να αφορούν τόσο στην αύξηση του λειτουργικού κόστους όσο και στην απώλεια εσόδων. Οι άμεσες απώλειες μπορεί να εκδηλώνονται όταν τα ΠΣ επιτελούν επιχειρηματικές λειτουργίες του οργανισμού, οι οποίες μεγιστοποιούνται όταν αυτές σχετίζονται με ηλεκτρονικό επιχειρείν. Ταυτόχρονα οι νομικές επιπτώσεις και η μείωση της παραγωγικότητας του προσωπικού μπορεί πάλι με έμμεσο τρόπο να μεταφραστεί σε οικονομική απώλεια. Αυτές οι συνέπειες μπορεί να εκδηλώνονται είτε ως στιγμιαίες απώλειες, και για όσο διαρκεί η μη διαθεσιμότητα των ΠΣ, είτε ως μακροχρόνιες οικονομικές συνέπειες που μπορεί να επακολουθούν την ενδεχόμενη απώλεια φήμης και έλλειψης εμπιστοσύνης από τρίτους.

2.2.3 Λειτουργικές-Παραγωγικές

Η έλλειψη διαθεσιμότητας των ΠΣ μπορεί ενδεχομένως να έχει καταστροφικές επιπτώσεις στις παρεχόμενες υπηρεσίες ή λειτουργίες του οργανισμού όταν αυτές στηρίζονται σε αυτά. Οι συνέπειες αυτές μπορεί να κυμαίνονται από άμεση ή έμμεση μείωση της παραγωγικότητας μιας υπηρεσίας έως και παντελή διακοπή της όταν είναι πλήρως εξαρτώμενες από ΠΣ, ιδίως όταν δεν υπάρχει δυνατότητα να παρασχεθούν χειροκίνητα (χωρίς την λειτουργία των ΠΣ) και σε ανεκτό ποιοτικά επίπεδο. Μια παρατεταμένη διακοπή λειτουργίας των ΠΣ δημιουργεί την ανάγκη για επιπρόσθετο χρόνο εκτέλεσης μιας εργασίας γεγονός το οποίο μπορεί να οδηγήσει σε οικονομικές επιπτώσεις, λόγω ενδεχόμενης υπερωριακής απασχόλησης, αλλά και σε αναστάτωσης της εργασιακής καθημερινότητας του προσωπικού.

2.2.4 Υγιεινή και Ασφάλεια

Όσον αφορά στον τομέα της υγιεινής και της ασφάλειας η επίδραση της απώλειας των ΠΣ μπορεί να έχει άμεσες και έμμεσες αρνητικές συνέπειες, από περιβαλλοντικές καταστροφές έως και κίνδυνο απώλειας ζωών. Σε οργανισμούς όπου τα ΠΣ μπορεί είτε να διαχειρίζονται είτε να ελέγχουν επικίνδυνα μηχανήματα (όπως στις βιομηχανίες και τον κατασκευαστικός κλάδο), εγκαταστάσεις περιβαλλοντικού ελέγχου (όπως είναι τα συστήματα BCM σε επικίνδυνα εργασιακά περιβάλλοντα) ή συστήματα ελέγχου πρόσβασης, μια ενδεχόμενη δυσλειτουργία τους μπορεί να προκαλέσει αλυσιδωτές καταστροφές. Άλλωστε η

διασφάλιση της λειτουργίας τέτοιων συστημάτων μπορεί να κρίνεται και υποχρεωτική προκειμένου να υπάρχει συμμόρφωση με την Ευρωπαϊκή νομοθεσία που σχετίζεται με την Υγιεινή και την Ασφάλεια στο χώρο εργασίας, όπως αυτή εκφράζεται μέσα από την οδηγία 89/391/EEC(12/6/1989) [4].

2.2.5 Υπόληψη-Υστεροφημία

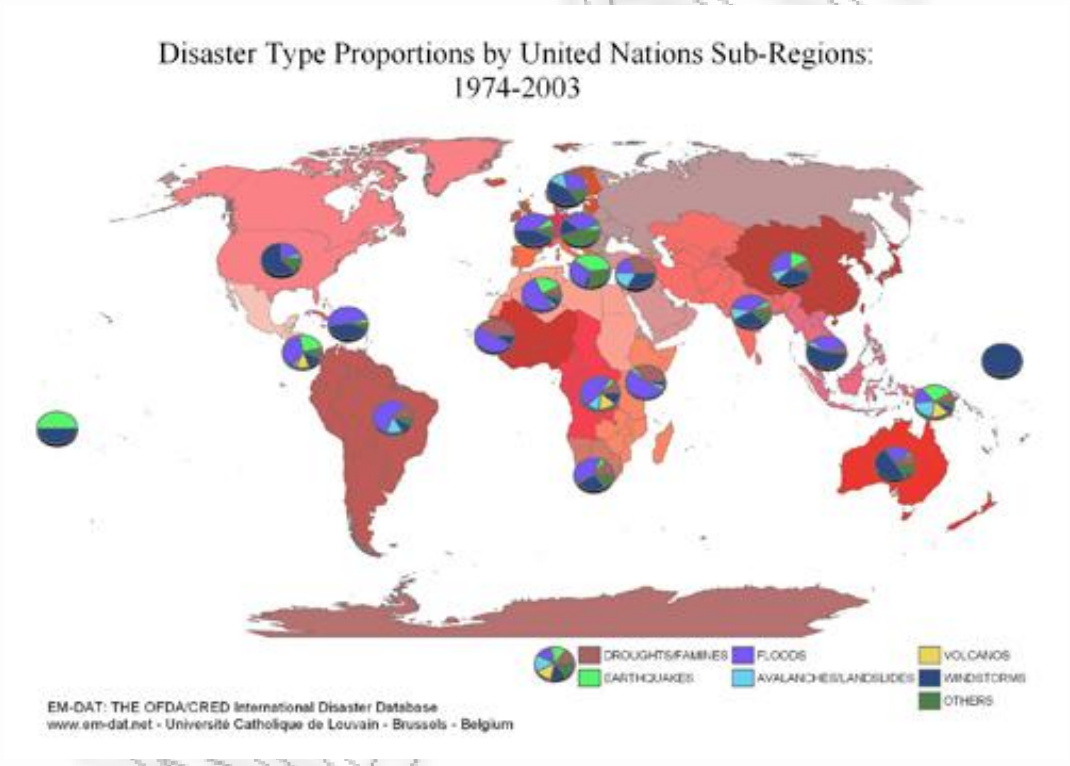
Η διακοπή της λειτουργίας των ΠΣ μπορεί να έχουν άμεσο αντίκτυπο και στις σχέσεις με τρίτους είτε αφορά πελάτες, προμηθευτές ή κάποια εποπτεύουσα αρχή με τη μορφή απώλειας της εμπιστοσύνης, της αξιοπιστίας και της φήμης του οργανισμού στον τομέα όπου δραστηριοποιείται. Αυτή η κατηγορία επιπτώσεων ίσως είναι και η πιο επικίνδυνη καθώς οι συνέπειες μπορεί να είναι μακροχρόνιες και να μην υπάρχουν διαθέσιμες ενέργειες για την άμεση αποκατάστασή τους. Άλλωστε η έννοια τόσο της αξιοπιστίας όσο και της εμπιστοσύνης είναι συνδεδεμένες με αυτή της διάρκειας στο χρόνο, και παρόλη την ενδεχόμενη επάρκεια οικονομικών και άλλων πόρων να μην καθίσταται δυνατή η ανάκτησή τους.

2.2.6 Άλλες

Πέρα από όλες τις παραπάνω επιπτώσεις, που μπορεί να προκαλέσει μια ενδεχόμενη καταστροφή των ΠΣ ενός οργανισμού, υπάρχουν και ειδικότερου τύπου επιπτώσεις. Αυτές ανάλογα με τη φύση, το έργο και την αποστολή του οργανισμού μπορεί να ξεφεύγουν από τα στενά πλαίσια του οργανισμού. Χαρακτηριστικά, όταν ο οργανισμός αποτελεί φορέα δημόσιας διοίκησης, η έλλειψη της διάθεσης κρίσιμων λειτουργιών που εξυπηρετούνται από ΠΣ μπορεί να προκαλέσει διοικητικό έλλειμμα και σε ακραίες συνθήκες ακόμα και κυβερνητικό έλλειμμα. Σε άλλη περίπτωση όταν ο οργανισμός διαχειρίζεται ευαίσθητα δεδομένα, η ενδεχόμενη καταστροφή τους ή η έλλειψη στη διαθεσιμότητάς τους δημιουργεί ταυτόχρονα έλλειμμα σε επίπεδο ασφάλειας πληροφοριών. Πολύ περισσότερο οι επιπτώσεις μπορεί να λάβουν τεράστιες διαστάσεις όταν αφορούν παρεχόμενες υπηρεσίες από ΠΣ τα οποία εξυπηρετούν υποδομές ζωτικής σημασίας, όπως μπορεί για παράδειγμα να είναι ένας αερολιμένας ή ένα νοσοκομείο. Σε τέτοιες περιπτώσεις η απουσία ύπαρξης διαδικασιών άμεσης ανάκαμψης των ΠΣ θεωρείται μη αποδεκτή, καθώς μπορεί να οδηγήσει ακόμα και σε επιπτώσεις σε εθνικό επίπεδο.

2.3 Ιστορικά στοιχεία καταστροφικών περιστατικών

Σε μια προσπάθεια να εξετάσει κανείς ιστορικά την συχνότητα εμφάνισης καταστροφικών περιστατικών, είτε οφείλονται σε φυσικά φαινόμενα είτε σε τεχνολογικές αστοχίες, παρατηρεί ότι υπάρχει αύξηση και μάλιστα με πολύ γρήγορο ρυθμό. Αντλώντας στοιχεία από τη βάση δεδομένων περιστατικών έκτακτης ανάγκης (EM-DAT) [5] που διατηρεί το Κέντρο Έρευνας για την Επιδημιολογία των Καταστροφών (Centre for Research on the Epidemiology of Disasters -CRED) [6] σε συνεργασία με το Αμερικανικό Γραφείο Βοηθείας Καταστροφών Εξωτερικού (Office of U.S. Foreign Disaster Assistance-OFDA) διαμορφώνονται οι παρακάτω χάρτες σε παγκόσμιο επίπεδο:



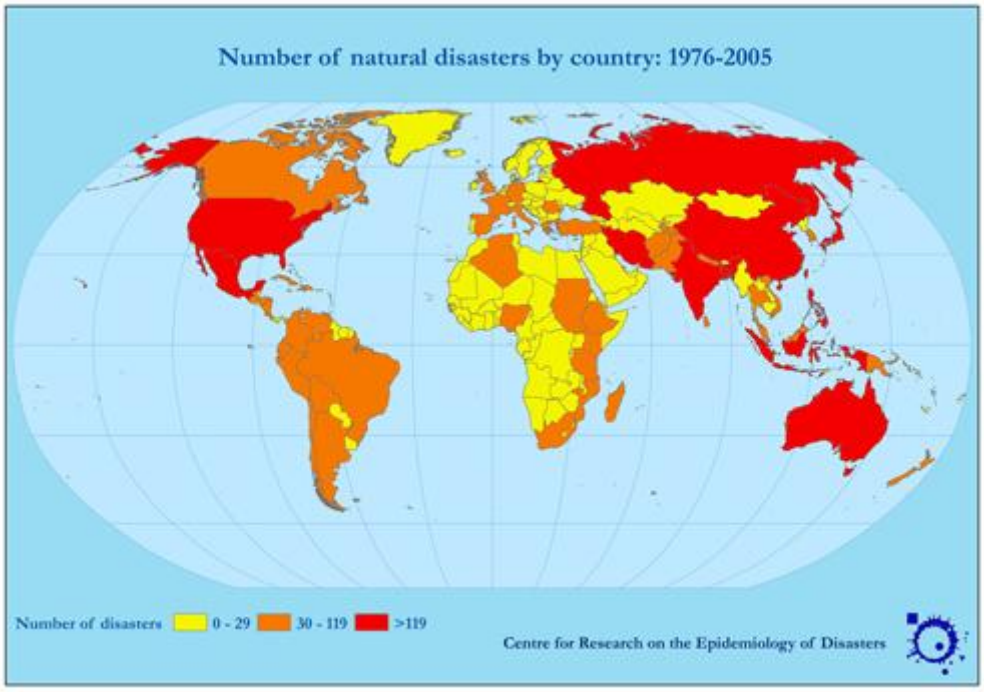
Σχήμα 1: *Γεωγραφική κατανομή φυσικών καταστροφών 1974-2003 [5]*

Στον παραπάνω χάρτη (Σχήμα 1) παρατηρείται το είδος των καταστροφών που αναλογεί σε κάθε περιοχή του πλανήτη για την περίοδο 1974-2003, όπου αποτυπώνεται και η έντονη εμφάνιση καταστροφών από σεισμούς και πλημμύρες στην περιοχή του ελλαδικού χώρου. Αυτό γίνεται ακόμα πιο εμφανές αν εξετάσουμε τα στοιχεία του Πίνακα 1 που αφορά στη σύνοψη των φυσικών καταστροφών στην Ελλάδα για την περίοδο 1900-2012.

Summarized Table of Natural Disasters in Greece from 1900 to 2012					
Disaster Type	**Description**	**# of Events**	**Killed**	**Total Affected**	**Damage (000 US$)**
Drought	Drought	1	-	-	1000000
	ave. per event		-	-	1000000.0
Earthquake (seismic activity)	Earthquake (ground shaking)	29	951	960398	7099300
	ave. per event		32.8	33117.2	244803.4
Extreme temperature	Cold wave	2	10	-	-
	ave. per event		5.0	-	-
	Heat wave	5	1119	176	3000
	ave. per event		223.8	35.2	600.0
Flood	Unspecified	8	66	9730	188000
	ave. per event		8.3	1216.3	23500.0
	General flood	12	18	6100	1043359
	ave. per event		1.5	508.3	86946.6
Storm	Unspecified	6	56	612	690000
	ave. per event		9.3	102.0	115000.0
	Local storm	1	22	-	-
	ave. per event		22.0	-	-
	Tropical cyclone	1	43	-	-
	ave. per event		43.0	-	-
Volcano	Volcanic eruption	1	48	-	-
	ave. per event		48.0	-	-
Wildfire	Forest fire	11	94	8559	1750000
	ave. per event		8.5	778.1	159090.9
	Scrub/grassland fire	2	14	500	675000
	ave. per event		7.0	250.0	337500.0

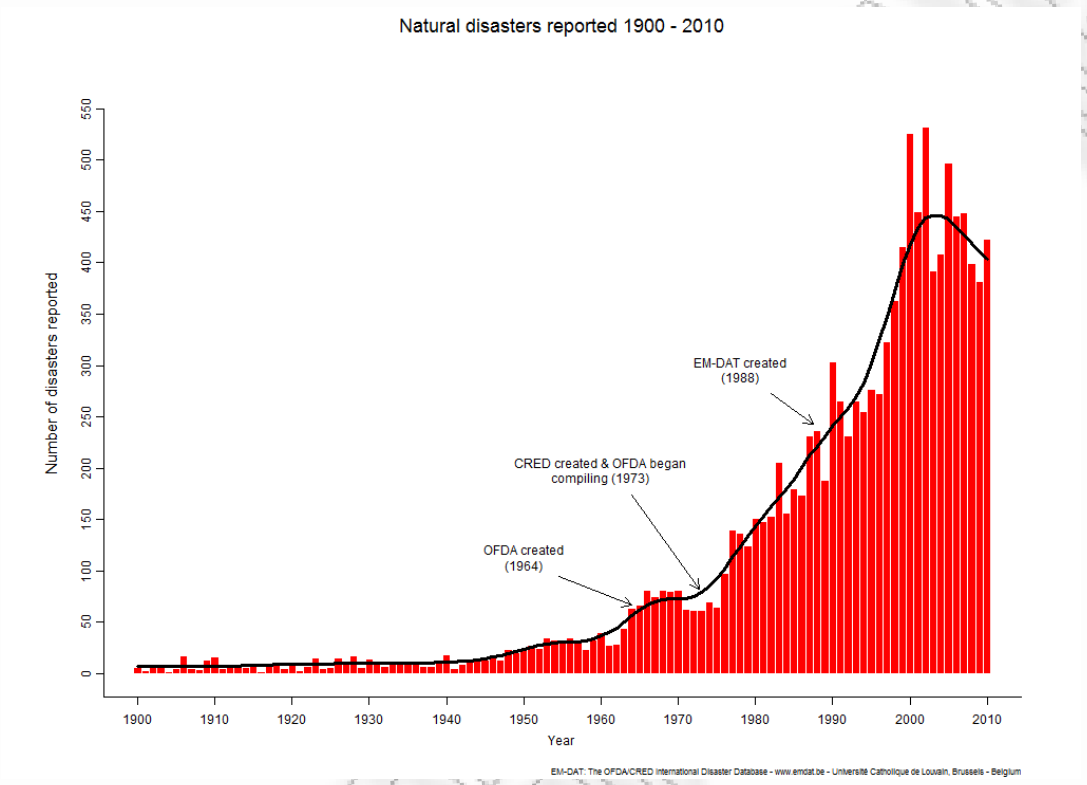
Πίνακας 1: *Φυσικές καταστροφές στην Ελλάδα 1900-2012 [5]*

Στον χάρτη (Σχήμα 2) ο οποίος αναφέρεται στην περίοδο 1976-2005 εμφανίζεται η κατηγοριοποίηση των χωρών ανάλογα με την κατανομή των περιστατικών σε απόλυτους αριθμούς. Σύμφωνα με τον οποίο ο ελλαδικός χώρος κατατάσσεται στη μέση κατηγορία επικινδυνότητας.

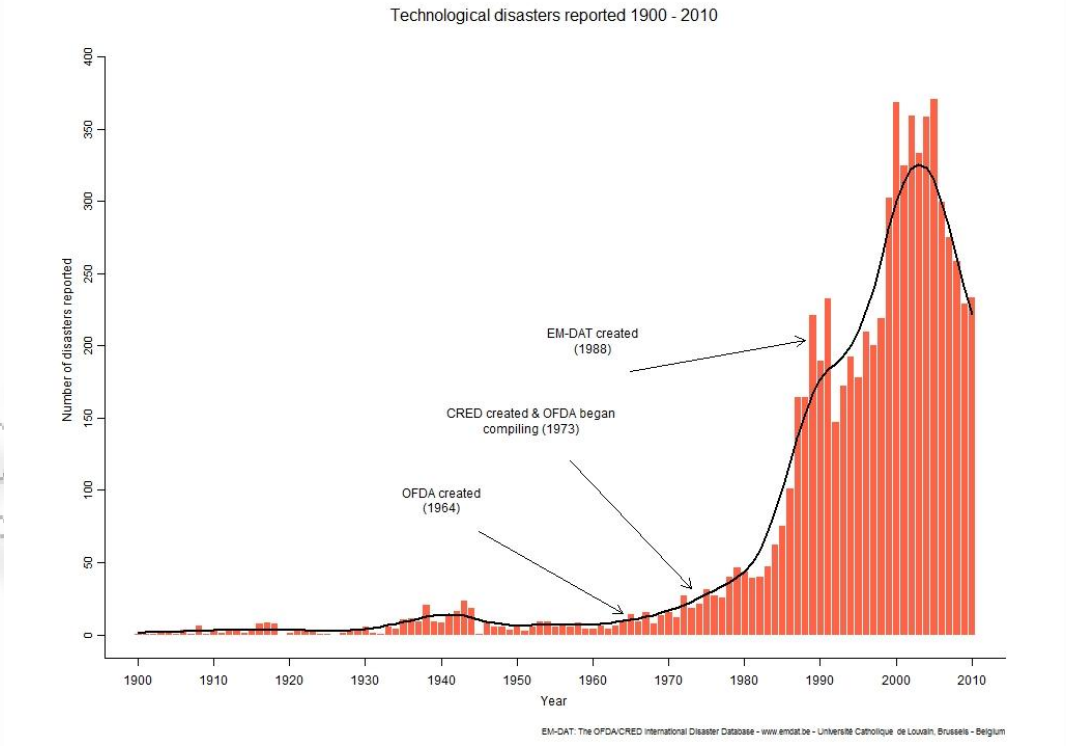


Σχήμα 2: *Γεωγραφική κατανομή φυσικών καταστροφών 1976-2005[5]*

Παράλληλα εξετάζοντας τη συχνότητα των καταστροφών διαχρονικά και σε παγκόσμιο επίπεδο, είτε φυσικών είτε τεχνολογικών, προκύπτει το διάγραμμα του Σχήματος 3 και του Σχήματος 4 αντίστοιχα.



Σχήμα 3: *Καταγραφή φυσικών καταστροφών 1900-2010 [5]*



Σχήμα 4: *Καταγραφή τεχνολογικών καταστροφών 1900-2010 [5]*

Παρατηρούμε ότι και στα δυο διαγράμματα η συχνότητα των καταστροφών παρουσιάζει υψηλή άνοδο από το 1980 και μετά. Αυτό μπορεί να ερμηνευτεί με διάφορους τρόπους όπως:

- Οι οργανισμοί OFDA και CRED ξεκίνησαν τη συνεργασία τους περί το 1973 με τη συστηματική καταγραφή των περιστατικών και τη δημιουργία της βάσης EM-DAT το 1988. Επομένως θεωρείται φυσικό να ανιχνεύεται και να καταγράφεται μεγαλύτερο πλήθος περιστατικών.
- Αναλύοντας κανείς περαιτέρω τα στοιχεία της βάσης EM-DAT των τελευταίων ετών, ανακαλύπτει μεγάλη αύξηση των περιστατικών που έχουν άμεση σχέση με την υπερθέρμανση του πλανήτη όπως είναι οι πλημμύρες και οι τυφώνες.
- Η ραγδαία ανάπτυξη, εισχώρηση και χρήση των τεχνολογιών στην καθημερινότητα έχει ως φυσικό επακόλουθο την αύξηση των τεχνολογικών καταστροφών.

Όποιοι και να είναι οι λόγοι της αύξησης των καταστροφών, γίνεται φανερό ότι θα πρέπει να λαμβάνονται μέτρα με πιο εντατικούς ρυθμούς για την αντιμετώπιση της ολοένα αυξανόμενη συχνότητα εμφάνισης τους, αλλά και λόγω της μεγέθυνσης των επιπτώσεων τους. Η παρατήρηση αυτή θα πρέπει να απασχολήσει ιδιαίτερα όσους δραστηριοποιούνται στον ελλαδικό χώρο καθώς αποτελεί περιοχή αυξημένης επικινδυνότητας.

2.4 Κατηγορίες σχεδίων αντιμετώπισης περιστατικών

Για την εξασφάλιση της επιχειρησιακής συνέχειας, σε περίπτωση κάποιου επιβλαβούς συμβάντος, απαιτείται ο σχεδιασμός και προγραμματισμός ενός μεγάλου εύρους από ενέργειες οι οποίες θα καταστήσουν τον οργανισμό άμεσα λειτουργικό. Για την καλύτερη οργάνωση και σχεδιασμό αυτών των ενεργειών έχουν προταθεί διάφορα «σχέδια αντιμετώπισης» ανάλογα με το σκοπό και το πεδίο στο οποίο αυτά αναφέρονται (πληροφοριακούς πόρους, αντιμετώπιση περιστατικών, διαχείριση κρίσης κ.α.). Παρακάτω δίνεται η περιγραφή και κατηγοριοποίηση των σχεδίων αυτών σύμφωνα με τον NIST [7].

2.4.1 Σχέδιο Επιχειρησιακής Συνέχειας

(Business Continuity Plan-BCP)

Το σχέδιο αυτό περιγράφει τις διαδικασίες οι οποίες πρέπει να ακολουθηθούν από τον οργανισμό ώστε να εξασφαλιστεί η αδιάλειπτη παροχή υπηρεσιών κατά τη διάρκεια αλλά και μετά από ένα καταστροφικό γεγονός. Το σχέδιο αυτό μπορεί να περιλαμβάνει είτε μόνο τη συνέχεια παροχής των κρίσιμων λειτουργιών του οργανισμού είτε να περικλείει όλες τις λειτουργίες του οργανισμού.

2.4.2 Σχέδιο Συνέχειας Λειτουργιών

(Continuity of Operations Plan-COOP)

Το σχέδιο αυτό αναφέρεται στην αποκατάσταση των κρίσιμων λειτουργιών του οργανισμού σε κάποια εναλλακτική τοποθεσία. Ο NIST προτείνει ως στόχο του σχεδίου τη δυνατότητα παροχής των υπηρεσιών έως και 30 ημέρες πριν την πλήρη αποκατάσταση της αρχικής λειτουργίας. Διαφοροποιείται από το BCP στο ότι αφορά κυρίως τις κρίσιμες λειτουργίες και απευθύνεται σε κυβερνητικούς οργανισμούς και υπηρεσίες.

2.4.3 Σχέδιο Επικοινωνιών Κρίσης

(Crisis Communication Plan)

Σε περίπτωση κάποιου περιστατικού το σχέδιο αυτό περιγράφει όλες αυτές τις απαραίτητες διαδικασίες που απαιτούνται για την επικοινωνιακή διευθέτηση του περιστατικού είτε εσωτερικά είτε εξωτερικά του οργανισμού. Στόχος του είναι ο έλεγχος της πληροφορίας με σκοπό την αποφυγή αρνητικής παραπληροφόρησης και συνήθως είναι υπό τη διαχείριση του υπεύθυνου δημοσίων σχέσεων του οργανισμού.

2.4.4 Σχέδιο Προστασίας Κρίσιμων Υποδομών

(Critical Infrastructure Protection Plan-CIP)

Το σχέδιο αυτό αφορά κρίσιμες υποδομές εθνικής σημασίας και περιλαμβάνει σειρά από πολιτικές και διαδικασίες για την προστασία τους από τον κίνδυνο καταστροφών, τον περιορισμό των ευπαθειών αλλά και την αποκατάστασή τους σε περίπτωση προσβολής. Ως κρίσιμες υποδομές ορίζονται αυτές που επηρεάζουν την ασφάλεια, την υγεία ή την οικονομία ενός κράτους.

2.4.5 Σχέδιο Αντιμετώπισης Περιστατικών Κυβερνοχώρου

(Cyber Incident Response Plan-CIRP)

Το σχέδιο CIRP καθορίζει τις διαδικασίες που πρέπει να ακολουθούνται σε περίπτωση προσβολής των πληροφοριακών συστημάτων ενός οργανισμού από κυβερνοεπιθέσεις. Απευθύνεται σε επαγγελματίες πληροφορικής και ασφάλειας πληροφοριακών συστημάτων ώστε να είναι σε θέση για την έγκαιρη αναγνώριση και αποτελεσματική αντιμετώπιση αυτών των ιδιαίτερων απειλών. Συνήθως αυτό το σχέδιο αποτελεί προσάρτημα στο BCP.

2.4.6 Σχέδιο Ανάκαμψης από Καταστροφή

(Disaster Recovery Plan-DRP)

Το Σχέδιο Ανάκαμψης από Καταστροφή αφορά συνήθως καταστροφές μεγάλης έκτασης οι οποίες προσβάλουν κυρίως τα πληροφοριακά συστήματα ενός οργανισμού. Σκοπός του είναι να καθορίσει πολιτικές και διαδικασίες ώστε να διασφαλιστεί η αποκατάσταση και η συνέχιση της λειτουργίας των πληροφοριακών συστημάτων ακόμα και μέσω της μεταγωγής τους σε εναλλακτικές εγκαταστάσεις. Συνήθως συμπληρώνει τα σχέδια BCP ή COOP ενώ μπορεί να συμπεριλαμβάνει επιμέρους σχέδια τύπου ISCP.

2.4.7 Σχέδιο Αντιμετώπισης Καταστροφής Πληροφοριακών Συστημάτων

(Information System Contingency Plan-ISCP)

Στόχος του σχεδίου ISCP είναι η ανάκτηση κάποιου πληροφοριακού συστήματος από μερική ή πλήρη καταστροφή. Περιλαμβάνει αναλυτικά όλα τα ειδικά μέτρα και διαδικασίες που πρέπει να εκτελεστούν για την επαναφορά κάποιο συγκεκριμένου συστήματος χωρίς να είναι απαραίτητη η χρήση εναλλακτικής εγκατάστασης. Συνήθως αποτελεί επιμέρους σχέδιο του DRP.

2.4.8 Σχέδιο Έκτακτης Ανάγκης Παρευρισκομένων

(Occupant Emergency Plan-OEP)

Το σχέδιο OEP περιγράφει όλες εκείνες τις ενέργειες που πρέπει να ακολουθηθούν από τους παρευρισκόμενους (εργαζόμενους-επισκέπτες) σε ένα οργανισμό κατά την εκδήλωση κάποιας καταστροφής. Σκοπός του είναι να καθορίσει τις άμεσες αντιδράσεις των παρευρισκομένων με στόχο την ασφάλεια των ατόμων, του περιβάλλοντος και των

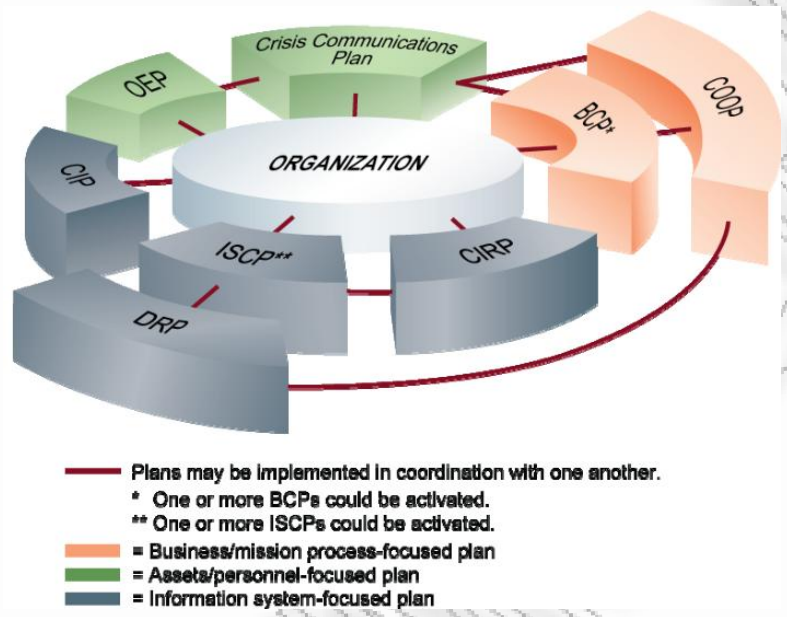
εγκαταστάσεων του οργανισμού. Τα σχέδια αυτά είναι προσαρμοσμένα στις εκάστοτε ιδιαιτερότητες των κτιριακών εγκαταστάσεων του οργανισμού.

Στο Πίνακα 2 αναφέρεται συνοπτικά ο σκοπός, το πεδίο αναφοράς και ο συσχετισμός των σχεδίων αυτών.

Plan	Purpose	Scope	Plan Relationship
Business Continuity Plan (BCP)	Provides procedures for sustaining mission/business operations while recovering from a significant disruption.	Addresses mission/business functions at a lower or expanded level from COOP mission-essential functions.	Mission/business process focused plan that may be activated in coordination with a COOP plan to sustain non-mission-essential functions.
Continuity of Operations (COOP) Plan	Provides procedures and guidance to sustain an organization's mission essential functions at an alternate site for up to 30 days; mandated by federal directives.	Addresses mission-essential functions at a facility; information systems are addressed based only on their support of the mission-essential functions.	Mission-essential functions focused plan that may also activate several business unit-level BCPs, ISCPs, or DRPs, as appropriate.
Crisis Communica-tions Plan	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors.	Addresses communications with personnel and the public; not information system-focused.	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event.
Critical Infrastructure Protection (CIP) Plan	Provides policies and procedures for protection of national critical infrastructure components, as defined in the National Infrastructure Protection Plan.	Addresses critical infrastructure components that are supported or operated by an agency or organization.	Risk management plan that supports COOP plans for organizations with critical infrastructure and key resource assets.
Cyber Incident Response Plan	Provides procedures for mitigating and correcting a cyber attack, such as a virus, worm, or Trojan horse.	Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information.	Information system-focused plan that may activate an ISCP or DRP, depending on the extent of the attack.
Disaster Recovery Plan (DRP)	Provides procedures for relocating information systems operations to an alternate location.	Activated after major system disruptions with long-term effects.	Information system-focused plan that activates one or more ISCPs for recovery of individual systems.
Information System Contingency Plan (ISCP)	Provides procedures and capabilities for recovering an information system.	Addresses single information system recovery at the current or, if appropriate alternate location.	Information system-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP, and/or BCP.
Occupant Emergency Plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat.	Focuses on personnel and property particular to the specific facility; not mission/business process or information system-based.	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation.

Πίνακας 2: *Είδη σχεδίων αντιμετώπισης περιστατικών [7]*

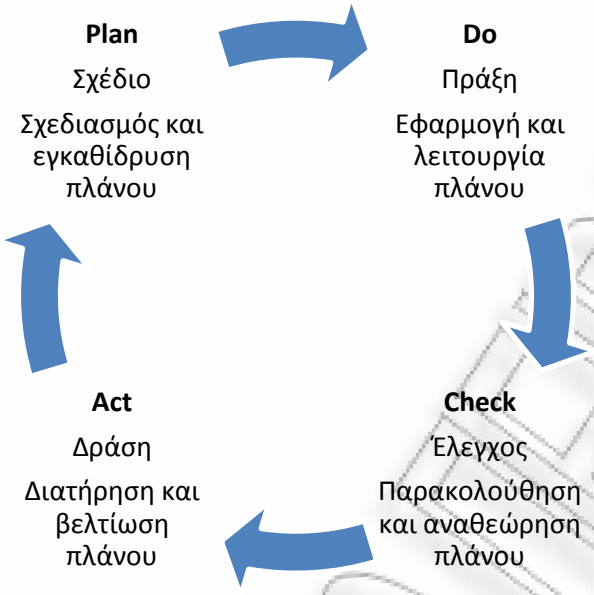
Όπως παρατηρούμε τα σχέδια αυτά δρουν συμπληρωματικά και συνδυαστικά το ένα με το άλλο με στόχο την ολιστική αντιμετώπιση των περιστατικών που μπορεί να θέσουν σε κίνδυνο την λειτουργία κάποιου οργανισμού. Στο Σχήμα 5 απεικονίζεται αυτός ο συσχετισμός σύμφωνα με τον NIST.



Σχήμα 5: *Συσχετισμός σχεδίων αντιμετώπισης περιστατικών [7]*

2.5 Κύκλος ζωής σχεδίων

Κάθε σχέδιο, ως ένα σύνολο από διαδικασίες και ενέργειες, για να είναι αποτελεσματικό δεν θα πρέπει να αντιμετωπίζεται ως ένα στατικό αλλά ως ένα δυναμικά εξελισσόμενο μέτρο προστασίας. Επομένως απαιτείται η συνεχής παρακολούθησή του και η προσαρμογή του στις εκάστοτε συνθήκες. Για να επιτευχθεί αυτό ενδείκνυται η εφαρμογή της μεθοδολογίας του κύκλου του Deming, ή αλλιώς κύκλος PDCA (Plan-Do-Check-Act) όπως είναι ευρέως γνωστή. Η μεθοδολογία αυτή όπως έχει εξελιχθεί σήμερα [8] αποτελείται από τέσσερα επαναλαμβανόμενα βήματα-στάδια, όπως φαίνεται σχηματικά παρακάτω (Σχήμα 6), τα οποία εφαρμοζόμενα στα εκάστοτε σχέδια μπορούν να προσδιορίσουν τον κύκλο ζωής τους.



Σχήμα 6: *Ο κύκλος PDCA*

Αυτά τα βήματα-στάδια εφαρμοζόμενα στα σχέδια ανάκαμψης μπορούν να περιγραφούν συνοπτικά ως εξής:

Plan-Σχέδιο: Το στάδιο κατά το οποίο καθορίζεται-εγκαθιδρύεται το σχέδιο και προσδιορίζονται οι προσδοκώμενοι στόχοι και τα αναμενόμενα αποτελέσματα. Σε αυτό το στάδιο επίσης καθορίζεται και ο τρόπος με τον οποίο θα εκτελεστούν τα βήματα του κύκλου PDCA (ποιός, τι, πού, πότε) ώστε να διασφαλιστεί η επαναληψιμότητά τους και η ανατροφοδότησή του κύκλου.

Do-Πράξη: Στο στάδιο αυτό εφαρμόζεται και τίθεται σε πλήρη λειτουργία το σχέδιο. Καταγράφονται τα προβλήματα και κάθε απροσδόκητο περιστατικό, ενώ παράλληλα ξεκινάει η ανάλυσή τους.

Check-Έλεγχος: Ολοκληρώνεται η ανάλυση των παρατηρήσεων από το προηγούμενο στάδιο (Do) και συγκρίνονται τα αποτελέσματα της εφαρμογής του σχεδίου με αυτά που είχαν προσδιοριστεί κατά το πρώτο στάδιο (Plan). Καταγράφονται οι όποιες διαφορές-αποκλίσεις και γίνεται προσπάθεια εξαγωγής συμπερασμάτων για να χρησιμοποιηθούν στο επόμενο στάδιο.

Act-Δράση: Γίνεται ανασκόπηση των συμπερασμάτων από το προηγούμενο στάδιο (Check), αναλύονται τα αίτια στα οποία οφείλονται οι όποιες αποκλίσεις και αποφασίζονται οι

διορθωτικές ενέργειες-βελτιώσεις που απαιτούνται ώστε να αντιμετωπιστούν αποτελεσματικά. Στο στάδιο αυτό πραγματοποιείται και η ανασκόπηση της αποτελεσματικότητας του ίδιου του κύκλου PDCA ο οποίος αφού διορθωθεί, εφόσον απαιτείται, δίδεται το έναυσμα για την εφαρμογή ενός νέου κύκλου.

Ο κύκλος PDCA θεωρείται επιτυχής όταν με την ολοκλήρωσή του (στάδιο Act) υπεισέρχονται είτε διορθωτικές είτε βελτιωτικές ενέργειες. Σε περίπτωση που δεν προκύψει κάποιο από τα παραπάνω θεωρείται ότι είτε κάποιο στάδιο δεν εκτελέστηκε σωστά είτε ότι δεν έχει προσδιοριστεί με την απαιτούμενη λεπτομέρεια. Επομένως ο κύκλος PDCA αποτελεί μια ιδανική μεθοδολογία για τη συνεχή αξιολόγηση και βελτίωση των σχεδίων.

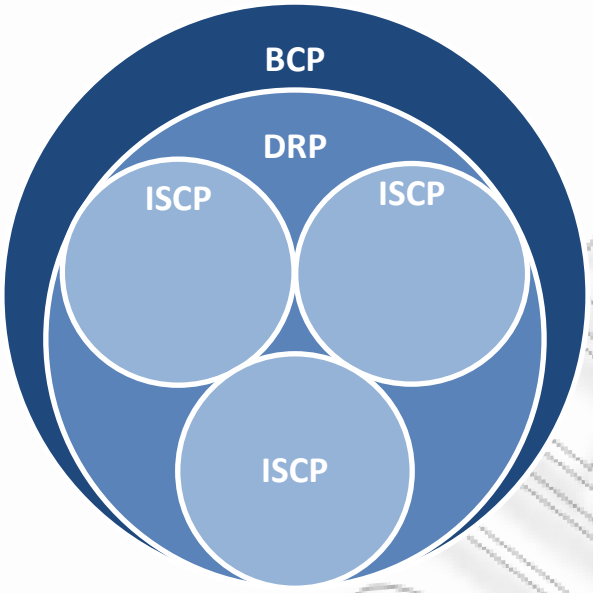
3 Ειδικά θέματα Σχεδιασμού Ανάκαμψης από Καταστροφές

3.1 Η σημασία του ΣΑΚ και η σχέση του με την Επιχειρησιακή Συνέχεια

Είναι συχνό φαινόμενο πολλές φορές να συγχέεται το Σχέδιο Ανάκαμψης από Καταστροφές (ΣΑΚ-DRP) με το Σχέδιο Επιχειρησιακής Συνέχειας (BCP) και το Σχέδιο Αντιμετώπισης Καταστροφής Πληροφοριακών Συστημάτων (ISCP). Σύμφωνα και με τα όσα περιγράφονται στην §2.4 οι βασικές έννοιες που αφορούν τα σχέδια αυτά είναι οι κάτωθι:

- **Επιχειρησιακή συνέχεια (BCP):** αφορά στην ικανότητα να διατηρείται ένα αποδεκτό επίπεδο λειτουργικότητας του οργανισμού ακόμα και σε περίπτωση καταστροφής.
- **Ανάκαμψη από καταστροφές (DRP):** αφορά στην ικανότητα άμεσης απόκρισης σε περίπτωση ολικής καταστροφής των Πληροφοριακών Συστημάτων, που υποστηρίζουν κρίσιμες λειτουργίες του οργανισμού, και στην ανάκαμψή τους εντός προκαθορισμένου χρόνου.
- **Αντιμετώπιση καταστροφών ΠΣ (ISCP):** αφορά στη ικανότητα ανάκτησης κάποιου ΠΣ ύστερα από μερική ή ολική καταστροφή του.

Παρατηρούμε ότι ενώ το BCP αναφέρεται κυρίως στις παρεχόμενες υπηρεσίες-λειτουργίες και στην συνέχιση της παροχής τους μετά από κάποιο συμβάν, το DRP αναφέρεται κυρίως στα Πληροφοριακά Συστήματα τα οποία υποστηρίζουν αυτές τις παρεχόμενες υπηρεσίες-λειτουργίες και στον τρόπο με τον οποίο αυτά μπορούν να επιστρέψουν σε κανονική λειτουργία μετά από κάποια καταστροφή. Επομένως μπορεί να θεωρηθεί ότι το DRP αποτελεί μέρος ενός ευρύτερου σχεδίου BCP. Αντίστοιχα το DRP με τη σειρά του μπορεί να περικλείει το σύνολο των ISCP που αφορούν σε κάθε διακριτό Πληροφοριακό Σύστημα (Σχήμα 7).



Σχήμα 7: *Σχέση DRP με BCP και ISCP*

Η ραγδαία αύξηση των καταστροφικών περιστατικών τα τελευταία χρόνια, όπως παρουσιάζεται και στην §2.3, έχει ως φυσικό επακόλουθο την αύξηση της επικινδυνότητας για την καταστροφή των Πληροφοριακών Συστημάτων που εξυπηρετούν τις κρίσιμες λειτουργίες κάποιου οργανισμού. Ωστόσο πολλά κέντρα δεδομένων δεν είναι σωστά προετοιμασμένα για μια τέτοια πιθανότητα καταστροφής. Σύμφωνα με έρευνα που διεξήγαγε η AFCOM [9] σε 358 διαχειριστές κέντρων δεδομένων ανά τον κόσμο:

- Πάνω από 15% των ερωτηθέντων δεν διαθέτουν συγκροτημένο σχέδιο για τη λήψη και ανάκτηση δεδομένων
- 50% δεν διαθέτουν σχέδιο για την αντικατάσταση εξοπλισμού που μπορεί να πληγεί από ενδεχόμενη καταστροφή
- Περίπου 65% δεν έχουν κανένα σχέδιο για την αντιμετώπιση κυβερνο-εγκληματιών

Παράλληλα ένα μεγάλο ποσοστό των επιχειρήσεων των οποίων οι λειτουργίες αναστέλλονται, λόγω μη διαθεσιμότητας των Πληροφοριακών τους Συστημάτων, αναγκάζονται να κηρύξουν πτώχευση αν δεν επιτύχουν την ανάκαμψή τους μέσα σε σύντομο χρονικό διάστημα.

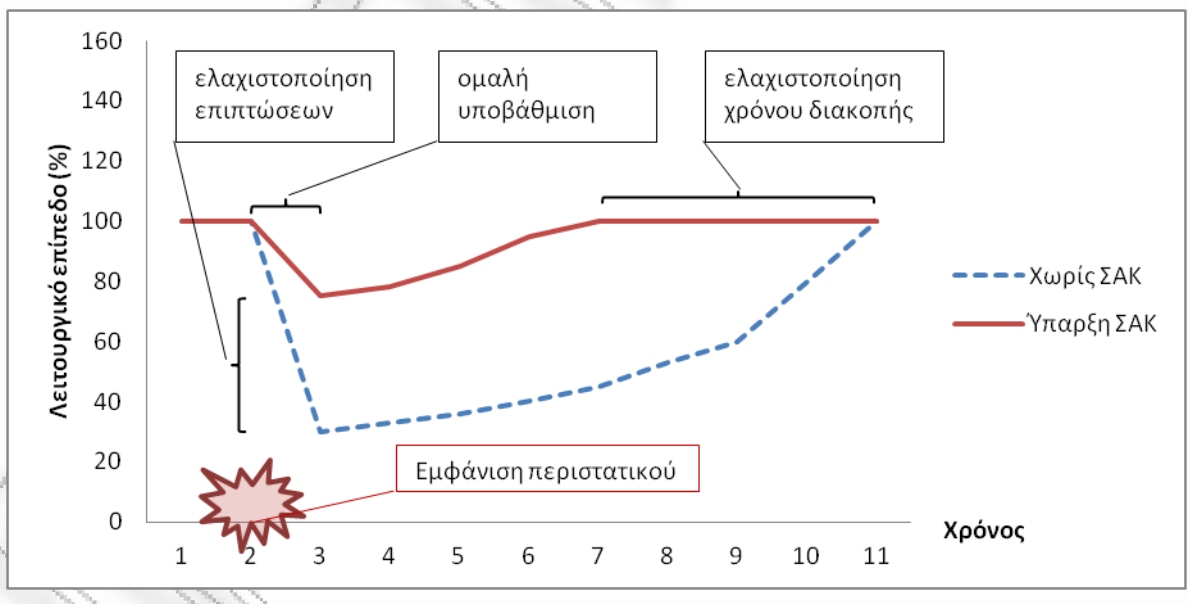
Παρατηρούμε λοιπόν ότι είναι επιτακτική η ανάγκη για την εφαρμογή μέτρων για τη διασφάλιση της επιχειρησιακής συνέχειας σε περίπτωση καταστροφής. Αυτά τα μέτρα πρέπει να αναφέρονται τόσο στο πεδίο της πρόληψης πριν την εκδήλωση μιας

καταστροφής, όσο και στη συνέχιση των κρίσιμων λειτουργιών κατά τη διάρκεια της καταστροφής αλλά και στην ανάκτηση μετά το πέρας της.

Την παραπάνω ανάγκη καλείται να καλύψει η εφαρμογή ενός Σχεδίου Ανάκαμψης από Καταστροφές, το οποίο έχει σαν κύριους στόχους:

- την έγκαιρη ανίχνευση μιας καταστροφής
- την ελαχιστοποίηση των επιπτώσεων μιας καταστροφής
- την ομαλή υποβάθμιση των λειτουργιών από την εμφάνιση ενός περιστατικού
- την ελαχιστοποίηση του χρόνου διακοπής και αποκατάστασης των ΠΣ
- την εύρεση εναλλακτικών μέσων συνέχισης των λειτουργιών των ΠΣ
- τη διασφάλιση της ύπαρξης προκαθορισμένων και κατανοητών διαδικασιών για την αντιμετώπιση των περιστατικών
- την εκπαίδευση του προσωπικού με σκοπό την αντιμετώπιση εκτάκτων περιστατικών και την εξοικείωσή του με συνθήκες έκτακτης ανάγκης

Στο Σχήμα 8 παρουσιάζεται η αναμενόμενη επίδραση από την ύπαρξη και εφαρμογή ενός ΣΑΚ, κατά την εμφάνιση ενός καταστροφικού συμβάντος.



Σχήμα 8: *Επίδραση ύπαρξης ΣΑΚ σε περίπτωση καταστροφής*

Παρατηρούμε ότι, σε περίπτωση καταστροφής, η ύπαρξη ενός ΣΑΚ αναμένεται να βελτιώσει σε μεγάλο βαθμό τόσο τον χρόνο ανάκαμψης όσο και τη διατήρηση της

λειτουργικότητας σε ανεκτό επίπεδο. Η αξία που προσφέρουν τα μέτρα αυτά στους οργανισμούς γίνεται φανερή και από το γεγονός ότι πολλές φορές οι ασφαλιστικές εταιρείες προσφέρουν εκπτώσεις όταν εφαρμόζονται επαρκή μέτρα ανάκαμψης και επιχειρησιακής συνέχειας. Ιδίως στην Ιαπωνία, όπου παρά τις συχνές φυσικές καταστροφές η υιοθέτηση μέτρων επιχειρησιακής συνέχειας παραμένει χαμηλότερη από 20%, η Τράπεζα Ανάπτυξης της Ιαπωνίας αποφάσισε να προσφέρει ακόμα και δάνειο «Πρόληψης Καταστροφών», με μειωμένο επιτόκιο, για την ανάπτυξη και εφαρμογή μέτρων αντιμετώπισης [10].

Ένα Σχέδιο Ανάκαμψης από Καταστροφές, πέρα από την αξία του ως μέτρο αντιμετώπισης των επιπτώσεων από μια ενδεχόμενη καταστροφή, μπορεί να προσδώσει και μεγάλο βαθμό «επιχειρησιακής ευελιξίας» σε έναν οργανισμό. Στο πλέον διεθνοποιημένο οικονομικό περιβάλλον όπου η δράση των επιχειρήσεων απλώνεται σε διάφορα κράτη, οπού επικρατούν διαφορετικές οικονομικές-κοινωνικές-πολιτικές συνθήκες, ένα ΣΑΚ μπορεί να αποτελέσει κρίσιμο και αποτελεσματικό εργαλείο για τη άμεση μεταφορά της επιχειρησιακής λειτουργίας σε πιο ασφαλή επιχειρηματικά περιβάλλοντα, εφόσον αυτό απαιτηθεί.

3.2 Ασφάλεια πληροφοριών και ΣΑΚ

Η διαχείριση και διατήρηση της ασφάλειας πληροφοριών αποτελεί ολοένα και μεγαλύτερη προτεραιότητα καθώς με την αύξηση της διείσδυσης των νέων τεχνολογιών, λαμβάνοντας σταδιακά τη μορφή του «απανταχού υπολογίζειν», παρουσιάζεται και αλματώδης αύξηση στους κινδύνους που απειλούν τα ηλεκτρονικά δεδομένα. Οι κίνδυνοι αυτοί συνήθως απειλούν το τρίπτυχο από το οποίο ορίζεται άτυπα η έννοια της ασφάλειας πληροφοριών [11]:

- Εμπιστευτικότητα (Confidentiality): αποτροπή αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένα άτομα
- Ακεραιότητα (Integrity): αποτροπή μη αναστρέψιμης μεταβολής ή διαγραφής δεδομένων και με τρόπο που δε μπορεί να γίνει αντιληπτός.
- Διαθεσιμότητα (Availability): αποτροπή της μη διαθεσιμότητας των πληροφοριών όποτε απαιτούνται.

Σχήμα 9: *Συστατικά στοιχεία ασφάλειας πληροφοριών*

Σήμερα οι αυξημένες απαιτήσεις πρόσβασης σε πληροφορίες έχουν εξελίξει την έννοια της διαθεσιμότητας, από τη δυνατότητας ανάκαμψης από καταστροφές σε δυνατότητα συνεχούς και ανεπηρέαστης λειτουργίας.

Σύμφωνα με τα παραπάνω ένα Σχέδιο Ανάκαμψης από Καταστροφές έρχεται να αντιμετωπίσει κυρίως τη διαθεσιμότητα και δευτερευόντως την ακεραιότητα των πληροφοριών, που βρίσκονται σε ηλεκτρονική μορφή ή διακινούνται με ηλεκτρονικά μέσα, διατηρώντας παράλληλα και την εμπιστευτικότητά τους κατά την εφαρμογή του.

3.3 Νομικά θέματα

Πολλοί οργανισμοί θεωρούν τον σχεδιασμό και την υλοποίηση μέτρων ανάκαμψης από καταστροφές ως ένα πρόβλημα που αφορά μόνο την υπηρεσία Πληροφορικής τείνοντας να το αντιμετωπίζουν ως ένα ακόμα πρόσθετο, και πιθανόν περιττό, κόστος για τον οργανισμό. Αγνοούν έτσι ότι η ύπαρξη σχεδίου ανάκαμψης από καταστροφές σε πολλές περιπτώσεις πέρα από βελτιωτικό μέτρο μπορεί να αποτελεί, με έμμεσο τρόπο, ακόμα και νομική ή κανονιστική απαίτηση. Ιδίως σε οργανισμούς οι οποίοι δραστηριοποιούνται σε κρίσιμους τομείς όπως ο δημόσιος, η κοινή ωφέλεια, ο χρηματοπιστωτικός και η υγεία.

Αν και δεν υπάρχει κάποιος νόμος ο οποίος να επιβάλλει ρητά την ύπαρξη ΣΑΚ, υπάρχουν αρκετοί οι οποίοι επιβάλλουν στους οργανισμούς, ως υποχρέωση, την διασφάλιση της διαθεσιμότητας και της ακεραιότητας των δεδομένων που διαχειρίζονται. Επομένως στα πλαίσια της εφαρμοστικής ερμηνείας τους προϋποθέτουν την ύπαρξή κατάλληλων μέτρων, όπως είναι το ΣΑΚ, για την αντιμετώπιση και την ανάκαμψη από καταστροφές που πλήττουν τα Πληροφοριακά τους Συστήματα.

Σε περίπτωση που ένας οργανισμός οδηγηθεί στη δικαιοσύνη, σχετικά με τη μη τήρηση κατάλληλων μέτρων για την προστασία από καταστροφή των κρίσιμων λειτουργιών ή των δεδομένων που διαχειρίζεται, τα δικαστήρια θα αξιολογήσουν την ευθύνη που προκύπτει από την πιθανότητα καταστροφής και το μέγεθος των επιπτώσεων συναρτήσει του κόστους της λήψης μέτρων αντιμετώπισης. Εκτιμάται ότι υπάρχει σαφές νομικό προηγούμενο, προς αξιοποίηση από τα δικαστήρια, για να κριθεί κατά πόσο ο οργανισμός φρόντισε ή παραμέλησε να λάβει όλα τα εύλογα μέτρα για τον περιορισμό της ζημιάς που προκλήθηκε από την καταστροφή [12].

Εστιάζοντας κυρίως στο ευρωπαϊκό νομοθετικό πλαίσιο, όπως αυτό εκφράζεται μέσα από σχετικούς κανονισμούς και οδηγίες, και στον τρόπο που αυτό μεταφέρεται και ενσωματώνεται στο ελληνικό δίκαιο [13] παρουσιάζονται παρακάτω όλες οι σχετικές με ΣΑΚ νομικές ή/και κανονιστικές απαιτήσεις. Για λόγους ευκολίας κατατάσσονται ανάλογα με το δεσμευτικό τους χαρακτήρα τους σε νομικές δεσμεύσεις, απαιτήσεις συμμόρφωσης και απλές συστάσεις.

Όνομα	Έτος	Τίτλος	Αντικείμενο	Αφορά	Χαρακτήρας	Άρθρα σχετικά με ΣΑΚ	Ενσωμάτωση σε ελληνικό δίκαιο
Οδηγία 95/46/ΕΚ	1995	"για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών"	Προστασία επεξεργασίας δεδομένων προσωπικού χαρακτήρα	Κράτη μέλη (ΕΚ)	Νομική Δέσμευση	17, 25	v.2472/1997
Κανονισμός 45/2001	2001	"σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών"	Προστασία επεξεργασίας δεδομένων προσωπικού χαρακτήρα	Όργανα και οργανισμούς (ΕΚ)	Νομική Δέσμευση	9, 22, 23, 35	-
Οδηγία 2002/22/ΕΚ (Τροποποίηση με 2009/136/εκ)	2002	"για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών" (οδηγία καθολικής υπηρεσίας)	Εξασφάλιση διαθεσιμότητας και καλής ποιότητας παροχής δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών σε ολόκληρη την Κοινότητα	Παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίου δικτύου επικοινωνιών (ΕΚ)	Νομική Δέσμευση	23	v.3431/2006 (Τροποποίηση με v.4070/2012)
Οδηγία 2002/58/ΕC (Τροποποίηση με 2009/136/εκ)	2002	"σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών" (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)	Προστασία επεξεργασίας δεδομένων προσωπικού χαρακτήρα	Παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίου δικτύου επικοινωνιών (ΕΚ)	Νομική Δέσμευση	4	v.3471/2006 (Τροποποίηση με v.4070/2012)
Οδηγία 2006/24/ΕΚ	2006	"για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ"	Διατήρηση δεδομένων, συμπεριλαμβανομένου δεδομένων κίνησης και θέσης, ώστε να διασφαλιστεί η διερεύνηση, διαπίστωση και δίωξη σοβαρών ποινικών αδικημάτων.	Παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίου δικτύου επικοινωνιών (ΕΚ)	Νομική Δέσμευση	7, 8	v.3917/2011
Οδηγία 2008/114/ΕΚ	2008	"σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους"	Προσδιορισμός ευρωπαϊκών υποδομών ζωτικής σημασίας (ΕΥΖΣ), και προστασίας τους	Ευρωπαϊκές υποδομές ζωτικής σημασίας (ΕΥΖΣ) (ΕΚ)	Νομική Δέσμευση	5, ΠΑΡΑΡΤΗΜΑ ΙΙ	ΕΝΣΩΜΑΤΩΘΗΚΕ πλήρως με ΠΔ 39/2011
Council of Europe (CoE)	1981	"Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data"	Προστασία επεξεργασίας δεδομένων προσωπικού χαρακτήρα	Κράτη μέλη (CoE)	Απαίτηση	7	-
Safe Harbor Framework	2000	"Safe Harbour Privacy Principles"	Προστασία επεξεργασίας δεδομένων προσωπικού χαρακτήρα και διακίνηση τους μεταξύ ΕΕ και Η.Π.Α.	Οργανισμούς των Η.Π.Α. που επιθυμούν εμπορικές συνεργασίες με κράτη μέλη της ΕΕ που αφορούν προσωπικά δεδομένα	Απαίτηση		-
OECD Guidelines (ΟΟΣΑ)	1980	"Recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data"	Προστασία επεξεργασίας δεδομένων προσωπικού χαρακτήρα	Κράτη μέλη (ΟΟΣΑ)	Σύσταση	11, 16	-
UN Guidelines (ΟΗΕ)	1990	"for the Regulation of Computerized Personal Data Files"	Προστασία επεξεργασίας δεδομένων προσωπικού χαρακτήρα	Κράτη μέλη (ΟΗΕ)	Σύσταση	7	-
OECD Guidelines (ΟΟΣΑ)	2002	"Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security"	Προαγωγή κουλτούρας για την ασφάλεια και προστασία των πληροφοριακών συστημάτων και δικτύων	Κράτη μέλη (ΟΟΣΑ)	Σύσταση	3, 8	-

Πίνακας 3: *Σύνοψη νομικών/κανονιστικών απαιτήσεων*

3.3.1 Νομικές δεσμεύσεις

- **Οδηγία 95/46/ΕΚ -** ***"για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών"*** [14]

Η οδηγία αυτή αποτελεί την πρώτη προσπάθεια δεσμευτικού χαρακτήρα της Ευρωπαϊκής Κοινότητας για την προστασία των προσωπικών δεδομένων. Αναφέρεται στην αναγκαιότητα ύπαρξης κατάλληλων μέτρων για την προστασία των δεδομένων αυτών, ανάμεσα στα οποία μπορούμε να δεχτούμε ότι ανήκουν και όσα προβλέπονται από ένα σχέδιο ανάκαμψης από καταστροφές. Συγκεκριμένα περιγράφεται:

«...Άρθρο 17

Ασφάλεια της επεξεργασίας

1. Τα κράτη μέλη προβλέπουν ότι ο υπεύθυνος της επεξεργασίας πρέπει να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία από τυχαία ή παράνομη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση, ιδίως εάν η επεξεργασία συμπεριλαμβάνει και διαβίβαση των δεδομένων μέσων δικτύου, και από κάθε άλλη μορφή αθέμιτης επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Τα μέτρα αυτά πρέπει να εξασφαλίζουν, λαμβανομένης υπόψη της τεχνολογικής εξέλιξης και του κόστους εφαρμογής τους, επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που απορρέουν από την επεξεργασία και τη φύση των δεδομένων που απολαύουν προστασίας.

2. Τα κράτη μέλη προβλέπουν ότι ο υπεύθυνος της επεξεργασίας οφείλει, σε περίπτωση επεξεργασίας για λογαριασμό του, να επιλέγει προς εκτέλεση της επεξεργασίας πρόσωπο το οποίο παρέχει επαρκείς εγγυήσεις όσον αφορά τα μέτρα τεχνικής ασφάλειας και οργάνωσης της επεξεργασίας και να εξασφαλίζει την τήρηση των μέτρων αυτών.

3. Η εκτέλεση επεξεργασίας μέσω άλλου προσώπου πρέπει να διέπεται από σύμβαση ή δικαιοπραξία που συνδέει τον εκτελούντα με τον υπεύθυνο της επεξεργασίας και προβλέπει ιδίως:

- ότι ο εκτελών την επεξεργασία ενεργεί μόνον κατ'εντολήν του υπευθύνου της επεξεργασίας,

- ότι οι υποχρεώσεις που προβλέπονται στην παράγραφο 1, όπως ορίζονται από τη νομοθεσία του κράτους μέλους στο οποίο είναι εγκατεστημένος ο εκτελών την επεξεργασία, βαρύνουν και τον εκτελούντα την επεξεργασία.

4. Για αποδεικτικούς λόγους, τα τμήματα της σύμβασης ή δικαιοπραξίας που αφορούν την προστασία των δεδομένων και τις απαιτήσεις σχετικά με τα μέτρα που προβλέπονται στην παράγραφο 1 καταρτίζονται εγγράφως ή σε άλλη ανάλογη μορφή. [...]

ΚΕΦΑΛΑΙΟ IV ΔΙΑΒΙΒΑΣΗ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΠΡΟΣ ΤΡΙΤΕΣ ΧΩΡΕΣ

Άρθρο 25

Βασικές αρχές

1. Τα κράτη μέλη προβλέπουν ότι η διαβίβαση προς τρίτη χώρα δεδομένων προσωπικού χαρακτήρα, που έχουν υποστεί επεξεργασία ή πρόκειται να υποστούν επεξεργασία μετά τη διαβίβασή τους, επιτρέπεται μόνον εάν, τηρουμένων των εθνικών διατάξεων που θεσπίζονται σύμφωνα με τις λοιπές διατάξεις της παρούσας οδηγίας, η εν λόγω τρίτη χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας.

2. Η επάρκεια της προστασίας που παρέχεται από τρίτη χώρα σταθμίζεται λαμβανομένων υπόψη όλων των περιστάσεων που επηρεάζουν μια διαβίβαση ή κατηγορία διαβιβάσεων δεδομένων 7 ειδικότερα, εξετάζονται η φύση των δεδομένων, οι σκοποί και η διάρκειά της ή των προβλεπομένων επεξεργασιών, η χώρα προέλευσης και τελικού προορισμού, οι γενικοί ή τομεακοί κανόνες δικαίου, οι επαγγελματικοί κανόνες και τα μέτρα ασφαλείας που ισχύουν στην εν λόγω τρίτη χώρα....»

Παρατηρούμε ότι η απαίτηση για κατάλληλα μέτρα προστασίας από καταστροφές υπάρχει τόσο για τον ίδιο τον οργανισμό που διαχειρίζεται τα προσωπικά δεδομένα αλλά και για τυχόν τρίτους που εμπλέκονται, απαιτώντας την ύπαρξη έγγραφων δεσμεύσεων.

Η οδηγία αυτή ενσωματώθηκε στο ελληνικό δίκαιο με τον νόμο 2472/1997 [15], όπου αναφέρεται ότι:

«...Άρθρο 10

Απόρρητο και ασφάλεια της επεξεργασίας

1. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απόρρητη. Διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνον κατ' εντολή του.

2. Για τη διεξαγωγή της επεξεργασίας ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου.

3. Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Με την επιφύλαξη άλλων διατάξεων, η Αρχή παρέχει οδηγίες ή εκδίδει κανονιστικές πράξεις σύμφωνα με το άρθρο 19 παρ. 1 ι' για τη ρύθμιση θεμάτων σχετικά με τον βαθμό ασφαλείας των

δεδομένων και των υπολογιστικών και επικοινωνιακών υποδομών, τα μέτρα ασφάλειας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία και επεξεργασία δεδομένων, καθώς και για τη χρήση τεχνολογιών ενίσχυσης της ιδιωτικότητας.

4. Αν η επεξεργασία διεξάγεται για λογαριασμό του υπεύθυνου από πρόσωπο μη εξαρτώμενο από αυτόν, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως. Η ανάθεση προβλέπει υποχρεωτικά ότι ο ενεργών την επεξεργασία την διεξάγει μόνο κατ' εντολή του υπεύθυνου και ότι οι λοιπές υποχρεώσεις του παρόντος άρθρου βαρύνουν αναλόγως και αυτόν...»

Με τον ίδιο νόμο προβλέπονται τόσο διοικητικές και ποινικές κυρώσεις, όσο και αστική ευθύνη για τους οργανισμούς που δεν τηρούν όσα περιγράφονται. Ο ίδιος νόμος ίδρυσε την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), ως ανεξάρτητη διοικητική αρχή, η οποία εκδίδει κανονιστικές πράξεις υποχρεωτικού χαρακτήρα σχετικά με μέτρα που αφορούν την προστασία των προσωπικών δεδομένων. Η Αρχή κάνει ιδιαίτερη μνεία στην αναγκαιότητα ύπαρξης σχεδίου ανάκαμψης από καταστροφές [16], όπου χαρακτηριστικά αναφέρει:

«...

Η κατάρτιση πολιτικής ασφαλείας, σχεδίου ασφαλείας και σχεδίου ανάκαμψης από καταστροφές κρίνεται απαραίτητη για την ασφαλή επεξεργασία και προστασία των προσωπικών δεδομένων[...]

Το Σχέδιο Ανάκαμψης από Καταστροφές (Disaster Recovery and Contingency Plan) είναι το έγγραφο που αναφέρεται στα μέτρα προστασίας, ανάκαμψης και αποκατάστασης πληροφοριακών συστημάτων και τεχνολογικών υποδομών σε περιπτώσεις έκτακτης ανάγκης, όπως φυσικές καταστροφές, εξωτερικές επιθέσεις/εισβολές, κ.λπ.

Το σχέδιο αυτό είναι απαραίτητο για την αποτύπωση των διαδικασιών και των τεχνικών μέτρων που πρέπει να εφαρμόσει ο υπεύθυνος επεξεργασίας για την προστασία των προσωπικών δεδομένων σε περίπτωση κάποιου έκτακτου περιστατικού...»

- **Κανονισμός 45/2001/ΕΚ - *"σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών"*** [17]

Ο κανονισμός αυτός αποτελεί ειδική εφαρμογή της οδηγίας 95/46/ΕΚ και αφορά στην λειτουργία των οργάνων και οργανισμών της Ευρωπαϊκής Κοινότητας. Με τον κανονισμό αυτό γίνεται εμφανής η ιδιαίτερη σημασία που δίνει η Κοινότητα στην ύπαρξη μέτρων προστασίας. Χαρακτηριστικά αναφέρεται:

«...Άρθρο 9

Διαβίβαση δεδομένων προσωπικού χαρακτήρα προς αποδέκτες άλλους , εκτός από τα όργανα και τους οργανισμούς της Κοινότητας , οι οποίοι δεν υπόκεινται στην οδηγία 95/46/ΕΚ

1. Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς αποδέκτες άλλους, εκτός από τα όργανα και τους οργανισμούς της Κοινότητας, οι οποίοι δεν υπόκεινται στην εθνική νομοθεσία που θεσπίζεται κατ' εφαρμογή της οδηγίας 95/46/ΕΚ, επιτρέπεται μόνον εφόσον διασφαλίζεται επαρκής βαθμός προστασίας στη χώρα του αποδέκτη ή στο πλαίσιο του

αποδέκτη διεθνούς οργανισμού και εφόσον η διαβίβαση αποβλέπει αποκλειστικά στο να διευκολύνει την εκτέλεση καθήκοντος που εμπίπτει στην αρμοδιότητα του υπεύθυνου της επεξεργασίας[...]

Άρθρο 22

Ασφάλεια της επεξεργασίας

1. Λαμβάνοντας υπόψη την πρόοδο της επιστήμης και το σχετικό κόστος εφαρμογής, ο υπεύθυνος της επεξεργασίας εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την κατοχύρωση κατάλληλου βαθμού ασφάλειας ενόψει των κινδύνων της επεξεργασίας και της φύσης των δεδομένων προσωπικού χαρακτήρα που πρέπει να προστατευθούν. Τα μέτρα αυτά λαμβάνονται ιδίως για να αποτρέπεται οποιαδήποτε μη επιτρεπόμενη διαβίβαση ή πρόσβαση, τυχαία ή παράνομη καταστροφή ή τυχαία απώλεια ή αλλοίωση, καθώς και οιαδήποτε άλλη μορφή παράνομης επεξεργασίας.

2. Όταν τα δεδομένα προσωπικού χαρακτήρα αποτελούν αντικείμενο αυτοματοποιημένης επεξεργασίας, λαμβάνονται μέτρα, εφόσον απαιτούνται, ανάλογα με τον κίνδυνο, ιδίως με σκοπό:

[...]

ι) η εσωτερική οργανωτική δομή ενός οργάνου ή οργανισμού να σχεδιάζεται κατά τρόπο ώστε να πληρούνται οι ειδικές προϋποθέσεις που ισχύουν για την προστασία των δεδομένων.

Άρθρο 23

Επεξεργασία δεδομένων προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας

1. Ο υπεύθυνος της επεξεργασίας οφείλει, σε περίπτωση που η επεξεργασία πραγματοποιείται για λογαριασμό του, να επιλέγει ως εκτελούντα την επεξεργασία ένα πρόσωπο το οποίο να παρέχει επαρκείς εγγυήσεις όσον αφορά τα τεχνικά και οργανωτικά μέτρα ασφάλειας που προβλέπονται από το άρθρο 22 και να μεριμνά για την τήρηση των μέτρων αυτών.

2. Η εκτέλεση επεξεργασιών μέσω ανάθεσης της εκτέλεσης της επεξεργασίας πρέπει να διέπεται από σύμβαση ή νομική πράξη η οποία να συνδέει τον εκτελούντα την επεξεργασία με τον υπεύθυνο της επεξεργασίας και να προβλέπει ιδίως:

α) ότι ο εκτελών την επεξεργασία ενεργεί μόνον κατ' εντολή του υπευθύνου της επεξεργασίας,

β) ότι οι υποχρεώσεις που προβλέπονται στα άρθρα 21 και 22 βαρύνουν και τον εκτελούντα την επεξεργασία, εκτός εάν, δυνάμει του άρθρου 16 ή του άρθρου 17 παράγραφος 3, δεύτερη περίπτωση της οδηγίας 95/46/ΕΚ, ο εκτελών την επεξεργασία υπόκειται ήδη σε υποχρεώσεις περί εμπιστευτικότητας και ασφαλείας που προβλέπονται από την εθνική νομοθεσία ενός κράτους μέλους.

3. Για τους σκοπούς της διατήρησης των αποδείξεων, τα τμήματα της σύμβασης ή της νομικής πράξης που αφορούν την προστασία των δεδομένων και τις προϋποθέσεις σχετικά με τα μέτρα που προβλέπονται στο άρθρο 22, καταρτίζονται εγγράφως ή υπό άλλη ισοδύναμη μορφή[...]

Άρθρο 35

Ασφάλεια

1. Τα όργανα και οι οργανισμοί της Κοινότητας λαμβάνουν <u>τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα</u> με σκοπό την κατοχύρωση της ασφαλούς χρήσης των τηλεπικοινωνιακών δικτύων και του τερματικού εξοπλισμού, ενδεχομένως σε συνεννόηση με τους φορείς παροχής κοινόχρηστων τηλεπικοινωνιακών υπηρεσιών ή τους φορείς παροχής δημόσιων τηλεπικοινωνιακών δικτύων. Τα εν λόγω μέτρα είναι ικανά να κατοχυρώνουν ένα βαθμό ασφάλειας ανάλογο με το μέγεθος του κινδύνου, λαμβανομένης υπόψη της πλέον πρόσφατης επιστημονικής προόδου και του κόστους της εφαρμογής των εν λόγω μέτρων.

2. Όταν συντρέχει ιδιαίτερος κίνδυνος παραβίασης της ασφάλειας του δικτύου και του τερματικού εξοπλισμού, το οικείο όργανο ή οργανισμός της Κοινότητας ενημερώνει τους χρήστες του δικτύου για τον κίνδυνο αυτό, καθώς και για τα μέτρα που είναι δυνατόν να άρουν τον κίνδυνο και τα εναλλακτικά μέσα επικοινωνίας που μπορούν να χρησιμοποιηθούν...»

- **Οδηγία 2002/22/ΕΚ -** ***"για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών" (οδηγία καθολικής υπηρεσίας)*** [18]

Με την οδηγία αυτή επιχειρείται η εξασφάλιση της διαθεσιμότητας και του επιπέδου παροχής ηλεκτρονικών υπηρεσιών και υπηρεσιών δικτύου. Αφορά τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών και διαχείρισης δημοσίων δικτύων επικοινωνιών που δραστηριοποιούνται στα κράτη-μέλη της Ευρωπαϊκής Κοινότητας. Τροποποιήθηκε με την οδηγία 2009/136/ΕΚ [19] και αναφέρει σχετικά με την αναγκαιότητα ύπαρξης μέτρων αντιμετώπισης καταστροφών:

«...Άρθρο 23

Διαθεσιμότητα των υπηρεσιών

Τα κράτη μέλη λαμβάνουν όλα τα απαιτούμενα μέτρα ώστε να εξασφαλίζουν τη μέγιστη δυνατή διαθεσιμότητα διαθέσιμων στο κοινό τηλεφωνικών υπηρεσιών που παρέχονται μέσω των δημόσιων δικτύων επικοινωνιών σε περίπτωση καταστροφικής βλάβης του δικτύου ή σε περιπτώσεις ανωτέρας βίας. Τα κράτη μέλη εξασφαλίζουν ότι οι επιχειρήσεις που παρέχουν διαθέσιμες στο κοινό τηλεφωνικές υπηρεσίες λαμβάνουν όλα τα αναγκαία μέτρα ώστε να εξασφαλίζουν αδιάλειπτη πρόσβαση σε υπηρεσίες έκτακτης ανάγκης…»

Η ενσωμάτωση της οδηγίας στο ελληνικό δίκαιο έγινε με τον νόμο 3431/2006 [20] και η ενσωμάτωση της τροποποίηση 2009/136/ΕΚ με το νόμο 4070/2012 [21], όπου:

«...Άρθρο 37
Ασφάλεια και ακεραιότητα δικτύων και υπηρεσιών
1. Οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό λαμβάνουν πρόσφορα τεχνικά και οργανωτικά μέτρα για την κατάλληλη διαχείριση του κινδύνου όσον αφορά στην ασφάλεια των δικτύων και υπηρεσιών. Τα μέτρα αυτά, λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες, πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τον υφιστάμενο κίνδυνο. Οι επιχειρήσεις αυτές λαμβάνουν ιδίως μέτρα για την αποτροπή και ελαχιστοποίηση των επιπτώσεων από περιστατικά ασφαλείας που επηρεάζουν τους χρήστες και τα διασυνδεμένα δίκτυα.

2. Οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών λαμβάνουν όλα τα κατάλληλα μέτρα για την εξασφάλιση της ακεραιότητας των δικτύων τους έτσι ώστε να διασφαλίζεται η συνέχεια της παροχής των υπηρεσιών που διανέμονται μέσω των δικτύων αυτών.

3. Τα μέτρα των παραγράφων 1 και 2 καθορίζονται από την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) με κανονιστικές πράξεις[...]

Άρθρο 67

Ποιότητα και διαθεσιμότητα παρεχόμενων υπηρεσιών

[...]

3. Προκειμένου οι επιχειρήσεις που παρέχουν διαθέσιμες στο κοινό τηλεφωνικές υπηρεσίες μέσω δημόσιων δικτύων επικοινωνιών να εξασφαλίζουν τη μέγιστη δυνατή διαθεσιμότητα αυτών σε περιπτώσεις καταστροφικής βλάβης δικτύου ή σε περίπτωση ανωτέρας βίας, υποχρεούνται να λαμβάνουν όλα τα απαιτούμενα μέτρα. Οι ανωτέρω επιχειρήσεις υποχρεούνται να λαμβάνουν όλα τα απαραίτητα μέτρα για να διασφαλίζουν αδιάλειπτη πρόσβαση σε υπηρεσίες έκτακτης ανάγκης. Προς υλοποίηση των ανωτέρω, η Ε.Ε.Τ.Τ. έχει τη δυνατότητα να ζητά από τις επιχειρήσεις την παροχή σχετικών πληροφοριών και δύναται κατόπιν δημόσιας διαβούλευσης να εισηγηθεί την υιοθέτηση κατάλληλων και αναγκαίων μέτρων. Με κοινή απόφαση των Υπουργών Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων, κατόπιν εισήγησης της Ε.Ε.Τ.Τ., καθορίζονται οι ελάχιστες υποχρεώσεις, προς τις οποίες οφείλουν να συμμορφώνονται οι επιχειρήσεις. Αρμόδιος φορέας για τον έλεγχο των επιχειρήσεων σχετικά με την τήρηση των ανωτέρω ελάχιστων υποχρεώσεων είναι η Ε.Ε.Τ.Τ...»

- **Οδηγία 2002/58/ΕC - *"σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών" (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)*** [22]

Η οδηγία αυτή αντικατέστησε την οδηγία 97/66/ΕΚ και οι διατάξεις της εξειδικεύουν και συμπληρώνουν την οδηγία 95/46/ΕΚ, για την προστασία των προσωπικών δεδομένων, απευθυνόμενη κυρίως σε παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών και διαχείρισης

δημοσίων δικτύων επικοινωνιών που δραστηριοποιούνται στα κράτη-μέλη της Ευρωπαϊκής Κοινότητας. Αναφέρεται ότι:

«…Άρθρο 4

Ασφάλεια

1. Ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να λαμβάνει, εν ανάγκη από κοινού με τον φορέα παροχής του δημοσίου δικτύου επικοινωνιών καθόσον αφορά την ασφάλεια του δικτύου, τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του. Λαμβανομένων υπόψη των πλέον πρόσφατων τεχνικών δυνατοτήτων και του κόστους εφαρμογής τους, τα μέτρα αυτά πρέπει να κατοχυρώνουν επίπεδο ασφαλείας ανάλογο προς τον υπάρχοντα κίνδυνο.

2. Σε περίπτωση που υπάρχει ιδιαίτερος κίνδυνος παραβίασης της ασφάλειας του δικτύου, ο φορέας που παρέχει διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών οφείλει να ενημερώνει τους συνδρομητές για τον κίνδυνο αυτό και, εφόσον ο κίνδυνος κείται εκτός του πεδίου των μέτρων που οφείλει να λαμβάνει ο πάροχος της υπηρεσίας, για όλες τις τυχόν δυνατότητες αποτροπής του, καθώς και για το αναμενόμενο κόστος τους…»

Η οδηγία τροποποιήθηκε και συμπληρώθηκε περαιτέρω με την 2009/136/ΕΚ ως εξής:

«…4) Το άρθρο 4 τροποποιείται ως εξής:

α) ο τίτλος αντικαθίσταται από τον ακόλουθο:

"Ασφάλεια της επεξεργασίας"·

β) παρεμβάλλεται η ακόλουθη παράγραφος:

"1α. Με την επιφύλαξη των διατάξεων της οδηγίας 95/46/ΕΚ, τα μέτρα της παραγράφου 1 τουλάχιστον:

- εξασφαλίζουν ότι πρόσβαση σε προσωπικά δεδομένα μπορεί να έχει μόνον εξουσιοδοτημένο προσωπικό για αυστηρά νομίμως εγκεκριμένους σκοπούς,

- προστατεύουν τα αποθηκευμένα ή διαβιβασθέντα δεδομένα προσωπικού χαρακτήρα από τυχαία ή παράνομη καταστροφή, τυχαία απώλεια ή αλλοίωση, και από μη εγκεκριμένη ή παράνομη αποθήκευση, επεξεργασία, πρόσβαση ή αποκάλυψη και

- διασφαλίζουν την εφαρμογή πολιτικής ασφάλειας σε σχέση με την επεξεργασία προσωπικών δεδομένων.

Οι αρμόδιες εθνικές αρχές πρέπει να είναι σε θέση να ελέγχουν τα μέτρα που λαμβάνονται από παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών και να εκδίδουν συστάσεις σχετικά με βέλτιστες πρακτικές όσον αφορά το επίπεδο ασφάλειας το οποίο πρέπει να επιτυγχάνεται με αυτά τα μέτρα."…»

Η οδηγία ενσωματώθηκε στο ελληνικό δίκαιο με τον νόμο 3471/2006 [23] και η ενσωμάτωση της τροποποίησης 2009/136/ΕΚ έγινε με το νόμο 4070/2012 [21]. Τα παραπάνω αποσπάσματα που αναφέρονται στην αντιμετώπιση καταστροφών έχουν μεταφερθεί αυτούσια στους ελληνικούς νόμους.

- **Οδηγία 2006/24/ΕΚ - *"για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ"*** [24]

Η οδηγία αυτή αφορά ρυθμίσεις για τη διατήρηση δεδομένων με σκοπό τη διερεύνηση και δίωξη σοβαρών αδικημάτων και αφορά παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών και διαχείρισης δημοσίων δικτύων επικοινωνιών που δραστηριοποιούνται στα κράτη-μέλη της Ευρωπαϊκής Κοινότητας. Αναφέρεται ότι:

«…Άρθρο 7

Προστασία και ασφάλεια των δεδομένων.

Με την επιφύλαξη των διατάξεων που θεσπίστηκαν δυνάμει της οδηγίας 95/46/ΕΚ και της οδηγίας 2002/58/ΕΚ, κάθε κράτος μέλος εξασφαλίζει ότι στα δεδομένα που διατηρούνται σύμφωνα με την παρούσα οδηγία εφαρμόζονται τουλάχιστον οι εξής αρχές ασφαλείας από

τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών διαθέσιμων στο κοινό ή δημοσίου δικτύου επικοινωνιών:

α) τα διατηρούμενα δεδομένα είναι ίδιας ποιότητας και τυγχάνουν της αυτής προστασίας και ασφάλειας με τα δεδομένα που περιέχει το δίκτυο

β) λαμβάνονται τα δέοντα τεχνικά και οργανωτικά μέτρα προστασίας των δεδομένων κατά τυχαίας ή παράνομης καταστροφής τους ή τυχαίας απώλειας, αλλοίωσης, μη εξουσιοδοτημένης ή παράνομης αποθήκευσης, επεξεργασίας, πρόσβασης ή αποκάλυψης·

γ) λαμβάνονται τα δέοντα τεχνικά και οργανωτικά μέτρα για να διασφαλισθεί ότι στα δεδομένα έχει πρόσβαση μόνο ειδικά εξουσιοδοτημένο προσωπικό και

δ) τα δεδομένα καταστρέφονται στο τέλος του χρονικού διαστήματος διατήρησης, εκτός από εκείνα στα οποία έχει αποκτηθεί πρόσβαση και τα οποία έχουν φυλαχθεί.

Άρθρο 8

Απαιτήσεις αποθήκευσης για τα διατηρούμενα δεδομένα

Τα κράτη μέλη διασφαλίζουν ότι τα δεδομένα που ορίζει το άρθρο 5 διατηρούνται σύμφωνα με την παρούσα οδηγία με τέτοιο τρόπο ώστε τα διατηρούμενα δεδομένα και κάθε άλλη πληροφορία σχετικά με αυτά να μπορούν να διαβιβαστούν κατόπιν αιτήματος στις αρμόδιες αρχές χωρίς αδικαιολόγητη καθυστέρηση…»

Η ενσωμάτωση στο ελληνικό δίκαιο έγινε με το νόμο 3917/2011 [25] ο οποίος προβλέπει αυστηρότατες κυρώσεις, διοικητικές και ποινικές, καθώς και αστική ευθύνη για τη μη τήρησή του. Ο νόμος αυτός επεκτείνει τις ρυθμίσεις της οδηγίας υποχρεώνοντας για την κατάρτιση ειδικού σχεδίου για την προστασία των δεδομένων από καταστροφές:

«...Άρθρο 7

Υποχρεώσεις παρόχων ως προς την προστασία και ασφάλεια των δεδομένων

(Άρθρο 7 στοιχεία α΄ έως γ΄ της Οδηγίας 2006/24/ΕΚ)

[...]

2. Οι πάροχοι διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιου δικτύου επικοινωνιών υποχρεούνται να καταρτίζουν και να εφαρμόζουν ειδικό σχέδιο πολιτικής ασφάλειας ως προς τα μέσα, τις μεθόδους και τα μέτρα που διασφαλίζουν την τήρηση των αρχών της παραγράφου 1. Η εφαρμογή του σχεδίου αυτού ανατίθεται από τον πάροχο σε εξουσιοδοτημένο στέλεχος, το οποίο ορίζεται ως υπεύθυνος ασφάλειας δεδομένων. Με κοινή πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.), η οποία εκδίδεται μέσα σε τρεις μήνες από την έναρξη ισχύος του παρόντος νόμου, καθορίζεται κάθε θέμα σχετικό με τη διαδικασία και τον τρόπο εφαρμογής των διατάξεων του παρόντος άρθρου...»

- **Οδηγία 2008/114/ΕΚ - *"σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους"*** [26]

Η οδηγία αυτή αφορά στον προσδιορισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας (ΕΥΖΣ) αλλά και την υποχρέωση κατάρτισης Σχεδίων Ασφαλείας της Λειτουργίας τους (ΣΑΛ) από τα κράτη μέλη. Χαρακτηριστικά αναφέρεται ότι:

«…

Άρθρο 5

Σχέδια ασφαλείας λειτουργίας

1. Η διαδικασία των σχεδίων ασφαλείας λειτουργίας (ΣΑΛ) προσδιορίζει τα περιουσιακά στοιχεία των ΕΥΖΣ και τις λύσεις ασφαλείας οι οποίες υπάρχουν ή εφαρμόζονται για την προστασία τους. Στο παράρτημα ΙΙ εκτίθεται το ελάχιστο περιεχόμενο που καλύπτει η διαδικασία ΣΑΛ για μια ΕΥΖΣ.

2. Κάθε κράτος μέλος οφείλει να αξιολογεί εάν οι χαρακτηριζόμενες ως ΕΥΖΣ που βρίσκονται στο έδαφός του διαθέτουν ΣΑΛ ή εφαρμόζουν ισοδύναμα μέτρα για την αντιμετώπιση των ζητημάτων που προσδιορίζονται στο παράρτημα ΙΙ. Αν ένα κράτος μέλος διαπιστώσει ότι

υφίσταται ΣΑΛ ή ισοδύναμο σχέδιο και ότι τούτο επικαιροποιείται τακτικά, δεν απαιτούνται περαιτέρω ενέργειες.

3. Εάν ένα κράτος μέλος διαπιστώσει ότι δεν έχει εκπονηθεί ΣΑΛ ή ισοδύναμό του, διασφαλίζει, με όποια μέτρα κρίνονται αναγκαία, την εκπόνηση ΣΑΛ ή ισοδυνάμου που να καλύπτει τα ζητήματα του παραρτήματος ΙΙ.

Κάθε κράτος μέλος διασφαλίζει ότι τα ΣΑΛ ή τα ισοδύναμά τους έχουν τεθεί σε εφαρμογή και αναθεωρούνται τακτικά εντός ενός έτους από τον χαρακτηρισμό υποδομής ζωτικής σημασίας ως ΕΥΖΣ. Η περίοδος αυτή μπορεί να παραταθεί υπό εξαιρετικές συνθήκες, κατόπιν συμφωνίας με την αρχή του κράτους μέλους και με κοινοποίηση στην Επιτροπή.

4. Σε περίπτωση που υφίστανται ήδη ρυθμίσεις περί εποπτείας ή ελέγχου σε σχέση με ΕΥΖΣ, οι εν λόγω ρυθμίσεις δεν επηρεάζονται από το παρόν άρθρο και η αρμόδια αρχή του κράτους μέλους που αναφέρεται στο παρόν άρθρο ασκεί την εποπτεία δυνάμει αυτών των υφισταμένων ρυθμίσεων.

5. Η συμμόρφωση με τα μέτρα, συμπεριλαμβανομένων των κοινοτικών μέτρων για τα οποία απαιτείται, σε συγκεκριμένο τομέα, να υπάρχει σχέδιο παρόμοιο ή ισοδύναμο με ΣΑΛ καθώς και ο έλεγχος ενός τέτοιου σχεδίου από την αρμόδια αρχή, θεωρείται ότι ικανοποιεί όλες τις απαιτήσεις που βαρύνουν τα κράτη μέλη και οι οποίες απορρέουν από το παρόν άρθρο ή υιοθετούνται δυνάμει αυτού. Στις κατευθυντήριες γραμμές εφαρμογής, περί των οποίων το άρθρο 3 παράγραφος 2, περιέχεται ενδεικτικός κατάλογος των μέτρων αυτών.

[…]

ΠΑΡΑΡΤΗΜΑ ΙΙ

ΔΙΑΔΙΚΑΣΙΑ ΣΑΛ

Το ΣΑΛ προσδιορίζει τα περιουσιακά στοιχεία των υποδομών ζωτικής σημασίας και τις λύσεις ασφαλείας οι οποίες υπάρχουν ή εφαρμόζονται για την προστασία τους. Η διαδικασία ΣΑΛ για ΕΥΖΣ καλύπτει τουλάχιστον:

1. τον προσδιορισμό των σημαντικών περιουσιακών στοιχείων

2. τη διεξαγωγή ανάλυσης κινδύνων βασιζόμενης στα κυριότερα σενάρια απειλών, στα τρωτά σημεία κάθε περιουσιακού στοιχείου, καθώς και στις δυνητικές επιπτώσεις· και

3. προσδιορισμό, επιλογή και αναγνώριση προτεραιότητας στα αντίμετρα και διαδικασίες, με την εξής διάκριση:

— διαρκή μέτρα ασφαλείας, όπου προσδιορίζονται οι αναγκαίες επενδύσεις και μέσα ασφαλείας τα οποία είναι κατάλληλα προς χρησιμοποίηση οποιαδήποτε χρονική στιγμή. Η κατηγορία αυτή περιλαμβάνει στοιχεία σχετικά με τα γενικά μέτρα ασφαλείας, όπως τεχνικά μέτρα (συμπεριλαμβανόμενων της εγκατάστασης ανιχνευτών, του ελέγχου πρόσβασης, των μέσων προστασίας και πρόληψης), οργανωτικά μέτρα (συμπεριλαμβανόμενων των διαδικασιών συναγερμού και διαχείρισης κρίσεων), μέτρα ελέγχου και επαλήθευσης, επικοινωνία, ευαισθητοποίηση και κατάρτιση, και συστήματα ασφαλείας των πληροφοριών,

— βαθμιαία μέτρα ασφαλείας τα οποία μπορούν να ενεργοποιούνται ανάλογα με το επίπεδο κινδύνου και απειλής…»

Η ενσωμάτωση στο ελληνικό δίκαιο έγινε αυτούσια με το Π.Δ. 39/2011(ΦΕΚ 104/Α/06-05-2011) [27], σύμφωνα με το οποίο την ευθύνη εφαρμογής του αναλαμβάνει το Κέντρο Μελετών Ασφάλειας (ΚΕ.ΜΕ.Α.) [28].

3.3.2 Απαιτήσεις

- **Council of Europe (CoE) - *"Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data"*** [29]

Το 1981 τα μέλη του Συμβουλίου της Ευρώπης εξέδωσαν μια σύμβαση, σχετικά με την προστασία των προσωπικών δεδομένων, δεσμευόμενοι, μεταξύ άλλων, και για τη λήψη κατάλληλων μέτρων προστασίας από καταστροφές:

«…Article 7 – Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination…»

- **Safe Harbor Framework - *"Safe Harbor Privacy Principles"*** [30]

Η Ευρωπαϊκή Κοινότητα, όπως παρουσιάστηκε παραπάνω από τις οδηγίες που έχει εκδώσει κατά καιρούς, δίδει ιδιαίτερη σημασία στα προσωπικά δεδομένα και στην ιδιωτικότητα του ατόμου και έχει αναπτύξει για το σκοπό αυτό ένα αρκετά αυστηρό πλαίσιο προστασίας. Σύμφωνα με αυτό το πλαίσιο απαγορεύεται στα μέλη της ΕΕ να διαβιβάσουν προσωπικά δεδομένα σε μη μέλη της Ένωσης, εκτός και εάν υπάρχουν εγγυήσεις ότι θα τύχουν αντίστοιχου επιπέδου προστασίας. Το γεγονός αυτό δημιούργησε αρκετά προβλήματα στις εμπορικές συναλλαγές μεταξύ οργανισμών της Ευρώπης και των Η.Π.Α. οι οποίες απαιτούν την ανταλλαγή τέτοιων δεδομένων, καθώς δεν υπήρχε πλαίσιο, αντίστοιχου επιπέδου προστασίας, στην αμερικανική νομοθεσία. Ως λύση προτάθηκε το 2000 το πλαίσιο πιστοποίησης «Safe Harbor», το οποίο επιχειρεί να ευθυγραμμίσει το επίπεδο προστασίας των οργανισμών των Η.Π.Α. με όσα προβλέπονται από τις ευρωπαϊκές οδηγίες για την προστασία προσωπικών δεδομένων, ώστε να καταστεί εφικτή η ανταλλαγή των σχετικών δεδομένων. Το πλαίσιο αυτό απαρτίζεται από την υποχρέωση τήρησης 7 βασικών αρχών ανάμεσα στις οποίες περιλαμβάνεται και η υποχρέωση λήψης μέτρων για την προστασία των δεδομένων από καταστροφή:

«…SAFE HARBOR PRIVACY PRINCIPLES […]

SECURITY: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction...»

3.3.3 Συστάσεις

- **OECD Guidelines (ΟΟΣΑ) - *"Recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data"*** [31]

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (Ο.Ο.Σ.Α.) εξέδωσε το 1980 συστάσεις σχετικά με την προστασία προσωπικών δεδομένων ώστε να εναρμονίσει τις ακολουθούμενες πρακτικές μεταξύ των οργανισμών των κρατών-μελών. Σύμφωνα με αυτές προτείνεται και η λήψη μέτρων προστασίας από καταστροφές:

> *«…Security Safeguards Principle*
>
> *11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data […]*
>
> *16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure…»*

- **UN Guidelines - *"for the Regulation of Computerized Personal Data Files"***[32]

Η Γενική Συνέλευση του Οργανισμού Ηνωμένων Εθνών (Ο.Η.Ε.) εξέδωσε το 1990 ένα σύνολο 10 αρχών που συστήνει να ακολουθούνται, σχετικά με την προστασία προσωπικών δεδομένων. Ανάμεσα σε αυτές τις αρχές διακρίνεται και η αναγκαιότητα λήψης προστατευτικών μέτρων έναντι καταστροφών:

> *«…7. Principle of security*
>
> *Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses...»*

➢ **OECD Guidelines (ΟΟΣΑ) - *"for the Security of Information Systems and Networks: Towards a Culture of Security"*** [33]

Ο ΟΟΣΑ επιδιώκοντας να προωθήσει τη δημιουργία κουλτούρας υιοθέτησης πρακτικών ασφάλειας για τα Πληροφοριακά Συστήματα και τα δίκτυα εξέδωσε το 2002 ένα σύνολο 9 αρχών, τις οποίες προτείνει στα μέλη του. Ανάμεσα σε αυτές παρατηρεί κανείς και την ιδιαίτερη ανάγκη για απόκριση σε περιστατικά ασφαλείας, όπως είναι και τα περιστατικά καταστροφής. Χαρακτηριστικά αναφέρεται:

«...3) Response

Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents. Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation[...]

8) Security management

Participants should adopt a comprehensive approach to security management. Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements...»

3.4 Οικονομικά θέματα

3.4.1 Γενικά

Η απόφαση ενός οργανισμού να υιοθετήσει κάποιο σχέδιο ανάκαμψης από καταστροφές αν και συνήθως έχει κύριο στόχο τον περιορισμό των οικονομικών επιπτώσεων μπορεί πολλές φορές να επιβάλλεται και για λόγους νομικούς ή κανονιστικούς, ιδίως όσον αφορά οργανισμούς κοινής ωφέλειας που επεξεργάζονται ευαίσθητα δεδομένα, όπως παρουσιάστηκε και στο προηγούμενο κεφάλαιο. Σε κάθε περίπτωση όμως ο οικονομικός παράγοντας είναι αυτός που διαδραματίζει τον καθοριστικότερο ρόλο στην επιλογή του μοντέλου ανάκαμψης και των μέτρων που αυτό περικλείει. Κατά την επιλογή αυτή προκύπτουν βασικά ερωτήματα τα οποία πρέπει να απαντηθούν σχετικά με το πραγματικό κόστος των διαθέσιμων μέτρων ανάκαμψης αλλά και το κατά πόσο αυτό το κόστος αξίζει να επενδυθεί.

Εξετάζοντας λοιπόν το ζήτημα του ΣΑΚ με οικονομικούς όρους η σύγκριση με χρήση μετρήσιμων, ποσοτικών, κριτηρίων αποτελεί μονόδρομο καθιστώντας τη χρήση βοηθητικών οικονομικών δεικτών υποχρεωτική.

Οι πιο χαρακτηριστικοί δείκτες που χρησιμοποιούνται για την οικονομική αξιολόγηση και επιλογή Πληροφοριακών Συστημάτων είναι ο TCO (Total Cost of Ownership) και ο ROI (Return On Investment). Ειδικότερα, όσον αφορά στην αξιολόγηση της επένδυσης σε μέτρα ασφάλειας, ο δείκτης ROI παραλλάσσεται και μετατρέπεται στο δείκτη ROSI (Return On Security Investment). Προσπαθώντας να εξειδικεύσουμε ακόμα περισσότερο τον δείκτη ROSI, για την περίπτωση αξιολόγησης μέτρων ανάκαμψης, θα μελετήσουμε πως μπορεί να μετατραπεί σε ένα νέο δείκτη, τον οποίο, χάριν συνέπειας, θα αποκαλέσουμε RORI (Return On Recovery Investment).

Θα πρέπει να τονιστεί ότι οι δείκτες αυτοί αφορούν σε αμιγώς οικονομικά κριτήρια, τα οποία δε θα πρέπει να μονοπολούν κατά την αξιολόγηση ενός ΠΣ, καθώς μπορεί να οδηγήσουν σε εσφαλμένες εκτιμήσεις [34]. Άλλα κριτήρια όπως η επάρκεια, ή η αποτελεσματικότητα ενός ΠΣ ή ενός μέτρου συνήθως έχουν μεγαλύτερη βαρύτητα κατά την επιλογή του καταλληλότερου για κάθε περίπτωση.

3.4.2 TCO (Total Cost of Ownership)

Το 1987 το Gartner Group παρουσίασε μια μελέτη [35] σύμφωνα με την οποία οι περισσότεροι οργανισμοί κατά την προμήθεια κάποιου ΠΣ λαμβάνουν υπόψη τους μόνο το κόστος αγοράς, παρόλο που στην πραγματικότητα αυτό αποτελεί μόνο το 20% του συνολικού κόστους κτήσης και χρήσης του. Προτάθηκε λοιπόν η χρήση του μοντέλου "Total Cost of Owneship" (TCO) σύμφωνα με το οποίο υπολογίζεται το συνολικό κόστος καθ' όλη τη διάρκεια ζωής του ΠΣ. Έτσι υπολογίζεται το ολικό κόστος κτήσης το οποίο εμπεριέχει άμεσα και έμμεσα κόστη που μπορεί να αφορούν από την κτήση και λειτουργία του ΠΣ μέχρι και την απόσυρση του. Το TCO ενός προϊόντος-συστήματος μπορεί να αποτελείται από:

Κεφαλαιακές δαπάνες (Capital Expenses-CAPEX), όπως:

- αρχικό κόστος κτήσης-αγοράς
- κόστος εγκατάστασης
- κόστος εκπαίδευσης

Λειτουργικές δαπάνες (Operational Expenses-OPEX), όπως:

- κόστος συντήρησης
- κόστος λειτουργίας

Γενικά μπορούμε να πούμε ότι ισχύει:

$$\mathrm{TCO} = \mathrm{CAPEX} + \mathrm{OPEX}$$

Συμπεραίνουμε λοιπόν ότι το TCO αποτελεί ένα αποτελεσματικό και αξιόπιστο οικονομικό μέτρο σύγκρισης όταν καλούμαστε να επιλέξουμε μεταξύ διαφορετικών λύσεων.

3.4.3 ROI (Return On Investment)

Παρόλο που το TCO μπορεί να μας αποκαλύψει το πραγματικό κόστος των προσφερομένων λύσεων, δεν μπορεί να δώσει απάντηση στο κατά πόσο μια επένδυση, στην επιλεχθείσα λύση, είναι συμφέρουσα για τον οργανισμό. Για να απαντηθεί το ερώτημα αυτό θα πρέπει μαζί με το κόστος της επένδυσης να συνυπολογιστεί και το όφελος που θα προκύψει. Για το λόγο αυτό χρησιμοποιείται ο δείκτης "Return On Investment)" (ROI) ο οποίος δηλώνει το κέρδος από μια επένδυση σε σχέση με το κόστος της κατά τη διάρκεια κάποιου ορισμένου

χρόνου, αυτό το κόστος μπορεί να υπολογίζεται κατ' έτος ή για όλη τη διάρκεια ζωής του ΠΣ. Αυτός ο δείκτης μπορεί να εκφραστεί ως [36]:

$$\mathrm{ROI} = \frac{\sum \text{Expected Returns} - \sum \text{Cost of Investment}}{\sum \text{Cost of Investment}}$$

Παρατηρούμε ότι ο ROI εμπεριέχει την έννοια του TCO και μπορούμε να πούμε ότι ισχύει:

$$\mathrm{ROI} = \frac{\sum \text{Expected Returns} - \mathrm{TCO}}{\mathrm{TCO}}$$

Ο ROI, σε αντίθεση με το TCO, δεν αξιολογεί μόνο το μέγεθος-κόστος της επένδυσης αλλά και την κερδοφορία της, καθώς εισάγει και την έννοια του κέρδους που προκύπτει από μια επένδυση σε κάποιο ΠΣ.

3.4.4 ROSI (Return On Security Investement)

Όταν η επένδυση αφορά σε μέτρα ασφάλειας η έννοια του κέρδους, που μπορεί να προκύψει από τη λήψη τους, μπορεί να μην είναι τόσο ξεκάθαρη ιδίως όταν απευθύνεται σε πρόσωπα μη εξοικειωμένα με την έννοια της ασφάλειας πληροφοριών, όπως είναι τα αμιγώς διοικητικά και οικονομικά στελέχη ενός οργανισμού.

Σύμφωνα και με τον Shneier η ασφάλεια δεν πρέπει να αντιμετωπίζεται ως μια επένδυση που αποδίδει ανταποδοτικό κέρδος όπως μια κερδοφόρα επιχειρησιακή λειτουργία. Είναι ένα έξοδο το οποίο ελπίζουμε να ανταποδώσει με τη μείωση του κόστους μίας ενδεχόμενης απώλειας [37].

Επομένως κατά τον υπολογισμό του ROI, όταν αυτό αφορά επενδύσεις σε ασφάλεια πληροφοριών, θα πρέπει το υπολογιζόμενο όφελος (Expected Returns) να εμπεριέχει πέρα από το αναμενόμενο κέρδος (Expected Profit) και την αποφυγή κόστους (Cost Mitigation) από πιθανή καταστροφή. Σημειώνεται δε, ότι το αναμενόμενο κέρδος συνήθως είναι μηδενικό, αφού τα μέτρα ασφάλειας κατά κανόνα δεν βελτιώνουν την παραγωγικότητα του οργανισμού αλλά αντίθετα την επιβαρύνουν. Όπου:

$$\sum \text{Expected Returns} = \cancel{\sum \text{Expected Profit}}^{0} + \sum \text{Cost Mitigation}$$
$$= \sum \text{Cost Mitigation}$$

Για τον ποσοτικό υπολογισμό λοιπόν του ROI, σε επενδύσεις ασφάλειας, προτάθηκε ο υπολογισμός του αποφευχθέντος πιθανού κόστους καταστροφής (Cost Mitigation) ως ανάλογο της ποσοτικοποιημένης έκθεσης σε κίνδυνο (Risk Exposure) και του ποσοστού αποφυγής (Risk Mitigated) που επιφέρει το προς εξέταση μέτρο [38].

Το ROI προσαρμόζεται και μετατρέπεται-εξειδικεύεται με τον τρόπο αυτό σε "Return On Security Investment" (ROSI) το οποίο εκφράζεται ως:

$$\text{ROSI} = \frac{(\text{Risk Exposure} \cdot \%\text{Risk Mitigated}) - \text{TCO}}{\text{TCO}}$$

Για την ποσοτικοποίηση της έκθεσης σε κίνδυνο προτάθηκε η χρήση του "Annual Loss Exposure"(ALE) ως ετήσια έκθεση σε απώλεια από περιστατικά ασφαλείας:

$$\text{Risk Exposure} = \text{ALE} = \text{SLE} \cdot \text{ARO}$$

Όπου:

SLE: κόστος περιστατικού ασφαλείας (Single Loss Exposure)

ARO: ετήσια συχνότητα εμφάνισης (Annual Rate of Occurence)

Στην μελέτη αυτή [38] αναφέρεται το παράδειγμα ενός οργανισμού που θέλει να επενδύσει σε κάποια αντιϊκή λύση και έχει εκτιμήσει ότι το μέσο κόστος (ζημίες και παραγωγικότητα) από ένα περιστατικό προσβολής από ιό είναι 25.000$, η μέση ετήσια συχνότητα εμφάνισης είναι 4 ιοί κατ' έτος και η λύση που εξετάζει υπόσχεται την αποφυγή τουλάχιστον 3 εξ αυτών με συνολικό κόστος (CAPEX+OPEX) στα 25.000$. επομένως:

SLE=25.000

ARO=4

Risk Mitigated=75%

TCO=25.000

Προκύπτει ότι:

$$\text{ROSI} = \frac{(100000 * 75\%) - 25000}{25000} = 200\%$$

Σε πρώτη ανάγνωση μοιάζει να είναι μια σωστή επένδυση αλλά η πραγματικότητα μπορεί να διαφέρει σημαντικά. Όπως χαρακτηριστικά αναφέρεται, σε περίπτωση που η καταστροφή για κάθε έναν από τους ιούς εκτιμάται σε 5.000$ για τους μεν 3, και σε 85.000$ για τον 4 τότε, ανάλογα με τον ιό που θα διαφύγει από το αντιϊικό, το πραγματικό ROSI μπορεί να κυμανθεί από -40% έως 280%. Γίνεται φανερό ότι δε μπορεί να διασφαλιστεί η εγκυρότητα του ROSI, ως μετρική απόλυτων τιμών, παρά μόνο να χρησιμοποιηθεί ως ένα εργαλείο σύγκρισης με σχετικές τιμές. Προτείνεται λοιπόν όταν χρησιμοποιείται ως δείκτης, να συνοδεύεται τόσο από τις παραδοχές που έγιναν κατά τον υπολογισμό του, αλλά και με εκτίμηση του ποσοστού σφάλματος της τελικής του τιμής ώστε να ο αναγνώστης να έχει μια πιο ρεαλιστική εικόνα [34].

3.4.5 RORI (Return On Recovery Investment)

Γενικά μπορούμε να δεχτούμε ότι τα μέτρα ασφάλειας κατατάσσονται σε δυο κατηγορίες: σε αυτά που δρουν προληπτικά και μειώνουν τις ευπάθειες και σε αυτά που δρουν διορθωτικά και μειώνουν τις επιπτώσεις. Ανάλογα με την κατηγορία στην οποία ανήκει κάθε μέτρο διαφέρει και ο υπολογισμός του κέρδους που προκύπτει, υπό τη μορφή μείωσης του κόστους των συνεπειών, ενός ενδεχόμενου περιστατικού.

Στην περίπτωση των προληπτικών μέτρων η χρήση του δείκτη ROSI μπορεί να καλύψει αυτόν τον υπολογισμό ως αποτέλεσμα 4 ποσοτικοποιημένων παραμέτρων, όπως παρουσιάστηκε και παραπάνω [39], ήτοι:

-της συχνότητας-πιθανότητας εμφάνισης ενός περιστατικού (ARO)

-της επίπτωσης που έχει στην αξία των αγαθών (SLE)

-της αποτελεσματικότητας των μέτρων ασφάλειας στον περιορισμό του κινδύνου (%Risk Mitigated)

-του κόστους των μέτρων ασφάλειας (TCO)

όπου:

$$\text{ROSI} = \frac{(\text{SLE} * \text{ARO} * \%\text{Risk Mitigated}) - \text{TCO}}{\text{TCO}}$$

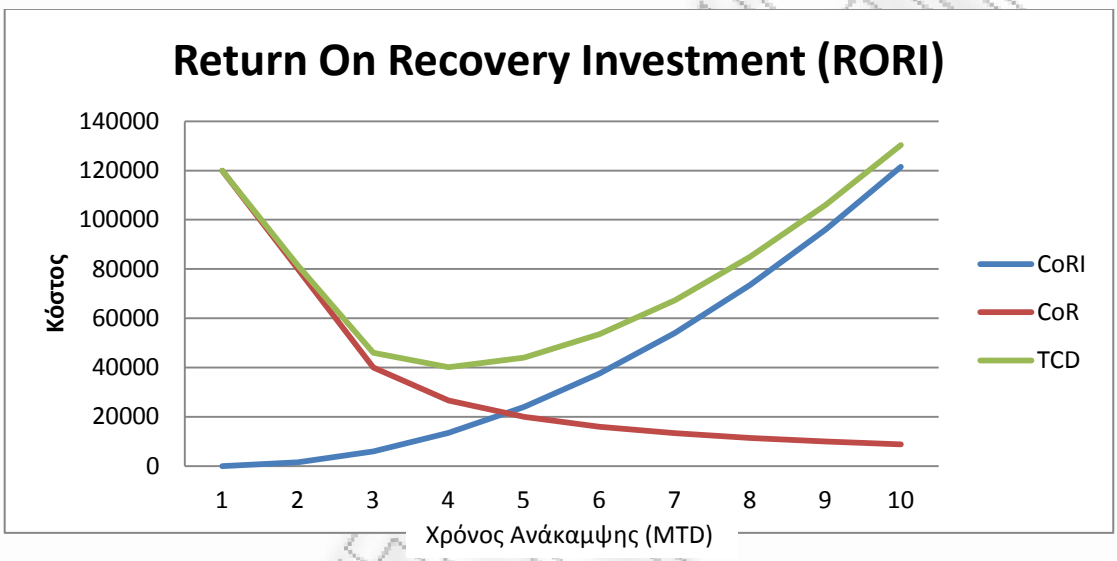
Στην περίπτωση όμως των διορθωτικών μέτρων, στα οποία ανήκουν και τα μέτρα ανάκαμψης από μια ενδεχόμενη καταστροφή που πραγματεύεται ένα ΣΑΚ, οι παραπάνω παράμετροι κρίνονται ανεπαρκής. Η επένδυση σε διορθωτικά μέτρα όπως είδαμε, ως ειδικά μέτρα ασφάλειας, δε θα πρέπει να αντιμετωπίζεται και να αξιολογείται με όρους ανταποδοτικών εσόδων αλλά ως μέσο αποφυγής εξόδων. Η διαφοροποίησή τους με τα προληπτικά έγκειται στο στόχο αυτών των μέτρων, ο οποίος δεν είναι ο περιορισμός του πιθανού κινδύνου αλλά ο περιορισμός των συνεπειών, θεωρώντας δεδομένη την εμφάνιση κάποιου καταστροφικού περιστατικού. Γίνεται αντιληπτό ότι η παράμετρος της πιθανότητας εμφάνισης του περιστατικού χάνει την αξία της (σταθερή τιμή ARO=1), ενώ η αποτελεσματικότητα των μέτρων (%Risk Mitigated) δεν μπορεί να ποσοστικοποιηθεί ως περιορισμός κινδύνου, όπως στην περίπτωση των προληπτικών μέτρων. Το ίδιο ισχύει και για την επίπτωση στα αγαθά (SLE) καθώς αυτή είναι δύσκολο να εκτιμηθεί ποσοτικά, αφού μια καταστροφή αν δεν αντιμετωπιστεί έγκαιρα μπορεί να οδηγήσει ακόμη και στην οριστική παύση του οργανισμού.

Ως εναλλακτική προσέγγιση στην **ποσοτικοποίηση της αποτελεσματικότητας των διορθωτικών μέτρων** προτείνεται η χρήση, ως μέτρου αναφοράς, του συνολικού κόστους καταστροφής μετά την εφαρμογή των μέτρων (Total Cost of Destruction-TCD), το οποίο αποτελεί άθροισμα του κόστους εφαρμογής των μέτρων (Cost of Recovery-CoR) και του εναπομείναντος κόστους από τη μη διαθεσιμότητα των ΠΣ μέχρι την ανάκαμψή τους από τα μέτρα αυτά (Cost of Remaining Impact-CoRI), συναρτήσει της χρονικής διάρκειας μέχρι την αναμενόμενη ανάκαμψη (Maximum Tolerable Downtime-MTD):

$$TCD_{MTD} = CoR + CoRI$$

Επομένως, για την περίπτωση των διορθωτικών μέτρων, μπορούμε να προτείνουμε το TCD ως δείκτη απόδοσης επένδυσης ο οποίος, χάριν συμφωνίας με τον ROSI, μπορεί να κληθεί ως “Return On Recovery Investment” (RORI), ο οποίος όσο μικρότερος είναι τόσο πιο αποδοτικά μπορούν να θεωρηθούν τα διορθωτικά μέτρα.

Σύμφωνα με τον NIST [7] μπορούμε να δεχτούμε ότι όσο περισσότερο διαρκεί η διακοπή μιας υπηρεσίας-λειτουργίας του οργανισμού τόσο μεγαλώνει το κόστος των επιπτώσεων της διακοπής για τον οργανισμό (CoRI). Σε αντίθεση όσο μικρότερος είναι ο χρόνος που απαιτείται για να ανακτηθεί η υπηρεσία-λειτουργία, τόσο αυξάνεται και το κόστος των απαιτούμενων μέτρων ανάκαμψης (CoR). Συνεπώς τα δύο αυτά μεγέθη μεταβάλλονται αντιστρόφως ανάλογα με την πάροδο του χρόνου ανάκαμψης. Αυτό εκφράζεται και διαγραμματικά στο Σχήμα 10.



Σχήμα 10: *Return On Recovery Investment (RORI)*

Βάσει του παραπάνω διαγράμματος επιχειρείται η ανάλυση περιπτώσεων, σε συμφωνία και με τη λογική ανάλυση η οποία συνήθως χρησιμοποιείται σε νομικές υποθέσεις, όπου διερευνάται ο διαχωρισμός μεταξύ αμέλειας και επάρκειας λήψης μέτρων για την αντιμετώπιση ενδεχόμενων κινδύνων. Χαρακτηριστικότερο παράδειγμα αποτελεί η υπόθεση "ΗΠΑ εναντίον Carroll Towing" [40] από την οποία προέκυψε και «ο τύπος του δικαστή Learned Hand» (ή τύπος BPL), ο οποίος επιχειρεί να διευθετήσει νομικά ζητήματα με οικονομικούς όρους. Σύμφωνα με αυτόν, όταν το κόστος των ληφθέντων μέτρων για την αντιμετώπιση ενδεχόμενων κινδύνων είναι μικρότερο του πιθανού κόστους των επιπτώσεων, μπορεί να θεωρηθεί ότι υπάρχει αμέλεια. Όταν δηλαδή B < PL, όπου:

B (burden): κόστος μέτρων προφυλάξεων

P (probability): πιθανότητα απώλειας

L (loss): μέγεθος απώλειας

Κατά αντιστοιχία μπορούμε να πούμε ότι σε περίπτωση καταστροφής των ΠΣ διακρίνονται οι εξής περιπτώσεις, όπου:

CoRI < CoR , το κόστος των μέτρων για την ανάκαμψη είναι μεγαλύτερο σε σχέση με το κόστος των επιπτώσεων μέχρι την ανάκαμψη. Επομένως τα μέτρα ανάκαμψης θεωρούνται ότι υπερκαλύπτουν την ενδεχόμενη καταστροφή και το κόστος τους κρίνεται οικονομικά ασύμφορο σε σχέση με το κόστος των επιπτώσεων, σε ενδεχόμενη καταστροφή.

CoRI > CoR , το κόστος των επιπτώσεων είναι μεγαλύτερο από το κόστος των μέτρων ανάκαμψης. Αυτό το κόστος, όταν η απόκλιση είναι μικρή, μπορεί να είναι αναμενόμενο και αποδεκτό για τον οργανισμό. Όταν όμως η απόκλιση είναι μεγάλη (B<PL) υπάρχει ο κίνδυνος να θεωρηθεί ότι, σε περίπτωση καταστροφής, τα μέτρα να μην επαρκούν για τη διασφάλιση του οργανισμού και για τον ικανοποιητικό περιορισμό των επιπτώσεων.

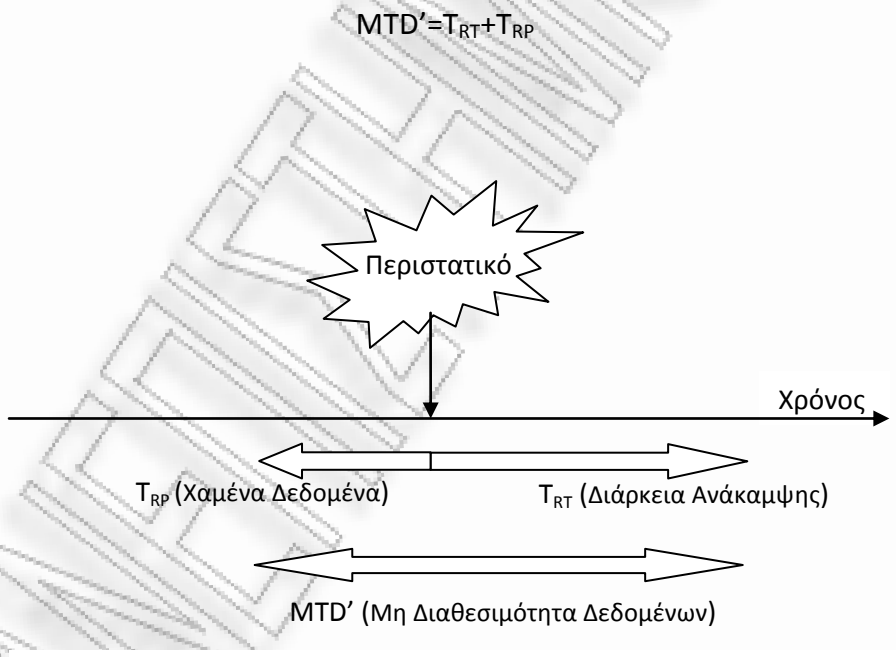
3.4.6 Εκτίμηση βέλτιστης επένδυσης σε μέτρα ανάκαμψης

Κάθε μέτρο ανάκαμψης διακρίνεται από δυο χαρακτηριστικά μεγέθη: το κόστος του και το χρόνο ανάκαμψης τον οποίον υπόσχεται (CoR, t_r).

Στο διάγραμμα (Σχήμα 10) παρατηρούμε ότι για να επιτευχθεί το βέλτιστο RORI, δηλαδή η μικρότερη δυνατή τιμή για το TCD_{MTD}, θα πρέπει κατά προσέγγιση να ισχύει CoR= CoRI, το οποίο φανερώνει το ιδανικό κόστος που θα πρέπει να έχουν τα μέτρα ανάκαμψης ώστε να επιτυγχάνουν το μέγιστο αποτέλεσμα για το ελάχιστο κόστος. Αυτό το σημείο αντιστοιχεί σε κάποια χρονική διάρκεια, στην οποία επέρχεται η ανάκαμψη των λειτουργιών του οργανισμού, η οποία θα πρέπει να είναι μικρότερη ή ίση με αυτή που μπορεί να επιβάλλεται εξαιτίας των απαιτήσεων ανοχής και από άλλες επιπτώσεις πέραν των οικονομικών (βλέπε MTD §4.2). Συνεπώς για να κριθεί αποδοτικό ένα μέτρο, ο χρόνος ανάκαμψης που προσφέρει δε θα πρέπει να ξεπερνά το μέγιστο αποδεκτό χρόνο (t_r<=MTD) ενώ το κόστος του δε θα πρέπει να υπερβαίνει το εναπομείναν κόστος από τη μη διαθεσιμότητα των ΠΣ μέχρι την ανάκαμψή τους από τα μέτρα αυτά (CoR<=CoRI).

Για να καταστεί εφικτή η κοστολόγηση για την αποδοτική επένδυση σε ένα μέτρο θα πρέπει, αφού εκτιμηθεί και αποφασιστεί ο μέγιστος αποδεκτός χρόνος μη διαθεσιμότητας (MTD), να υπολογιστεί το αντίστοιχο κόστος από τη μη διαθεσιμότητα των ΠΣ στη διάρκεια αυτή ($CoRI_{MTD}$).

Κατά τον υπολογισμό του κόστους μη διαθεσιμότητας ενός περιστατικού δε λαμβάνουμε τόσο υπόψη το κόστος του κατεστραμμένου εξοπλισμού, όσο την επίδραση που έχει η καταστροφή στην λειτουργία και κατ' επέκταση στην παραγωγικότητα του οργανισμού. Αυτή η επίδραση στην παραγωγικότητα μπορεί να εκφράζεται τόσο με την απώλεια εσόδων από τη μη λειτουργία των κερδοφόρων δραστηριοτήτων όσο και με το κόστος από την αδράνεια του προσωπικού, του οποίου το έργο είναι άμεσα εξαρτώμενο από τα πληγέντα ΠΣ. Παρατηρούμε συγχρόνως, ότι ενώ το κόστος αυτό είναι ανάλογο με τη διάρκεια της ανάκαμψης (Recovery Time,T_{RT}), όπως είδαμε και παραπάνω, μπορεί να περιλαμβάνει και το κόστος που προκύπτει από την απώλεια των δεδομένων από το τελευταίο διαθέσιμο αντίγραφο ασφαλείας (Recovery Point, T_{RP}). Αυτό προκαλείται καθώς είναι πολύ πιθανό να απαιτείται η επανακαταχώρηση και επεξεργασία όλων αυτών των δεδομένων, εκ νέου. Επομένως η πραγματική διάρκεια του κόστους μη διαθεσιμότητας θα πρέπει να περιλαμβάνει και το χρονικό διάστημα στο οποίο αφορούν τα απολεσθέντα δεδομένα, θεωρώντας ότι:



Σχήμα 11: *Χρόνος μη διαθεσιμότητας δεδομένων*

Ο Jason Buffington, λαμβάνοντας υπόψη όλα τα παραπάνω προτείνει ενδεικτικά τον υπολογισμό του συνολικού κόστους με τον παρακάτω μαθηματικό [41]:

$$CoRI_{MTD} = (T_{RT} + T_{RP}) \times (Hr + Pr)$$

Όπου:

$CoRI_{MTD}$ = Συνολικό κόστος από τη μη διαθεσιμότητα

T_{RT} = Διάρκεια μέχρι την ανάκαμψη (Time- recovery time)

T_{RP} = Διάρκεια που αντιστοιχεί στην περίοδο που αφορά η απώλεια δεδομένων (Time- recovery point)

*H*r = Κόστος/ώρα από εργατοώρες λόγω αδράνειας του προσωπικού

*P*r = Κόστος/ώρα από απώλεια εσόδων

Σαν παράδειγμα δίνει την περίπτωση καταστροφής των ΠΣ ενός μικρού οργανισμού (20 ατόμων) στις 2 μ.μ., όπου εφαρμόζεται σύστημα λήψης αντιγράφων ασφαλείας, με τις παρακάτω παραδοχές:

- Η λειτουργία του οργανισμού κυμαίνεται μεταξύ 8π.μ.-5μ.μ.
- Γίνεται επιτυχής λήψη αντιγράφου κάθε βράδυ
- Η διάρκεια επισκευής-ανάκαμψης είναι μέχρι το τέλος της επόμενης εργάσιμης
- Το κόστος εργασίας του προσωπικού είναι 160$/ώρα
- Τα έσοδα του οργανισμού είναι 1000$/ώρα
- Η μη διαθεσιμότητα των ΠΣ προκαλούν διακοπή των εργασιών σε ποσοστό 100%

Σύμφωνα με αυτό είναι:

T_{RT} = 12 εργατοώρες

T_{RP} = 6 εργατοώρες

*H*r = 160$/ώρα

*P*r = 1000$/ώρα

Άρα:

$$CoRI_{MTD} = (12+6) \times (160+1000) = 18 \times 1160 = 20.880\$$$

Συμπεραίνουμε λοιπόν ότι, σύμφωνα με τη παραπάνω προσέγγιση, το κόστος των μέτρων ανάκαμψης για να κριθεί οικονομικά αποδοτικό θα πρέπει να είναι μικρότερο από το παραπάνω κόστος.

Αν και η εκτίμηση του κόστους των μέτρων ανάκαμψης μπορεί να γίνεται για κάθε υπηρεσία-λειτουργία του οργανισμού είθισται να υπολογίζεται για το σύνολο των ΠΣ, ιδίως όταν πρόκειται για Ολοκληρωμένα Πληροφοριακά Συστήματα, όπως είναι η κυρίαρχη τάση σήμερα.

3.5 Πρότυπα και οδηγίες σχετικά με ΣΑΚ

Η σχεδίαση ανάκαμψης από καταστροφές, λόγω του πολυδιάστατου χαρακτήρα της, μπορεί να αποδειχθεί ιδιαίτερα πολύπλοκη διαδικασία. Η πολυπλοκότητα αυτή μπορεί να γίνεται αισθητή τόσο κατά τη σχεδίαση και εφαρμογή του ΣΑΚ, όσο και κατά την πιστοποίηση της αποτελεσματικότητάς του. Απαιτείται λοιπόν η ύπαρξη μιας καθορισμένης μεθοδολογίας που πρέπει να ακολουθείται καθώς και η ικανοποίηση ενός συνόλου σημείων-ελέγχου (controls) ώστε να γίνεται εφικτή η σχεδίαση, εφαρμογή και πιστοποίηση των ΣΑΚ με δομημένο τρόπο.

Για την κάλυψη αυτών των απαιτήσεων έχουν εκδοθεί κατά καιρούς διάφορα πρότυπα και οδηγίες από οργανισμούς προτυποποίησης όπως ο διεθνής “International Organization for Standardization” (ISO) και ο “National Institute of Standards and Technology” (NIST) των Η.Π.Α. Τα πρότυπα αυτά συνήθως περιορίζονται στο να περιγράφουν τι πρέπει να τηρεί ένας οργανισμός, δίνοντάς του την ευχέρεια να επιλέξει τον τρόπο με τον οποίο θα το εφαρμόσει, ανάλογα με τις ανάγκες του και τις ιδιαίτερες συνθήκες –απαιτήσεις που υφίστανται σε κάθε περίπτωση.

Η χρήση κάποιου καταξιωμένου προτύπου αποτελεί τον πλέον ενδεδειγμένο τρόπο είτε για την αξιολόγηση του υπάρχοντος ΣΑΚ είτε για τη σχεδίαση ενός νέου. Μερικά από αυτά μπορεί να συνοδεύονται και από αντίστοιχη διαδικασία πιστοποίησης επιτυχούς εφαρμογής. Πολλές φορές η αποτελεσματική εφαρμογή κάποιου προτύπου μπορεί να κρίνεται απαραίτητη για τη συμμόρφωση ενός οργανισμού με νομικές απαιτήσεις, όπως συμβαίνει συνήθως, για παράδειγμα, με τις Sarbanes–Oxley Act of 2002 (SOX) [42] για τα χρηματοπιστωτικά ιδρύματα και Health Insurance Portability and Accountability Act of 1996 (HIPAA) [43] για τον κλάδο υγειονομικής ασφάλισης στις Η.Π.Α.

Παρακάτω περιγράφονται συνοπτικά τα κυριότερα πρότυπα που υπάρχουν αυτή τη στιγμή και σχετίζονται με τη σχεδίαση ανάκαμψης από καταστροφές.

3.5.1 ISO 27001:2005

"Information Security Management System"

Ένα από τα πιο αναγνωρισμένα διεθνή πρότυπα σχετικά με την ασφάλεια πληροφοριών είναι το ISO 27001:2005 [44] το οποίο περιέχει όλα όσα απαιτείται να πληροί ένας οργανισμός για την εφαρμογή ενός αποτελεσματικού Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Οι περιγραφόμενες απαιτήσεις-ενέργειες είναι προληπτικού κυρίως χαρακτήρα και όχι διορθωτικού. Είναι διαρθρωμένο σε 11 Ρήτρες ελέγχου (control clauses) οι οποίες πρέπει να ικανοποιούνται. Ανάμεσα σε αυτές είναι και μια που αφορά εξολοκλήρου το κομμάτι της διαχείρισης της Επιχειρησιακής Συνέχειας (A.14-Business Continuity Management) σύμφωνα με το οποίο θα πρέπει:

- Να υπάρχει **ελεγχόμενη διαδικασία** η οποία να καθορίζει τις απαιτήσεις ασφάλειας πληροφοριών για την επιχειρησιακή συνέχεια του οργανισμού.
- Να έχουν αναγνωριστεί όλες οι **απειλές** για την επιχειρησιακή συνέχεια, να έχει αξιολογηθεί η **πιθανότητα** να συμβούν καθώς και να έχουν εκτιμηθεί οι **επιπτώσεις** τους στην ασφάλεια της πληροφορίας.
- Να έχουν σχεδιαστεί και εφαρμοστεί **πλάνα ανάκαμψης** και συνέχισης των επιχειρησιακών λειτουργιών με έμφαση στη διαθεσιμότητα της πληροφορίας
- Να υπάρχει **ενιαίο πλαίσιο σχεδίων** επιχειρησιακής συνέχειας με σκοπό την τυποποίηση του σχεδιασμού και την ενιαία αντιμετώπιση των απαιτήσεων ασφάλειας πληροφοριών.
- Τα πλάνα ανάκαμψης και επιχειρησιακής συνέχειας **να δοκιμάζονται και να αναθεωρούνται** σε τακτά χρονικά διαστήματα ώστε να παραμένουν επικαιροποιημένα και αποτελεσματικά.

Η αποτελεσματική εφαρμογή του ISO 27001:2005 οδηγεί σε λήψη της αντίστοιχης πιστοποίησης.

3.5.2 BS 25999:2007

"British Standard for Business Continuity Management"

Το BS 25999 [45] αποτελεί το πλέον καταξιωμένο πρότυπο σχετικά με την διασφάλιση της επιχειρησιακής συνέχειας ενός οργανισμού. Παρέχει οδηγίες σχετικά με τις απαιτήσεις που

πρέπει να ικανοποιούνται προκειμένου να διασφαλίζεται η επιχειρησιακή λειτουργία ενός οργανισμού σε περίπτωση καταστροφικού συμβάντος. Μπορεί να αποτελέσει τη βάση για κάποιον που θέλει να κατανοήσει τις αρχές και τις απαιτήσεις της επιχειρησιακής συνέχειας, ολικά, για τον οργανισμό. Συμπεριλαμβάνει, χωρίς να εξειδικεύει, θέματα σχετικά με την ανάκαμψη των Πληροφοριακών του Συστημάτων. Παρόλο που περιγράφονται διεξοδικά οι απαιτήσεις της επιχειρησιακής συνέχειας, δεν περιγράφεται ο τρόπος με τον οποίο αυτές εφαρμόζονται και οι πρακτικές που πρέπει να ακολουθούνται.

Το πρότυπο αυτό μπορεί μετά από επιτυχή έλεγχο να οδηγήσει σε λήψη της αντίστοιχης πιστοποίησης. Πρόκειται να αποσυρθεί μέσα στο 2012 και να αντικατασταθεί από το ISO 22301 [46].

3.5.3 BS 25777:2008

"Code of Practice for IT Service Continuity Management"

Το BS 25777 [47] μπορεί να θεωρηθεί ως συμπληρωματικό του BS 25999 καθώς εστιάζει στην διασφάλιση της συνέχισης της λειτουργίας των Πληροφοριακών Συστημάτων ενός οργανισμού. Αποτέλεσε την εξέλιξη του προτύπου PAS 77:2006 και περιλαμβάνει οδηγίες για την υλοποίηση των απαιτήσεων του BS 25999 όσον αφορά στα Πληροφοριακά Συστήματα ενός οργανισμού. Αντικαταστάθηκε πρόσφατα από το ISO 27031 [48].

3.5.4 ISO 24762:2008

"Guidelines for Information and Communications Technology Disaster Recovery Services"

Το πρότυπο ISO 24762 [49] περιγράφει τις βέλτιστες πρακτικές που σχετίζονται με σχέδια ΣΑΚ πληροφοριακών και επικοινωνιακών συστημάτων. Αναφέρεται σε θέματα ελαχιστοποίησης κινδύνων (όπως είναι η προστασία από πυρκαγιά, πτώση τάσης), ελέγχου φυσικής και λογικής πρόσβασης σε πληροφοριακά συστήματα, διαχείρισης πόρων και προμηθευτών, επιλογής εναλλακτικής εγκατάστασης και διαμόρφωσης σχεδίων ΣΑΚ.

Απευθύνεται, όχι τόσο σε οργανισμούς που θέλουν να αναπτύξουν ένα ΣΑΚ για να καλύψουν τις δικές τους ανάγκες, όσο σε οργανισμούς που επιθυμούν να παρέχουν την ανάκαμψη ως υπηρεσία προς τρίτους.

3.5.5 ISO 27031:2011

"Guidelines for Information and Communications Technology Readiness for Business Continuity"

Το ISO 27031 [48], ως ένα από τα νεότερα πρότυπα (Μάρτης 2011) που σχετίζονται με την ανάκαμψη από καταστροφές, επιχειρεί να περιγράψει της βασικές αρχές για την ετοιμότητα των πληροφοριακών και επικοινωνιακών συστημάτων ώστε να διασφαλίζουν την επιχειρησιακή συνέχεια.

Περιγράφει μεθόδους και διαδικασίες για τη διαχείριση περιστατικών ασφαλείας αλλά και για το σχεδιασμό ετοιμότητας των Πληροφοριακών Συστημάτων. Αποτελεί ένα πρότυπο το οποίο επιχειρεί το συγκερασμό της επιχειρησιακής συνέχειας (BS 25999) με τη διαχείριση της συνέχειας των Πληροφοριακών Συστημάτων (BS 25777) και την ανάκαμψή τους από καταστροφές (ISO 24762), προσαρμοσμένο έτσι ώστε να είναι συμβατό με το πλαίσιο που περιγράφεται στο ISO 27001. Αποτελεί με αυτό τον τρόπο ένα συμπλήρωμα για τις ειδικότερες απαιτήσεις της επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφές που απαιτούνται για τη συμμόρφωση με το ISO 27001.

3.5.6 NIST SP800-34 Rev. 1

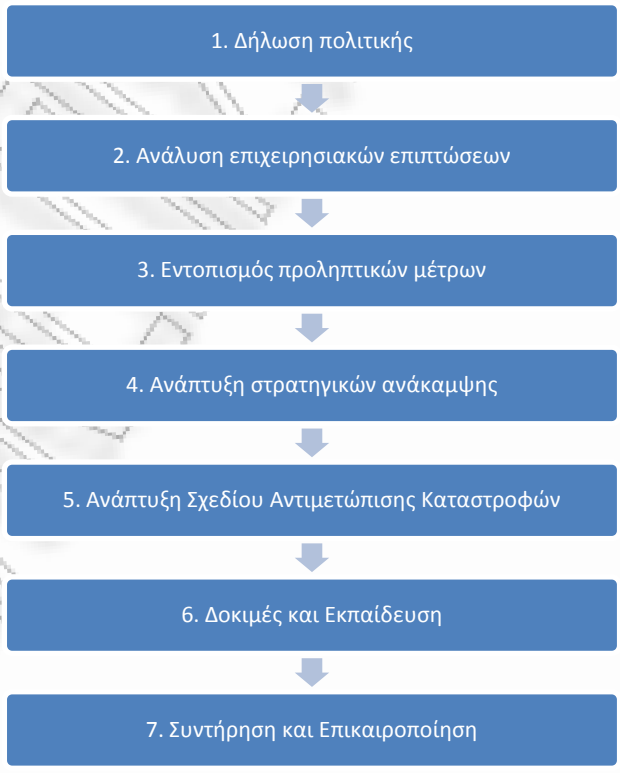
" Contingency Planning Guide for Federal Information Systems"

Ο οργανισμός NIST εξέδωσε το 2002 τον οδηγό 800-34 [7] για να κατευθύνει τους οργανισμούς που επιθυμούν να επιτύχουν επιχειρησιακή συνέχεια στις λειτουργίες των Πληροφοριακών τους Συστημάτων. Αποτελεί έναν καταξιωμένο, κατανοητό και εμπεριστατωμένο οδηγό ο οποίος αναφέρεται σε διοικητικά, λειτουργικά και τεχνικά ζητήματα που σχετίζονται με τον ΣΑΚ.

Η οδηγία SP800-34 αναθεωρήθηκε πρόσφατα με την έκδοση Rev.1 (2010) και, αντίθετα με τα υπόλοιπα αναγνωρίσιμα πρότυπα και οδηγίες, διατίθεται δωρεάν προς χρήση.

4 Διαδικασία σχεδιασμού πλάνου

Καθώς κάθε οργανισμός διαθέτει διαφορετικούς πόρους, διαφορετικό μοντέλο λειτουργίας και έχει διαφορετικές απαιτήσεις, όσον αφορά την ανάκαμψη από καταστροφές, δεν μπορεί να υπάρξει κάποιο απόλυτα προτυποποιημένο σχέδιο ανάκαμψης το οποίο να καλύπτει καθολικά τις ανάγκες κάθε οργανισμού. Επομένως ένα ΣΑΚ έχει μοναδικό χαρακτήρα για τον κάθε οργανισμό στον οποίο αναφέρεται και πρέπει να σχεδιάζεται κατά περίπτωση. Ωστόσο η διαδικασία σχεδιασμού η οποία ακολουθείται σε κάθε περίπτωση παρουσιάζει κοινά χαρακτηριστικά και εφαρμόζεται με ενιαίο τρόπο για κάθε πληροφοριακό σύστημα. Για την εφαρμογή αυτής της διαδικασίας μπορεί να χρησιμοποιηθεί οποιοδήποτε από τα παραπάνω περιγραφόμενα πρότυπα και οδηγίες, ανάλογα και με τις απαιτήσεις του κάθε οργανισμού. Για να παρουσιαστεί αυτή η διαδικασία επιλέχθηκε ως σημείο αναφοράς ο οδηγός του NIST [7], καθότι αποτελεί μία από τις πιο αναγνωρισμένες λύσεις αλλά και παρέχεται για ελεύθερη χρήση από κάθε ενδιαφερόμενο. Στην οδηγία αυτή περιγράφεται η διαδικασία του σχεδιασμού και της υλοποίησης ενός πλάνου ανάκαμψης ως μια ακολουθία επτά βημάτων (Σχήμα 12). Παρακάτω παρατίθενται τα βήματα αυτά.



Σχήμα 12: *Διαδικασία σχεδιασμού πλάνου ανάκαμψης κατά NIST*

4.1 Δήλωση πολιτικής

Το πρώτο βήμα που θα πρέπει να πραγματοποιηθεί για τη διασφάλιση του σχεδιασμού αλλά και της εφαρμογής ενός ΣΑΚ είναι η σαφής δήλωση της ακολουθούμενης πολιτικής στο ζήτημα αυτό, από τον οργανισμό. Η δήλωση πολιτικής πρέπει πρωτίστως να καθορίζει τους στόχους του ΣΑΚ και να εκφράζει τη δέσμευση του οργανισμού στην εφαρμογή του. Η δέσμευση αυτή πρέπει να εκφράζεται με τον πλέον επίσημο τρόπο, συνήθως με την υπογραφή της ανώτερης διοικητικής αρχής. Η δήλωση πολιτικής συνήθως αποτελείται από ένα σύντομο αλλά περιεκτικό κείμενο που μεταξύ άλλων μπορεί να περιέχει δεσμεύσεις για τα παρακάτω:

- ρόλους και αρμοδιότητες
- έκταση εφαρμογής
- απαιτήσεις πόρων
- απαιτήσεις εκπαίδευσης
- πρόγραμμα ασκήσεων και δοκιμών
- πρόγραμμα συντήρησης σχεδίου

4.2 Ανάλυση επιχειρησιακών επιπτώσεων

Επόμενο βήμα αποτελεί η ανάλυση των επιπτώσεων, στην περίπτωση που συμβεί μια καταστροφή. Αυτές οι επιπτώσεις στην επιχειρησιακή λειτουργία ενός οργανισμού αφορούν σε διαφορετικούς τομείς όπως περιγράφονται παραπάνω στην §2.2. Η προσπάθεια σε αυτό το στάδιο επικεντρώνεται στον προσδιορισμό, είτε ποσοτικά είτε ποιοτικά, των επιπτώσεων και στην ανάλυσή τους, έτσι ώστε να υπάρξει κατάλληλη αναγνώρισή τους και κατηγοριοποίηση τους ανάλογα με τις πραγματικές ανάγκες του οργανισμού (ένα χαρακτηριστικό παράδειγμα ποσοτικής ανάλυσης των οικονομικών επιπτώσεων είναι αυτό που περιγράφεται στην §3.4.6). Για να επιτευχθεί αυτός ο στόχος κύριο μέλημα θα πρέπει να είναι η κατά το δυνατόν καθολική συμμετοχή όλων των τμημάτων του οργανισμού στην ανάλυση και η ορθολογική αξιολόγηση των ευρημάτων, ώστε το αποτέλεσμα να είναι το πλέον αντικειμενικό.

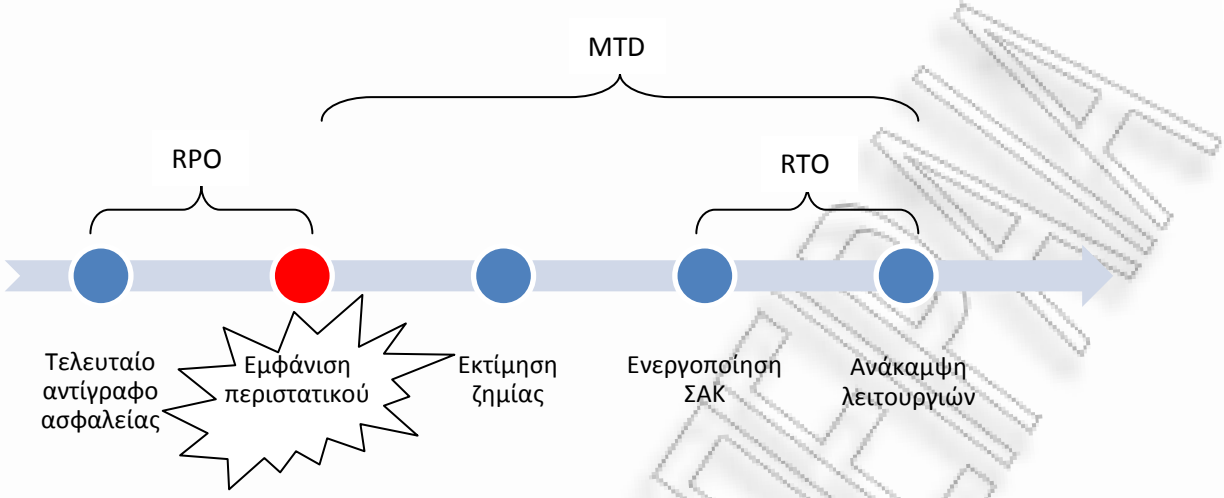
Για την πραγματοποίηση αυτής της διαδικασίας αξιολόγησης-ιεράρχησης χρησιμοποιούνται οι παρακάτω δείκτες ως σημεία αναφοράς:

- **Μέγιστος ανεκτός χρόνος δυσλειτουργίας (Maximum Tolerable Downtime-MTD)**. Ο δείκτης αυτός αφορά στο μέγιστο αποδεκτό χρόνο δυσλειτουργίας ή μη λειτουργίας κάποιας κρίσιμης επιχειρησιακής λειτουργίας. Για τον υπολογισμό του λαμβάνονται υπόψη όλες οι επιπτώσεις που μπορεί να έχει η μη παροχή της συγκεκριμένης υπηρεσίας στον οργανισμό.

- **Επιδιωκόμενος χρόνος ανάκτησης (Recovery Time Objective-RTO)**. Είναι ο χρόνος που χρειαζόμαστε για να ανακάμψουμε από μια καταστροφή. Ειδικότερα αφορά στο μέγιστο χρόνο κατά τον οποίο κάποιος πόρος μπορεί να παραμένει μη διαθέσιμος, χωρίς να προκαλούνται μη ανεκτές επιπτώσεις σε άλλους πόρους ή κρίσιμες επιχειρησιακές λειτουργίες ή να επηρεάζεται το MTD τους. Ανάλογα με τη τιμή του δείκτη RTO επιλέγονται και τα κατάλληλα μέτρα, που δύνανται να ικανοποιήσουν την απαίτηση αυτή ώστε να διασφαλίζεται, κατ' επέκταση, και το MTD της κρίσιμης λειτουργίας. Πρέπει να τονιστεί ότι ο χρόνος που μεσολαβεί από την εμφάνιση ενός περιστατικού μέχρι την ενεργοποίηση του ΣΑΚ θα πρέπει να λαμβάνεται υπόψη κατά τον υπολογισμό του RTO.

- **Επιδιωκόμενο σημείο ανάκτησης (Recovery Point Objective-RPO)**. Είναι η ανεκτή παλαιότητα των δεδομένων μετά από την ολοκλήρωση της διαδικασίας ανάκτησης. Αποτελεί δηλαδή το μέγιστο σημείο πίσω στο χρόνο στο οποίο αφορούν τα ανακτημένα δεδομένα, χωρίς να υπεισέρχονται μη ανεκτές επιπτώσεις. Για παράδειγμα εάν το RPO είναι 24 ώρες, μπορούμε να πούμε ότι είναι ανεκτό μετά από την ανάκτηση να μην είναι διαθέσιμα τα δεδομένα των τελευταίων 24 ωρών (πράγμα που τεχνικά σημαίνει ότι πρέπει να υπάρχει διαθέσιμο ολοκληρωμένο backup τις τελευταίες 24 ώρες).

Στο παρακάτω σχήμα (Σχήμα 13) φαίνεται ο συσχετισμός των δεικτών αυτών συναρτήσει του κύκλου ζωής ενός περιστατικού.



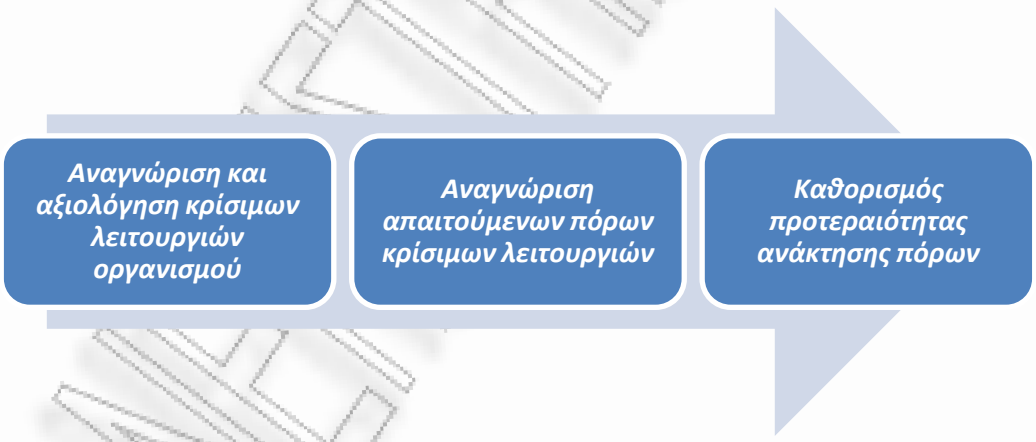
Σχήμα 13: *Συσχετισμός δεικτών ανάκαμψης (MTD-RPO-RTO)*

Η ανάλυση των επιπτώσεων, γνωστή κυρίως με το διεθνή όρο **Business Impact Analysis (BIA)**, θεωρείται ίσως η πιο κρίσιμη διαδικασία κατά τη σχεδίαση του ΣΑΚ και αποτελείται από την αναγνώριση και αξιολόγηση των κρίσιμων λειτουργιών του οργανισμού, την αναγνώριση των απαιτούμενων πληροφοριακών πόρων για αυτές τις λειτουργίες και τον καθορισμό της προτεραιότητας ανάκτησης των πόρων αυτών για την ανάκαμψη των λειτουργιών σε περίπτωση καταστροφής:

- ***Αναγνώριση και αξιολόγηση κρίσιμων λειτουργιών οργανισμού:*** Πρώτο στάδιο για την αποτελεσματική **ανάλυση των επιπτώσεων** αποτελεί η καταγραφή των κρίσιμων λειτουργιών ενός οργανισμού και των συνεπειών που μπορεί να έχει η μη διαθεσιμότητά τους. Όπως παρουσιάστηκε και παραπάνω (§2.2), αυτές οι συνέπειες μπορεί να είναι πολυποίκιλες, με διαφορετική βαρύτητα για κάθε λειτουργία και συνεπώς με διαφορετικό βαθμό ανοχής. Η διαδικασία αυτή πρέπει να γίνεται με τη συνδρομή όλων των δομών-τμημάτων του οργανισμού και να επικαιροποιείται από την ανώτατη διοικητική αρχή. Ως αποτέλεσμα έχουμε την **αναγνώριση** αλλά και την **προτεραιοποίηση** όλων των επιχειρησιακών λειτουργιών που πρέπει να διασφαλιστούν. Για να επιτευχθεί αυτή η προτεραιοποίηση γίνεται χρήση του δείκτη **MTD** ο οποίος αποκαλύπτει το βαθμό κρισιμότητα και τον απαιτούμενο χρόνο ανάκαμψης.

- ***Αναγνώριση απαιτούμενων πόρων κρίσιμων λειτουργιών:*** Επειδή κάθε επιχειρησιακή λειτουργία βασίζεται σε διαφορετικά πληροφοριακά συστήματα-πόρους, στο στάδιο αυτό γίνεται η αναγνώριση αυτών των **απαιτούμενων πόρων**. Οι πόροι αυτοί μπορεί να αποτελούνται από εξοπλισμό, ανθρώπους, προμηθευτές, τεχνολογίες και διαδικασίες. Στο στάδιο αυτό πρέπει να καθοριστεί και η μέγιστη ανοχή απώλειας δεδομένων από τα πληροφοριακά συστήματα, που συσχετίζονται με κάθε κρίσιμη λειτουργία, το οποίο θα χρησιμοποιηθεί για τον καθορισμό του **δείκτη RPO** για τους αντίστοιχους πόρους.

- ***Καθορισμός προτεραιότητας ανάκτησης πόρων:*** Έχοντας κατανοήσει τις ανάγκες του οργανισμού με τη μορφή των κρίσιμων λειτουργιών και αφού τις αντιστοιχίσουμε στους κατάλληλους πόρους από τους οποίους αυτές εξαρτώνται μπορούμε να προβούμε στο τελικό στάδιο της ιεράρχησης της ανάκτησης. Εδώ καλούμαστε να ιεραρχήσουμε την ανάκτηση των πληροφοριακών μας πόρων ώστε να πετύχουμε την ικανοποίηση των απαιτήσεων ανάκαμψης των εξαρτώμενων λειτουργιών. Στο στάδιο αυτό γίνεται σύνθεση των αποτελεσμάτων από τις προηγούμενες διεργασίες και καθορίζονται οι δείκτες RTO και RPO ως προσδοκώμενοι στόχοι ανάκτησης των πόρων.



Σχήμα 14: *Διαδικασία ανάλυσης επιχειρησιακών επιπτώσεων*

Όπως αντιλαμβάνεται κανείς αυτό το βήμα αποτελεί τον συνδετικό κρίκο μεταξύ των δομών της Διοίκησης και των δομών των ΤΠΕ μέσα σε έναν οργανισμό. Με την ολοκλήρωσή του επιτυγχάνεται η αντιστοίχιση των απαιτήσεων σε επιχειρησιακό επίπεδο με αυτές που απαιτούνται σε επίπεδο ΤΠΕ. Το γεγονός αυτό επιτρέπει την μετάβαση στα επόμενα βήματα τα οποία επικεντρώνονται πλέον στο πεδίο των ΤΠΕ.

4.3 Εντοπισμός προληπτικών μέτρων

Σε αυτό το βήμα γίνεται προσπάθεια να εντοπιστούν τα μέτρα τα οποία μπορούν να παρθούν από τον οργανισμό ώστε είτε να προληφθούν οι καταστροφές είτε να αναγνωριστούν εγκαίρως και να περιοριστούν οι συνέπειές τους. Είναι σημαντικό να εξευρεθούν και να εφαρμοστούν όλα αυτά τα πρόσφορα μέσα για κάθε πιθανή καταστροφή, καθώς κατά κανόνα τα προληπτικά μέτρα έχουν μικρότερο οικονομικό αντίκτυπο από αυτά της ανάκαμψης. Έχει γίνει προσπάθεια τόσο από το NIST με το 800-53 [50] όσο και από το ISO με το 27002:2005 [51] να καταγραφούν και να κατηγοριοποιηθούν τα διαθέσιμα προληπτικά μέτρα.

Ιδιαίτερη έμφαση πρέπει να δοθεί σε όσα αφορούν στον περιορισμό εξωτερικών ή περιβαλλοντικών απειλών, καθώς σχετίζονται άμεσα με τον κίνδυνο των καταστροφών ο οποίος και εξετάζεται στη παρούσα εργασία. Μερικά από αυτά τα μέτρα μπορεί να είναι ενδεικτικά:

- Εφεδρικά συστήματα (αδιάλειπτης παροχής ενέργειας, γεννήτριες Η/Ζ, ψύξης)
- Συστήματα υψηλής ανοχής σε ακραίες περιβαλλοντικές συνθήκες
- Χρήση ανιχνευτών (πυρασφάλειας, πλημμύρας, υπερθέρμανσης, διαρροής επικίνδυνων αερίων)
- Συστήματα ελέγχου πρόσβασης και ελέγχου εγκαταστάσεων

Η εφαρμογή ενός αναγνωρισμένου προτύπου ή η συμμόρφωση με κάποιες καταξιωμένες καλές πρακτικές, όπως είναι το ISO27001 και οι οδηγίες του NIST αντίστοιχα, μπορούν να αποτελέσουν για έναν οργανισμό εχέγγυο για τη λήψη των αναγκαίων προληπτικών μέτρων ώστε να περιοριστούν οι πιθανοί κίνδυνοι.

4.4 Επιλογή και Ανάπτυξη στρατηγικών ανάκαμψης

4.4.1 Επιλογή στρατηγικών

Αφού εντοπιστούν όλα τα πιθανά μέτρα που μπορεί να έχουν εφαρμογή στον υπό εξέταση οργανισμό, επόμενο βήμα αποτελεί η επιλογή των πλέον κατάλληλων στρατηγικών αντιμετώπισης καταστροφών.

Ένα από τα χρησιμοποιούμενα μοντέλα στο πεδίο της Διαχείρισης Κινδύνου είναι το «4T model» [45], όπου για την αντιμετώπιση των κινδύνων προτείνεται η επιλογή μεταξύ 4 στρατηγικών:

- Treat – Αντιμετώπιση
- Terminate - Τερματισμός
- Transfer - Μεταφορά
- Tolerate – Αποδοχή

Προσαρμόζοντας το μοντέλο αυτό στην διαδικασία επιλογής των στρατηγικών ανάκαμψης για κάθε επιχειρησιακή λειτουργία, και κατ' επέκταση για την ανάκαμψη των αντίστοιχων πληροφοριακών πόρων, μπορούμε να διακρίνουμε τις παρακάτω διαθέσιμες στρατηγικές [52]:

- **Treat** (Αντιμετώπιση)

  Αποδοχή και εφαρμογή των αναγνωρισμένων μέτρων, εφόσον κρίνεται ότι η αποτελεσματικότητά τους και το κόστος τους είναι σε αποδεκτό επίπεδο.

- **Terminate** (Τερματισμός)

  Ο κίνδυνος και κατ' επέκταση οι επιπτώσεις του για κάποια επιχειρησιακή λειτουργία εξαλείφονται μέσω της αλλαγής-αναμόρφωσης της ίδιας της λειτουργίας. Αυτό μπορεί να συμβεί όταν:

  -τα διαθέσιμα μέτρα έχουν πολύ υψηλό κόστος, ενώ οι επιπτώσεις μιας ενδεχόμενης καταστροφής δεν μπορούν να γίνουν αποδεκτές από τον οργανισμό.

  -η λειτουργία δύναται να αναμορφωθεί όταν αυτή η αναμόρφωση εξυπηρετεί και πρόσθετα οφέλη για τον οργανισμό, όπως η μείωση κόστους λειτουργίας, χωρίς να επηρεάζει τον κύριο σκοπό της.

  -κάθε διαθέσιμο αντίμετρο θα επέφερε αδυναμία αποδοτικής εκπλήρωσης της λειτουργίας-υπηρεσίας με τη παρούσα δομή της.

- **Transfer** (Μεταφορά-Μεταβίβαση)

  Μεταφορά της ευθύνης ανάκαμψης ή των επιπτώσεων της καταστροφής ή και της ίδιας της λειτουργίας, κυρίως μέσω ανάθεσης σε τρίτους ή μέσω ασφαλιστικών μέτρων. Αυτό μπορεί να επιλεγεί όταν:

  - οι επιπτώσεις είναι κατά βάση οικονομικού χαρακτήρα οπότε είναι μετρήσιμες ώστε να μπορούν να αποτελέσουν αντικείμενο ασφάλισης.
  - η λειτουργία-υπηρεσία μπορεί να ανατεθεί σε τρίτους με τρόπο που να εξυπηρετεί και άλλους σκοπούς, όπως η μείωση κόστους λειτουργίας.
  - οι τρίτοι που θα αναλάβουν την ευθύνη διαθέτουν την απαραίτητη τεχνογνωσία ώστε να αντιμετωπίσουν καλύτερα ένα καταστροφικό συμβάν.

- **Tolerate** (Αποδοχή)

  Αποδοχή των ενδεχόμενων επιπτώσεων χωρίς την εφαρμογή μέτρων αντιμετώπισης. Η στρατηγική αυτή μπορεί να εφαρμοστεί όταν:

  -οι επιπτώσεις μιας ενδεχόμενη καταστροφής είναι αμελητέες.

  -δεν υπάρχουν μέτρα τα οποία μπορούν να αντιμετωπίσουν ένα καταστροφικό γεγονός και πρακτικά οι επιπτώσεις δε μπορούν να αποφευχθούν.

  -το κόστος των μέτρων ξεπερνούν κατά πολύ το κόστος των ενδεχόμενων επιπτώσεων.

Λαμβάνοντας υπόψη τις διάφορες επιπτώσεις κάποιας καταστροφής στις υπηρεσίες-λειτουργίες, το βαθμό στον οποίο κρίνονται ανεκτές από τον οργανισμό καθώς και το κόστος των προσφερόμενων μέτρων, μπορούμε να επιλέξουμε τις απαραίτητες στρατηγικές αντιμετώπισης.

Βασικός στόχος θα πρέπει να είναι, όπως αναφέρεται παραπάνω και στην §3.4.5, η ακολουθούμενη στρατηγική να μην επιφέρει μεγαλύτερο κόστος για τον οργανισμό απ’ ότι οι ενδεχόμενες επιπτώσεις μιας καταστροφής.

4.4.2 Ανάπτυξη στρατηγικών

Έχοντας επιλέξει την εκάστοτε ακολουθούμενη στρατηγική για κάθε λειτουργία-υπηρεσία, ως επόμενο βήμα έχουμε την ανάπτυξη αυτών και τον σχεδιασμό εφαρμογής τους.

Μια επιτυχημένη και ολοκληρωμένη στρατηγική, σύμφωνα με τις αρχές διαχείρισης έργων, αποτελείται από την αλληλεπίδραση του τρίπτυχου ανθρώπων, διεργασιών και τεχνολογιών. Σε κάθε περίπτωση θα πρέπει να προσδιορίζονται πρωτίστως:

Άνθρωποι: Ποιοί είναι υπεύθυνοι για κάθε ενέργεια, ποιοι εμπλέκονται, ποιός ο ρόλος και οι αρμοδιότητες τους καθώς και πώς διασφαλίζεται ο βαθμός ετοιμότητάς τους.

Διεργασίες: Ποιές διεργασίες διακρίνονται, από τι αποτελούνται , ποια τα αναμενόμενα αποτελέσματά τους και πώς αυτές πρέπει να εφαρμόζονται.

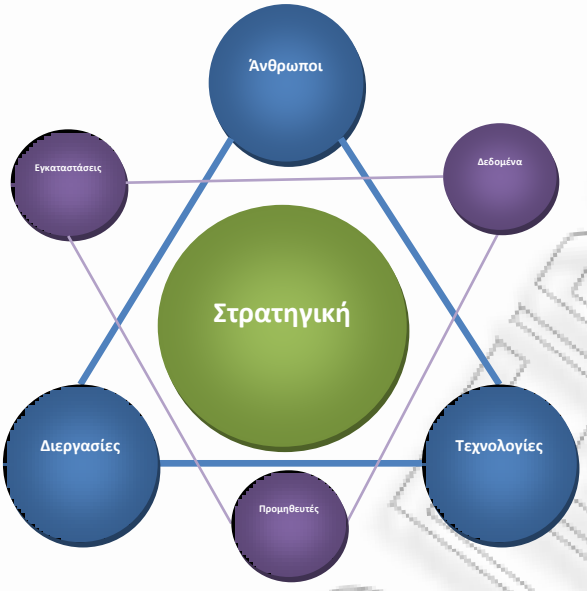
Τεχνολογίες: Ποιά τεχνολογικά μέσα χρησιμοποιούνται και με ποιο τρόπο, για την υποστήριξη της εφαρμοζόμενης στρατηγικής.

Συμπληρωματικά για την περίπτωση των ΠΣ θα πρέπει να προσδιορίζονται [45]:

Εγκαταστάσεις: Ποιές εγκαταστάσεις θα χρησιμοποιηθούν για την ανάκαμψη των λειτουργιών και κατά πόσο κρίνεται απαραίτητη η χρήση εναλλακτικών εγκαταστάσεων.

Δεδομένα: Ποιά δεδομένα κρίνονται απαραίτητα για την ανάκαμψη και με ποιό τρόπο αυτά διατηρούνται. Σε ποιά μορφή είναι διαθέσιμα και πως διασφαλίζονται ως προς την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα.

Εξοπλισμός- Προμηθευτές: Τι εξοπλισμός απαιτείται για την ανάκαμψη και πως διασφαλίζεται η επάρκειά του καθώς και πως εξασφαλίζεται η διαθεσιμότητά του από τους προμηθευτές. Ποιές είναι οι υποχρεώσεις των προμηθευτών και των παρόχων υπηρεσιών και πώς διασφαλίζεται το επίπεδο παροχής αυτών των υπηρεσιών.



Σχήμα 15: *Συστατικά διαμόρφωσης στρατηγικών αντιμετώπισης*

Αυτά τα έξι συστατικά και ο τρόπος που αλληλεπιδρούν διαμορφώνουν την εκάστοτε στρατηγική αντιμετώπισης-ανάκαμψης από καταστροφές. Παρακάτω στη §5 παρατίθενται, για κάθε ένα από αυτά τα συστατικά, τα σύγχρονα μέτρα αντιμετώπισης καθώς και τα κριτήρια με τα οποία θα πρέπει να επιλέγονται.

4.5 Ανάπτυξη Σχεδίου Ανάκαμψης από Καταστροφές

Το σύνολο των επιλεχθέντων στρατηγικών από το προηγούμενο βήμα, και ο τρόπος που αυτές εφαρμόζονται, για κάθε λειτουργία και για κάθε σχετικό με αυτές ΠΣ αποτελούν τον κύριο συστατικό του ΣΑΚ ενός οργανισμού. Απομένει λοιπόν να καθοριστούν τα κριτήρια και ο τρόπος με τον οποίο ενεργοποιούνται, εφαρμόζονται και ολοκληρώνονται αυτές οι στρατηγικές.

Για να επιτευχθεί αυτό απαιτείται η περιγραφή με σαφήνεια ενός συνόλου διαδικασιών-οδηγιών με τη μορφή σχεδίου δράσης (action plan). Ένα τέτοιο πλάνο (σχέδιο) δράσης απευθύνεται στα πρόσωπα που καλούνται να φέρουν εις πέρας την ανάκαμψη με στόχο να περιγράψει λεπτομερώς όλη τη διαδικασία που πρέπει να ακολουθηθεί.

Ο NIST [7] προτείνει να υπάρχει ισορροπία στο επίπεδο της λεπτομέρειας που παρέχεται, καθώς όσο πιο λεπτομερές γίνεται τόσο χάνει την ευελιξία του και την επεκτασιμότητά του.

Μια καλή στρατηγική αντιμετώπισης αυτής της λεπτής ισορροπίας θα ήταν το ΣΑΚ στα πρώτα στάδια σχεδιασμού του να είναι γενικό, ώστε να καλύπτει όσο το δυνατόν πιο ευρύ πεδίο, και με την ωρίμανσή του να γίνεται πιο λεπτομερές όπου απαιτείται (κυρίως στις τεχνικές διαδικασίες ώστε να αποφεύγονται λάθη και καθυστερήσεις). Με τον τρόπο αυτό το ΣΑΚ μπορεί να συμπορεύεται και να προσαρμόζεται με το επίπεδο ετοιμότητας και την εμπειρία των εμπλεκομένων μερών.

Για να είναι ολοκληρωμένο το ΣΑΚ, ως σχέδιο δράσης, θα πρέπει να περιέχει αναφορικά [7] [53]:

- Γενικά στοιχεία για τον οργανισμό και τα ΠΣ
- Τους στόχους ανάκαμψης
- Τις επιλεχθείσες στρατηγικές
- Τους ρόλους και τις αρμοδιότητες των εμπλεκομένων
- Τις απαραίτητες ενέργειες αντιμετώπισης
- Τα αρχεία-έντυπα που απαιτούνται

Στις επόμενες παραγράφους περιγράφονται αυτά τα συστατικά.

4.5.1 Γενικά στοιχεία

Αρχικά στο κεφάλαιο αυτό δίνονται πληροφορίες σχετικά με το ίδιο το ΣΑΚ όπως ο υπεύθυνος επικαιροποίσης, η τελευταία ημερομηνία έγκρισης και κατάλογος όλων των αλλαγών τις οποίες έχει υποστεί.

Δίδεται μια συνοπτική περιγραφή του οργανισμού όσον αφορά το αντικείμενο εργασίας του, τη νομική του μορφή και τις υποχρεώσεις του ως νομικό πρόσωπο. Ακολουθεί μια σύντομη περιγραφή των Πληροφοριακών Συστημάτων τα οποία εξυπηρετούν τον οργανισμό και τις λειτουργίες που υποστηρίζουν.

Σε περίπτωση που υπάρχουν εναλλακτικές εγκαταστάσεις θα πρέπει να υπάρχει μια σύντομη περιγραφή των δυνατοτήτων τους και τα απαραίτητα στοιχεία επικοινωνίας (τηλέφωνα, διεύθυνση). Στο κεφάλαιο αυτό θα πρέπει να υπάρχουν εν γένει όλες οι απαραίτητες πληροφορίες που κρίνονται ως οι πλέον σημαντικές, όπως είναι ο τόπος και ο

χρόνος συνάντησης μετά από την καταστροφή και τα στοιχεία επικοινωνίας του καθ' ύλην υπεύθυνου για το ΣΑΚ.

4.5.2 Στόχοι

Στο κεφάλαιο αυτό θα πρέπει να δηλώνονται οι στόχοι του ΣΑΚ τόσο για τα επιμέρους ΠΣ όσο και για το σύνολό τους, σε περίπτωση ολικής καταστροφής και μετάβασης σε εναλλακτικές εγκαταστάσεις. Οι στόχοι αυτοί προκύπτουν από τη διαδικασία εκτίμησης επιπτώσεων και εκφράζονται με τους δείκτες RTO, RPO, MTD καθώς και με την ιεραρχία ανάκτησης πόρων που προέκυψε (βλέπε §4.2). Παράλληλα εδώ θα πρέπει να αναφέρονται όλες οι παραδοχές που έγιναν κατά τον σχεδιασμό του ΣΑΚ.

4.5.3 Στρατηγικές

Εν συνεχεία περιγράφονται οι επιλεχθείσες στρατηγικές για κάθε ΠΣ και ο τρόπος που αυτές εφαρμόζονται. Προτείνεται για κάθε ΠΣ να δίδεται και εναλλακτική στρατηγική σε περίπτωση που για κάποιο λόγο αποδειχθεί ότι η κύρια είναι αναποτελεσματική, ώστε να μην προκύψει αδιέξοδο κατά τη διαδικασία ανάκτησης, η οποία μπορεί να επηρεάσει την επιτυχή έκβαση του ΣΑΚ.

4.5.4 Ρόλοι και αρμοδιότητες

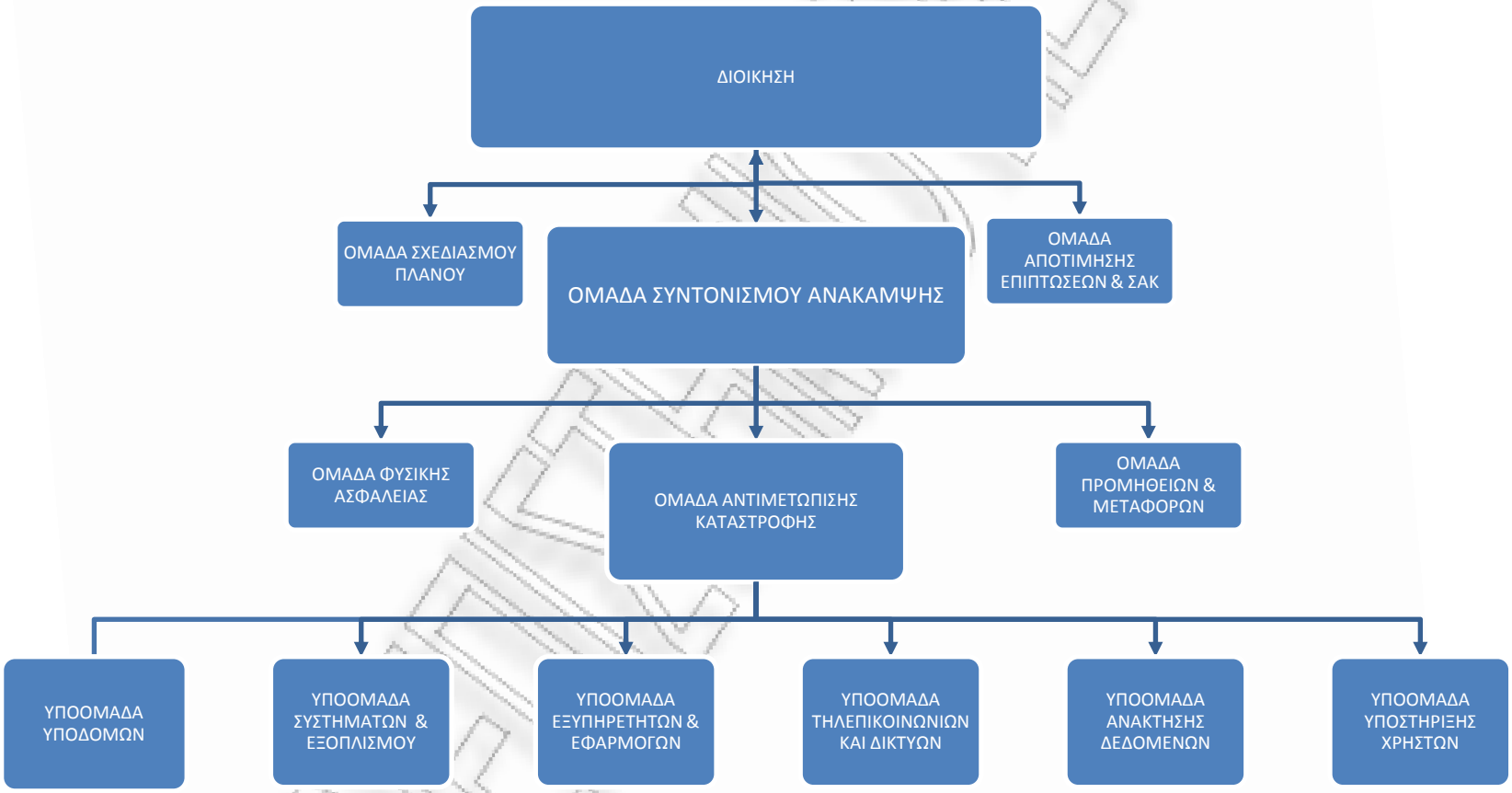
Ένα ΣΑΚ λόγω της κρισιμότητας που έχει για έναν οργανισμό θα πρέπει να γίνεται γνωστό και να εμπλέκει όλο το προσωπικό, με στόχο να το ευαισθητοποιήσει και να το εξοικειώσει με την εφαρμογή του, ώστε να εξαλειφθεί κάθε πιθανότητα πανικού ή διατάραξης της εργασιακής καθημερινότητας, όταν ενεργοποιηθεί.

Εντούτοις, πρωταρχικής σημασίας διαδικασία αποτελεί ο καθορισμός των ρόλων και των αρμοδιοτήτων των υπευθύνων ή ομάδων, οι οποίοι εμπλέκονται άμεσα στο σχεδιασμό και εφαρμογή ενός ΣΑΚ. Αυτές οι ομάδες θα επιφορτιστούν με την εκτέλεση του ΣΑΚ και για να καταστούν αποτελεσματικές θα πρέπει να τηρούν μια αυστηρά προκαθορισμένη ιεραρχία. Στη βιβλιογραφία προτείνονται διάφορες οργανωτικές παραλλαγές, οι οποίες απευθύνονται σε διαφορετικά μεγέθη οργανισμών και με διαφορετικό προσανατολισμό (διοικητικό, τεχνικό).

Ιδανικά, αυτή η ιεραρχία θα πρέπει να παραλληλίζεται με την υπάρχουσα ιεραρχική δομή του οργανισμού ώστε να χρησιμοποιούνται ήδη υπάρχουσες θέσεις εργασίας για αποφυγή επιπλέον κόστους λειτουργίας. Ο παράγοντας αυτός είναι πολύ σημαντικός για την περίπτωση μιας ΜΜΕ ή ενός ΜΜ οργανισμού, όπως εξετάζεται στην παρούσα εργασία. Παράλληλα, με τον τρόπο αυτό, επιτυγχάνεται υψηλή και ταχεία αφομοίωση των ρόλων αλλά και αποφυγή σύγχυσης κατά την εν παραλλήλω λειτουργία των δυο οργανογραμμάτων, σε περίπτωση ενεργοποίησης του ΣΑΚ.

Παρακάτω προτείνεται μια τέτοια ιεραρχική δομή με στόχο να έρχεται σε συμφωνία με ένα τυπικό οργανόγραμμα μιας ΜΜΕ ενώ παράλληλα να καλύπτει και τις κύριες λειτουργικές απαιτήσεις ενός ΣΑΚ.

i. Οργανόγραμμα



Σχήμα 16: *Οργανόγραμμα ανάκαμψης από καταστροφές*

ii. Υπεύθυνοι

Οι βασικοί ρόλοι οι οποίοι θα πρέπει να καθορίζονται είναι:

- **Υπεύθυνος Συντονισμού (Υπεύθυνος ΣΑΚ):**

  Αναφέρεται απευθείας στη Διοίκηση. Φέρει την κύρια ευθύνη για το σχεδιασμό, λειτουργία και συντήρηση του ΣΑΚ και δρα ως ενορχηστρωτής όλων των εμπλεκομένων μερών. Μπορεί να ηγείται τόσο της Ομάδας Διαχείρισης ΣΑΚ όσο και της Ομάδας Αντιμετώπισης Καταστροφής.

- **Υπεύθυνος Επικοινωνίας:**

  Είναι μέλος της Ομάδας Διαχείρισης ΣΑΚ και υπεύθυνος για την επικοινωνιακή διαχείριση της καταστροφής. Αναλαμβάνει να ενημερώσει όλους τους άμεσα εμπλεκόμενους (πελάτες, προμηθευτές, προσωπικό, διοίκηση) έγκαιρα και έγκυρα, προλαμβάνοντας φαινόμενα πανικού και διασφαλίζοντας την υπόληψη του οργανισμού.

- **Υπεύθυνος Επικαιροποίησης:**

  Είναι υπεύθυνος για την επικαιροποίηση του ΣΑΚ και την αναθεώρησή του, όποτε και αν απαιτείται. Αναλαμβάνει μετά από κάθε αλλαγή είτε στις λειτουργίες/υπηρεσίες του οργανισμού είτε στα ΠΣ να εξετάσει κατά πόσο απαιτείται προσαρμογή του ΣΑΚ.

- **Υπεύθυνος Νομικών ενεργειών:**

  Είναι υπεύθυνος για τη νομική κάλυψη του οργανισμού. που αφορούν στην εκδήλωση κάποιας καταστροφής. Φέρει την ευθύνη να εντοπίσει όλες τις νομικές υποχρεώσεις στις οποίες υποχρεούται να συμμορφώνεται ο οργανισμός. κυρίως όσον αφορά τα προσβεβλημένα δεδομένα σε σχέση με τρίτους (πελάτες, προσωπικό). Παράλληλα επικουρεί στην δημιουργία ρητρών στις συμβάσεις προμήθειας υπηρεσιών/υλικών με τρόπο που να εξυπηρετεί τις ανάγκες του ΣΑΚ. Κινεί άμεσα όλες τις απαραίτητες διαδικασίες, εφόσον προβλέπονται, για την αποζημίωση του οργανισμού από ασφαλιστήρια συμβόλαια κινδύνου ή ρήτρες (SLAs).

- **Υπεύθυνος Εκπαίδευσης():**

  Φέρει την ευθύνη για την επαρκή και συνεχή εκπαίδευση όλων των εμπλεκομένων μερών. Εισηγείται τις εκπαιδευτικές ανάγκες του προσωπικού, προγραμματίζει και σχεδιάζει τις απαραίτητες ασκήσεις που απαιτούνται για τη δοκιμή του ΣΑΚ.

iii. Ομάδες

Παράλληλα απαραίτητος κρίνεται ο καθορισμός των εξής ομάδων:

- **Ομάδα Διαχείρισης ΣΑΚ**

  Είναι η ομάδα που φέρει την ευθύνη για την πλήρη διαχείριση και εφαρμογή του ΣΑΚ και αναφέρεται στη Διοίκηση του Οργανισμού. Αποτελείται από το σύνολο των Υπευθύνων, όπως περιγράφονται παραπάνω, με επικεφαλής τον Υπεύθυνο Συντονισμού. Ανάλογα με την χρονική περίοδο σε σχέση με την εκτέλεση ενός ΣΑΚ δηλαδή πριν, κατά τη διάρκεια, η μετά την ολοκλήρωσή του η Ομάδα αυτή μπορεί να αναλάβει διαφορετικό ρόλο ως:

  - **(Ομάδα Σχεδιασμού Πλάνου)**

    Η οποία φέρει την ευθύνη για το σχεδιασμό, τη βελτίωση και τον έλεγχο της λειτουργικότητας του ΣΑΚ. Το έργο της αφορά κυρίως στον προπαρασκευαστικό τομέα και πριν την εμφάνιση κάποιας καταστροφής. Μπορεί να περιλαμβάνει επιπρόσθετα και έμπειρα μέλη από την Ομάδα Αντιμετώπισης Καταστροφής.

  - **(Ομάδα Συντονισμού Ανάκαμψης)**

    Αναλαμβάνει δράση με την εμφάνιση και αναγνώριση κάποιου περιστατικού καταστροφής και είναι υπεύθυνη για το συντονισμό του ΣΑΚ. Αποφασίζει για την ενεργοποίηση ή μη του ΣΑΚ, την επιλογή της ακολουθούμενης στρατηγικής και τη λήψη εκτελεστικών αποφάσεων. Εισηγείται στη Διοίκηση για σημαντικά θέματα όπως η αναγκαιότητα μετάβασης σε εναλλακτικές εγκαταστάσεις και αναλαμβάνει την εν γένει επικοινωνία και αλληλεπίδραση με τρίτους.

  - **(Ομάδα Αποτίμησης Επιπτώσεων και Αποτελεσματικότητας ΣΑΚ)**

    Με την ολοκλήρωση του ΣΑΚ και την επιστροφή στο επίπεδο λειτουργικότητας πριν την καταστροφή, η ομάδα αυτή καλείται να αποτιμήσει τις επιπτώσεις και τις όποιες συνέπειες της καταστροφής. Αναλύει την αποτελεσματικότητα του ΣΑΚ και προτείνει τυχόν διορθωτικές ενέργειες που απαιτούνται για την βελτίωσή του.

- **Ομάδα Αντιμετώπισης Καταστροφής**

  Η ομάδα αυτή είναι υπεύθυνη για το γενικό συντονισμό και την εφαρμογή ενεργειών για την αποκατάσταση/ανάκαμψη κυρίως σε τεχνικό/τεχνολογικό επίπεδο είτε στις τοπικές είτε σε εναλλακτικές εγκαταστάσεις. Αναλαμβάνει δράση με την απόφαση ενεργοποίησης του ΣΑΚ και αναφέρεται στον Υπεύθυνο Συντονισμού. Ανάλογα με την πολυπλοκότητα των Πληροφοριακών Συστημάτων η ομάδα αυτή μπορεί να διαχωρίζεται στις παρακάτω υποομάδες:

  - **Υποομάδα Υποδομών**

    Είναι υπεύθυνη για την αποκατάσταση των απαραίτητων υποδομών για τη λειτουργία των ΠΣ. Οι υποδομές αυτές μπορεί να αφορούν εξοπλισμό γραφείου, ισχυρά και ασθενή ρεύματα, δομημένη καλωδίωση.

  - **Υποομάδα Συστημάτων και Περιφερειακών**

    Είναι υπεύθυνη για την αποκατάσταση της λειτουργίας των συστημάτων των χρηστών και του λοιπού περιφερειακού εξοπλισμού (PC, printers).

  - **Υποομάδα Εξυπηρετητών και Εφαρμογών**

    Είναι υπεύθυνη για την αποκατάσταση της λειτουργίας των εξυπηρετητών καθώς και των κρίσιμων εφαρμογών του οργανισμού (OS, services).

  - **Υποομάδα Τηλεπικοινωνιών και δικτύων**

    Είναι υπεύθυνη για την αποκατάσταση των τηλεπικοινωνιακών και δικτυακών υπηρεσιών (LAN, WAN, WWW, Tphone).

  - **Υποομάδα Ανάκτησης δεδομένων**

    Είναι υπεύθυνη για τη διενέργεια δράσεων και για το συντονισμό ενεργειών για την ανάκτηση-αποκατάσταση όλων των δεδομένων (Backups, DBs).

  - **Υποομάδα Ενημέρωσης και υποστήριξης χρηστών**

    Η ομάδα αυτή αποτελεί τον επικοινωνιακό δίαυλο της Ομάδας Αντιμετώπισης, τόσο μεταξύ των Υποομάδων όσο και προς τις ιεραρχικά ανώτερες ομάδες. Αναλαμβάνει να ενημερώσει τους χρήστες του οργανισμού για την κατάσταση των ΠΣ και με σαφήνεια να τους υποδείξει τις αλλαγές στον τρόπο χειρισμού που απαιτούνται μέχρι την πλήρη επαναφορά σε κανονική λειτουργία. Παράλληλα αναλαμβάνει να υποδείξει εναλλακτικούς τρόπους με τους οποίους μπορούν να καλύψουν τις ανάγκες τους.

- **Ομάδα Προμηθειών και Μεταφοράς**

Η ομάδα αυτή είναι υπεύθυνη για την εξασφάλιση επαρκών προμηθειών (υλικών, εξοπλισμού, αναλωσίμων) που μπορεί να απαιτηθούν κατά την ανάκαμψη. Ταυτόχρονα είναι υπεύθυνη για την έγκαιρη μεταφορά τους, είτε στις κύριες είτε στις εναλλακτικές εγκαταστάσεις. Αναφέρεται στην Ομάδα Συντονισμού.

- **Ομάδα Φυσικής ασφάλειας**

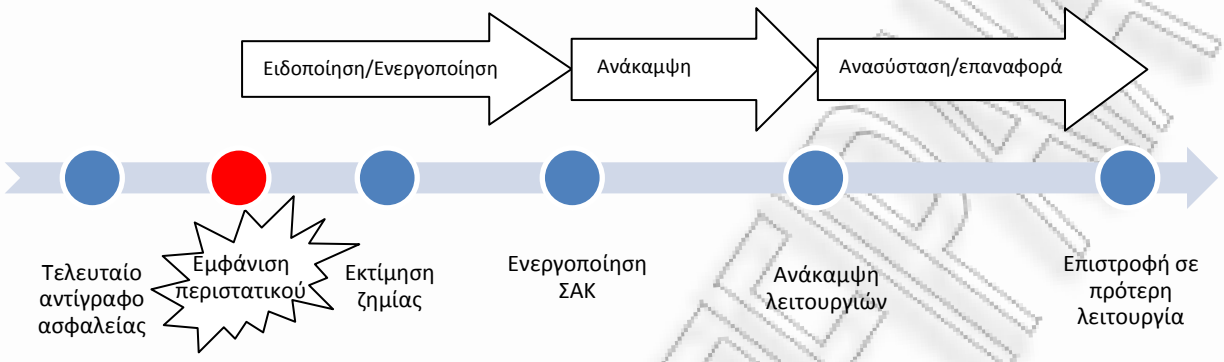
  Η ομάδα αυτή είναι υπεύθυνη για τη φυσική ασφάλεια των εγκαταστάσεων κατά την εκτέλεση του ΣΑΚ. Ασφαλίζει τις πληγείσες εγκαταστάσεις αλλά και τις εναλλακτικές από παράνομη πρόσβαση, για όσο διαρκεί η διαδικασία ανάκαμψης, διατηρώντας λίστα εγκεκριμένων προσώπων. Αναφέρεται στην Ομάδα Συντονισμού.

4.5.5 Ενέργειες αντιμετώπισης

Με την εμφάνιση ενός περιστατικού καταστροφής μέχρι και την οριστική παύση του θα πρέπει το ΣΑΚ να καθορίζει διαδικασίες που συνοδεύουν τον κύκλο ζωής του και μπορεί να περιλαμβάνει [45]:

-την ενημέρωση των απαραίτητων μερών
-την αναγνώριση του περιστατικού
-την ενεργοποίηση του ΣΑΚ
-την ολοκλήρωση του ΣΑΚ
-την παύση του περιστατικού
-την επιστροφή σε κανονική λειτουργία

Οι διαδικασίες αυτές ταξινομούνται σε τρεις διαφορετικές κατηγορίες-φάσεις: της ειδοποίησης/ενεργοποίησης, της ανάκαμψης και της ανασύστασης/επαναφοράς. Στο παρακάτω σχήμα (Σχήμα 17) φαίνεται ο χρονικός συσχετισμός αυτών των φάσεων, συναρτήσει του κύκλου ζωής ενός περιστατικού.



Σχήμα 17: *Κύκλος ζωής περιστατικού ανάκαμψης*

Στις παρακάτω παραγράφους θα επιχειρηθεί να περιγραφούν οι φάσεις αυτές καθώς και οι απαιτήσεις της κάθε μιας.

i. Ειδοποίηση/ενεργοποίηση

Είναι η φάση που καλύπτει χρονικά την περίοδο από την εκδήλωση ενός καταστροφικού συμβάντος μέχρι την αναγνώρισή του και την ενεργοποίηση του ΣΑΚ.

Αυτή αποτελεί την αρχική φάση, όπου η έγκαιρη ανίχνευση και ειδοποίηση των υπευθύνων για την ανάκαμψη είναι ικανή να επηρεάσει καθοριστικά τις συνέπειες ενός περιστατικού. Η αναγνώριση της καταστροφής και των συνεπειών της, δίνουν τις κατάλληλες πληροφορίες ώστε να γίνει σωστή αναγνώριση και ορθή λήψη της απόφασης περί της ενεργοποίησης ή μη και σε ποιο βαθμό του ΣΑΚ. Πρέπει να τονιστεί ότι η εσφαλμένη ενεργοποίηση του ΣΑΚ μπορεί να προκαλέσει περισσότερη αναστάτωση από το ίδιο το περιστατικό και να προκαλέσει περιττό κόστος. Για το λόγο αυτό μια τέτοια απόφαση, ιδίως στην περίπτωση που απαιτηθεί χρήση-μετακόμιση σε εναλλακτικές εγκαταστάσεις θα πρέπει συνήθως να λάβει την έγκριση της Διοικούσας Αρχής.

Με την ενεργοποίηση του ΣΑΚ πρέπει να ενημερωθούν άμεσα όλα τα εμπλεκόμενα πρόσωπα και να ληφθεί μέριμνα για την επικοινωνιακή διαχείριση του περιστατικού ιδίως αν επηρεάζει τις σχέσεις-υποχρεώσεις του οργανισμού έναντι τρίτων.

ii. Ανάκαμψη

Η φάση αυτή καλύπτει την περίοδο από την ενεργοποίηση του ΣΑΚ μέχρι την ανάκαμψη των κρίσιμων λειτουργιών του οργανισμού, στο ελάχιστο απαιτούμενο επίπεδο, σύμφωνα με τα όσα προβλέπονται στο ΣΑΚ.

Αφού ληφθεί η απόφαση ενεργοποίησης του ΣΑΚ και ενημερωθούν οι εμπλεκόμενοι, άμεση υποχρέωσή τους αποτελεί η συγκέντρωσή τους σε προκαθορισμένο χώρο. Εκεί αφού αναλυθούν και εξετασθούν οι τυχόν ειδικότερες απαιτήσεις, επικυρώνονται και εκκινούνται οι διαδικασίες ανάκαμψης που προβλέπονται από το ΣΑΚ. Κρίσιμος παράγοντας αποτελεί η έγκαιρη και επαρκής προμήθεια και μεταφορά όλων των απαιτούμενων υλικών που απαιτούνται για την ανάκαμψη από την έναρξή της μέχρι και την ολοκλήρωσή της. Θα πρέπει παράλληλα, καθ' όλη τη διάρκεια των εργασιών ανάκαμψης, είτε στις τοπικές είτε στις εναλλακτικές εγκαταστάσεις, να διασφαλίζεται ο έλεγχος της πρόσβασης μόνο σε εξουσιοδοτημένο προσωπικό.

Έχοντας εξασφαλίσει ασφαλή πρόσβαση στις εγκαταστάσεις και επάρκεια πόρων, το ειδικό βάρος μεταφέρεται στο συντονισμό και την εφαρμογή των επιλεχθέντων στρατηγικών ανάκαμψης. Κατά τη εφαρμογή των στρατηγικών αυτών γίνεται προτεραιοποίηση στην επιλογή των προς ανάκτηση πόρων σύμφωνα με τα αποτελέσματα της ανάλυσης επιπτώσεων και το επιθυμητό RTO (βλέπε §4.2).

Για κάθε ΠΣ εφαρμόζεται το αντίστοιχο ISCP, το οποίο περιέχει αναλυτικά οδηγίες για την διαδικασία ανάκτησής του. Με την ολοκλήρωση της ανάκτησης κάθε ΠΣ γίνεται έλεγχος για την καλή λειτουργία του. Σε περίπτωση που το λειτουργικό επίπεδο κρίνεται ανεκτό και ικανοποιούνται οι επιθυμητοί στόχοι (RPO) το σύστημα δίδεται προς χρήση. Εφόσον το λειτουργικό επίπεδο δεν κριθεί ανεκτό αναλύονται οι τυχόν ειδικές απαιτήσεις, οι οποίες είναι εφικτό να ικανοποιηθούν άμεσα, και επαναλαμβάνεται η διαδικασία ανάκτησής του. Σε περίπτωση που κρίνεται μη εφικτό το επιθυμητό λειτουργικό επίπεδο, γίνεται διαβίβαση

της διαπίστωσης σε ανώτερο ιεραρχικό επίπεδο και επιχειρείται επιλογή διαφορετικής στρατηγικής αντιμετώπισης (βλέπε §4.4).

Έχοντας ολοκληρώσει την ανάκτηση των απαιτούμενων ΠΣ και εξασφαλίζοντας την απρόσκοπτη εξυπηρέτηση των απαιτούμενων λειτουργιών-υπηρεσιών του οργανισμού καταγράφονται όλες οι παρατηρήσεις κατά τη διάρκεια της ανάκαμψης. Στις παρατηρήσεις αυτές μπορεί να περιλαμβάνονται ελλείψεις που παρατηρήθηκαν, προβλήματα που προέκυψαν και προτάσεις βελτίωσης του ΣΑΚ.

iii. Ανασύσταση- επαναφορά

Η τρίτη και τελευταία φάση αφορά την περίοδο από την ανάκαμψη των λειτουργιών στο ελάχιστο απαιτούμενο βαθμό, είτε στις ίδιες είτε σε εναλλακτικές εγκαταστάσεις, μέχρι την πλήρη επαναφορά τους στην πρότερη κατάσταση πλήρους λειτουργίας.

Στη φάση αυτή θα πρέπει να πραγματοποιηθούν οι απαραίτητες ενέργειες για την αποκατάσταση των πληγέντων κυρίως εγκαταστάσεων και των συστατικών στοιχείων των ΠΣ και να ελεγχθεί η ορθή λειτουργία τους. Με την επικύρωση της ορθότητας τους, θα πρέπει να ακολουθήσει η επαναφορά των ΠΣ στις λειτουργικές πλέον κύριες εγκαταστάσεις ώστε να επιστρέψουν στην κατάσταση που βρίσκονταν πριν το καταστροφικό περιστατικό. Εν συνεχεία ακολουθεί η ανασύσταση της ετοιμότητας του ΣΑΚ με την αναπλήρωση των προμηθειών-εξοπλισμού ανάκτησης που χρησιμοποιήθηκε, τη προετοιμασία των εναλλακτικών εγκαταστάσεων και διασφαλίζοντας τις εν γένει απαιτήσεις για την αντιμετώπιση μιας νέας καταστροφής.

Αφού συλλεχθούν όλες οι καταγεγραμμένες παρατηρήσεις από τα εμπλεκόμενα μέρη, κατά τις προηγούμενες φάσεις, ακολουθεί η αποτίμηση του περιστατικού και η αξιολόγηση της αποτελεσματικότητας του ΣΑΚ. Εφόσον διαπιστωθούν ελλείψεις, απαιτείται ο επανασχεδιασμός του ΣΑΚ και η λήψη όλων των απαραίτητων διορθωτικών μέτρων, ενώ καταγράφονται οι τυχόν πρόσθετες εκπαιδευτικές ανάγκες που απαιτούνται για την αποτελεσματική εφαρμογή του σχεδίου. Παράλληλα, λαμβάνονται αποφάσεις για νομικές ενέργειες σχετικά με προβλεπόμενες αποζημιώσεις και ρήτρες, βάσει συμβολαίων (SLA), και ενημερώνονται όλοι οι εμπλεκόμενοι για τη λήξη της διαδικασίας ανάκαμψης και τις ενδεχόμενες εκκρεμείς υποχρεώσεις τους.

Η φάση αυτή ολοκληρώνεται με την πλήρη καταγραφή του περιστατικού και την επικαιροποίηση του ΣΑΚ με τις τυχόν προσαρμογές που απαιτούνται. Πλέον μπορεί να θεωρηθεί ότι πληρούνται όλες οι προϋποθέσεις για τον τερματισμό του ΣΑΚ.

4.5.6 Αρχεία-Έντυπα

Το σχέδιο δράσης του ΣΑΚ ολοκληρώνεται με τη προσθήκη όλων των απαραίτητων αρχείων ή εντύπων τα οποία συνεπικουρούν την διαδικασία ανάκαμψης και τις υποχρεώσεις κάθε εμπλεκόμενου μέρους. Αυτά μπορεί να αφορούν:

- **Στοιχεία επικοινωνίας**: όλα τα απαραίτητα στοιχεία επικοινωνίας, που αφορούν τα εμπλεκόμενα πρόσωπα και περιλαμβάνει κυρίως υπεύθυνους, πελάτες, προμηθευτές, τεχνικούς-συντηρητές, παρόχους υπηρεσιών (ΔΕΗ, Τηλεπικοινωνίες) καθώς και υπηρεσίες έκτακτης ανάγκης (αστυνομία, πυροσβεστική, ΕΚΑΒ)
- **Επιμέρους σχέδια ISCP**: τα οποία περιλαμβάνουν οδηγίες αποκατάστασης για τα επιμέρους ΠΣ και μπορεί να περιέχουν:
    - Οδηγίες χρήσης εξοπλισμού
    - Άδειες χρήσης λογισμικού
    - Τεχνικά εγχειρίδια
    - Διαγράμματα δικτύου και διασυνδέσεων
- **Κωδικοί πρόσβασης**: περιέχονται όλοι οι απαραίτητοι κωδικοί διαχειριστή, οι οποίοι απαιτούνται. Το συγκεκριμένο έντυπο θα πρέπει να είναι διαβαθμισμένο και να μην είναι προσβάσιμο σε όλους τους εμπλεκόμενους αλλά να τηρείται από τον Υπεύθυνο Συντονισμού.
- **Διαγράμματα ροής εργασιών**: αφορά σε διαγράμματα τα οποία με σαφή και σύντομο τρόπο παρουσιάζουν τη ροή ενεργειών που θα πρέπει να ακολουθείται.
- **Συμβόλαια ασφάλισης**: σε περίπτωση που υπάρχουν συμβόλαια ασφάλισης για εξοπλισμό ή άλλους πόρους θα πρέπει να συμπεριλαμβάνονται.
- **Συμβόλαια εγγυημένου επιπέδου υπηρεσιών (SLAs)**: σε περίπτωση που υπάρχουν συμβόλαια που περιέχουν ρήτρες για συγκεκριμένο επίπεδο παροχής υπηρεσιών θα πρέπει να συμπεριλαμβάνονται.
- **Ανάλυση επιπτώσεων (BIA)**: θα πρέπει να περιέχεται έγγραφο με τα αποτελέσματα της ανάλυσης επιπτώσεων.

- **Προτεραιότητα ανάκτησης πόρων**: θα πρέπει να περιέχεται λίστα με την προτεραιότητα ανάκτησης πόρων ως απόρροια της ανάλυσης επιπτώσεων.
- **Ρόλοι και Αρμοδιότητες**: θα πρέπει να περιγράφονται με σαφήνεια οι ρόλοι και οι αρμοδιότητες των εμπλεκομένων, τόσο πριν την καταστροφή όσο και μετά την εκδήλωσή της.
- **Λίστα απαραίτητου εξοπλισμού ανάκαμψης**: όπου περιέχονται όλοι οι απαραίτητοι πόροι και υλικά που κρίνονται απαραίτητοι για τη διαδικασία της ανάκαμψης.
- **Κοστολόγια υπηρεσιών και πόρων**: σε περίπτωση που επιλεχθεί να μην χρησιμοποιηθούν προμήθειες και συμβόλαια υποστήριξης προληπτικού χαρακτήρα θα πρέπει να υπάρχει ενδεικτική κοστολόγηση ώστε να έχει διασφαλιστεί κατάλληλο προϋπολογισθέν ποσό για την κάλυψη αναγκών σε περίπτωση καταστροφής.
- **Στοιχεία εναλλακτικών εγκαταστάσεων**: περιλαμβάνει όλα τα απαραίτητα στοιχεία που αφορούν στις εναλλακτικές εγκαταστάσεις (στοιχεία επικοινωνίας, διαγράμματα, κα)
- **Έντυπα ελέγχου ορθής λειτουργίας**: αφορούν φόρμες-λίστες με σημεία ελέγχου για τον έλεγχο καλής λειτουργίας των ΠΣ που ανακτήθηκαν.
- **Έντυπα καταγραφής περιστατικού**: αφορούν φόρμες-λίστες σχετικά με την καταγραφή ενός περιστατικού καθώς και σχετικών παρατηρήσεων.

4.6 Δοκιμές και Εκπαίδευση

Αφού πλέον έχει υλοποιηθεί το ΣΑΚ απομένει να εξασφαλίσουμε ότι αποτελεί μια λύση η οποία είναι λειτουργική και μπορεί να ανταποκριθεί με επιτυχία σε περίπτωση καταστροφικού συμβάντος. Για να επιτευχθεί αυτό απαιτείται η επαρκής δοκιμή του Σχεδίου αλλά και η εκπαίδευση των εμπλεκομένων μερών ώστε να εξασφαλιστεί η ετοιμότητά τους. Η διεξαγωγή στοχευμένων ασκήσεων είναι το εργαλείο που μπορεί να αναδείξει τους προβληματικούς τομείς των ακολουθούμενων στρατηγικών και να βελτιώσει τη διαλειτουργικότητα μεταξύ των διεργασιών, των τεχνολογιών και των ανθρώπων όπως αυτή ορίζεται από το ΣΑΚ.

Ο NIST με την οδηγία 800-84 [54] επιχειρεί να καλύψει όλα όσα απαιτούνται για τη σχεδίαση και διεξαγωγή αποτελεσματικών προγραμμάτων δοκιμών, εκπαίδευσης και ασκήσεων σχετικά με θέματα Πληροφοριακών Συστημάτων. Τις ασκήσεις αυτές τις ταξινομεί σε δύο κατηγορίες:

-**Ασκήσεις επί χάρτου**: είναι ασκήσεις οι οποίες λαμβάνουν χώρα με τη μορφή συζήτησης και της λεκτικής προσομοίωσης. Αφού περιγραφεί το σενάριο της άσκησης, ακολουθεί συζήτηση και μέσω ερωταπαντήσεων επιχειρείται να εξετασθεί για κάθε εμπλεκόμενο μέλος ο ρόλος, οι υπευθυνότητες, ο τρόπος λειτουργίας και λήψης αποφάσεων. Οι ασκήσεις αυτές δεν έχουν στόχο να εξετάσουν τη λειτουργικότητα των τεχνολογικών μέσων τόσο όσο τις εφαρμοζόμενες διαδικασίες και τον ανθρώπινο παράγοντα.

-**Ασκήσεις προσομοίωσης**: Σε αυτές τις ασκήσεις εξετάζεται η λειτουργικότητα του σχεδίου και η ετοιμότητα των εμπλεκομένων μερών μέσα από την προσομοίωση πραγματικών συνθηκών. Ο τύπος αυτών των ασκήσεων δίνει τη δυνατότητα να αξιολογηθούν τόσο ο ανθρώπινος παράγοντας και οι εφαρμοζόμενες διαδικασίες όσο και η αποτελεσματικότητα των τεχνολογιών ανάκαμψης. Μέσα από τη δημιουργία σεναρίων και την προσομοίωση συνθηκών, όσο το δυνατόν πιο κοντά σε αυτά ενός πραγματικού συμβάντος, επιτυγχάνεται μια πληρέστερη εικόνα της αποτελεσματικότητας του ΣΑΚ.

Ανάλογα με το πεδίο στο οποίο αναφέρονται και το εύρος που καλύπτουν οι ασκήσεις αυτές μπορεί να αποτελούν [51]:

- Ασκήσεις τεχνικής ανάκαμψης, όπου επικεντρώνονται στη δοκιμή των διαδικασιών των σχετικών με την τεχνική ανάκαμψη των συστημάτων.

- Ασκήσεις ανάκαμψης σε εναλλακτικό χώρο, όπου σαν κύριο χαρακτηριστικό έχουν τον έλεγχο της λειτουργικότητας του ΣΑΚ όσον αφορά την αξιοποίηση των εναλλακτικών εγκαταστάσεων και το βαθμό ετοιμότητας αυτών.

- Ασκήσεις ελέγχου παρόχων εγκαταστάσεων και υπηρεσιών, με κύριο αντικείμενο ελέγχου το επίπεδο παροχής υπηρεσιών ανάκτησης από τρίτους και της τήρησης κατάλληλων συμβολαίων (SLAs).

- Ασκήσεις ανάκαμψης πλήρους κλίμακας, οι οποίες αποτελούν το πλέον ολοκληρωμένο μέσο αξιολόγησης ενός ΣΑΚ αφού εξετάζουν το σενάριο της ανάκτησης των ΠΣ μετά από πλήρη καταστροφή.

Στον Πίνακα 4 παρουσιάζεται μια συνοπτική σύγκριση των χαρακτηριστικών που συγκεντρώνει η κάθε κατηγορία ασκήσεων.

	Χρόνος	Κόστος	Εγκυρότητα	Αντικείμενο Ελέγχου		
				Άνθρωποι	Διαδικασίες	Τεχνολογίες
Ασκήσεις επί χάρτου	+	+	-	+	+	-
Ασκήσεις προσομοίωσης	-	-	+	+	+	+

Πίνακας 4: *Σύγκριση δοκιμαστικών ασκήσεων*

Κατά την επιλογή και τον καθορισμό της περιοδικότητας κάθε άσκησης θα πρέπει να λαμβάνονται υπόψη παράγοντες όπως το κόστος, οι εμπλεκόμενοι πόροι, η προηγούμενη εμπειρία διεξαγωγής ασκήσεων και η εκπαίδευση των εμπλεκομένων μερών. Σε περίπτωση που υπάρχουν περιορισμοί στα παραπάνω προτείνεται αρχικά η διεξαγωγή απλών ασκήσεων με σταδιακή αύξηση του εύρους αναφοράς και της πολυπλοκότητας τους [55].

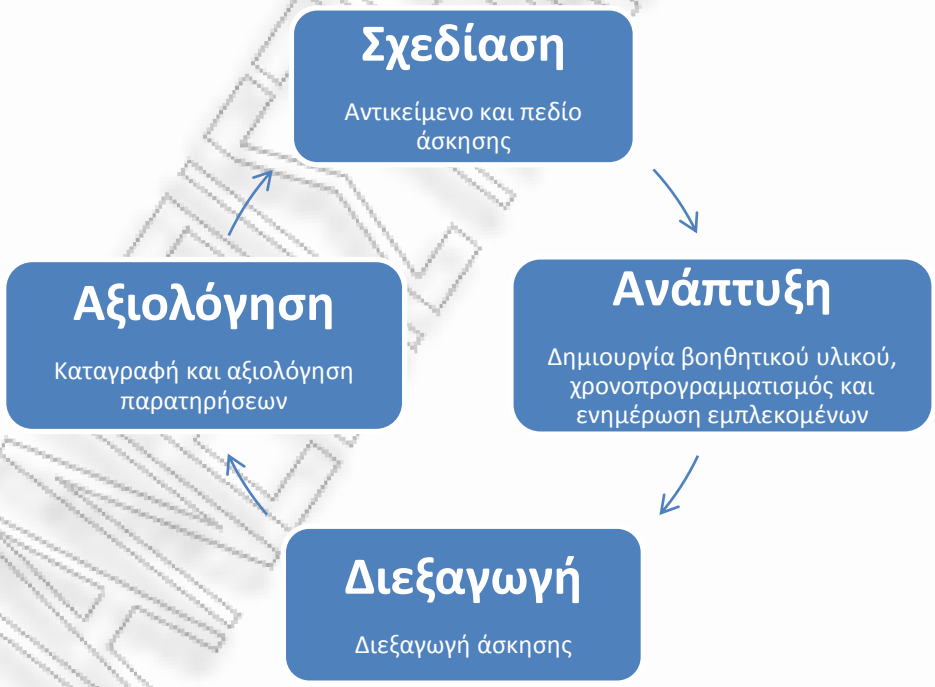
Για τη σχεδίαση και υλοποίηση των ασκήσεων ανάκαμψης προτείνεται από τον NIST [54] η εφαρμογή μιας μεθοδολογίας τεσσάρων φάσεων η οποία αποτελείται από:

Σχεδίαση: Στη φάση αυτή καθορίζεται το αντικείμενο και το πεδίο της άσκησης. Σύμφωνα με το καθορισμό των στόχων της άσκησης επιλέγονται τα πρόσωπα, οι διαδικασίες και οι τεχνολογίες που θα εξετασθούν.

Ανάπτυξη: Επόμενο βήμα αποτελεί η δημιουργία όλου του βοηθητικού υλικού που απαιτείται για τη διεξαγωγή της άσκησης όπως παραδοχές πριν την εκτέλεση, οδηγίες κατά την εκτέλεση και έντυπα παρατηρήσεων και αξιολόγησης. Παράλληλα γίνεται όλη η απαραίτητη προετοιμασία-προγραμματισμός για τη διεξαγωγή της άσκησης όπως είναι ο χρονοπρογραμματισμός και η ενημέρωση των εμμέσως ή αμέσως εμπλεκομένων μερών.

Διεξαγωγή: Όταν πλέον διαμορφωθούν οι κατάλληλες συνθήκες μπορούμε να περάσουμε στη φάση της διεξαγωγής της άσκησης όπου εφαρμόζονται όσα έχουν προβλεφθεί από το ΣΑΚ στο εξεταζόμενο αντικείμενο.

Αξιολόγηση: Αυτή είναι η τελική φάση κατά την οποία αναλύεται και αξιολογείται η διεξαγωγή της άσκησης. Στόχος είναι η εύρεση και διόρθωση των ενδεχόμενων αδυναμιών τόσο του ΣΑΚ όσο και της ίδιας της μεθοδολογίας των ασκήσεων. Στο στάδιο αυτό εξάγονται οι ανάγκες βελτίωσης ή εκπαίδευσης των ανθρώπων, των διεργασιών και των τεχνολογιών.



Σχήμα 18: *Μεθοδολογία σχεδιασμού και υλοποίησης ασκήσεων κατά NIST*

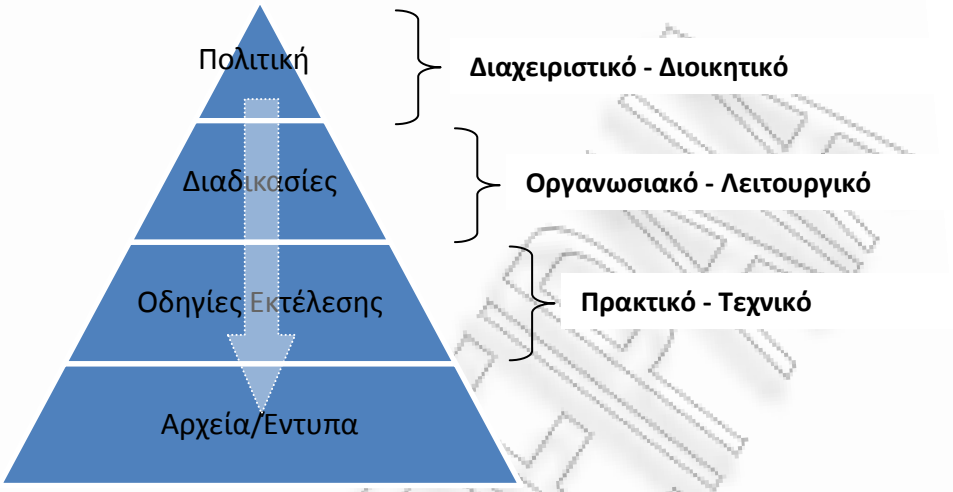
4.7 Συντήρηση και επικαιροποίηση

Τελευταίο βήμα αποτελεί η εξασφάλιση της συντήρησης και της επικαιροποίησης του ΣΑΚ. Καθώς μέσα σε ένα οργανισμό μπορεί να συντελούνται συνεχώς αλλαγές στις λειτουργίες ή τις υπηρεσίες του θα πρέπει να υπάρχει μέριμνα ώστε και το ΣΑΚ να προσαρμόζεται αποτελεσματικά στις νέες συνθήκες. Επομένως θα πρέπει να καθοριστεί η περιοδικότητα με την οποία θα επαναλαμβάνεται/επικαιροποιείται εξολοκλήρου η παραπάνω ακολουθία των επτά βημάτων για τη σχεδίαση του ΣΑΚ. Παράλληλα, αυτή η ευθύνη θα πρέπει να περιγράφεται και να αποδίδεται ως ρόλος-αρμοδιότητα ώστε να εξασφαλιστεί η συντήρηση-επικαιροποίηση του σχεδίου, πέρα από την προκαθορισμένη περιοδικότητα, και σε κάθε αλλαγή που αφορά [51]:

- προσωπικό
- στοιχεία επικοινωνίας εμπλεκομένων μερών
- την επιχειρησιακή στρατηγική
- εγκαταστάσεις, πόρους, τεχνολογίες
- στο νομικό πλαίσιο που διέπει τον οργανισμό
- στους προμηθευτές, συνεργάτες
- σε διαδικασίες (νέες ή παλιές)
- εξωτερικές συνθήκες που επηρεάζουν τους κινδύνους του οργανισμού (οικονομικούς, λειτουργικούς ή άλλους)

4.8 Σύνοψη συστατικών ολοκλήρωσης ΣΑΚ

Συνοψίζοντας όλα όσα παρουσιάστηκαν παραπάνω μπορούμε να πούμε ότι ένα ολοκληρωμένο Σχέδιο Ανάκαμψης από Καταστροφές θα πρέπει να δομείται ιεραρχικά σύμφωνα με το Σχήμα 19.



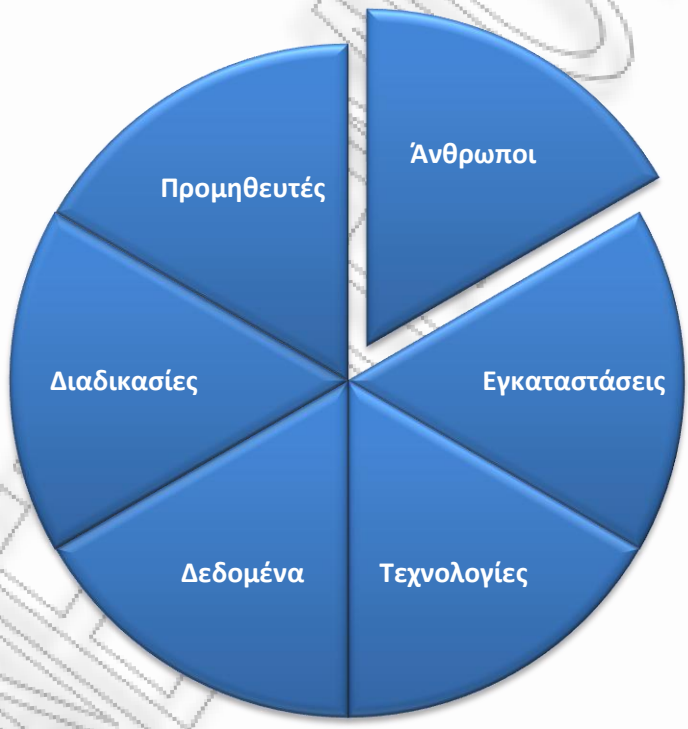
Σχήμα 19: *Συστατικά Σχεδίου Ανάκαμψης από Καταστροφές*

Αφού αποφασιστεί η ακολουθούμενη πολιτική αντιμετώπισης καταστροφών από τον οργανισμό, σε διαχειριστικό-διοικητικό επίπεδο, αυτή σταδιακά αναπτύσσεται και ενσωματώνεται, οργανωτικά και λειτουργικά, στον οργανισμό μέσω του καθορισμού σχετικών διαδικασιών. Αυτές με τη σειρά τους εξειδικεύονται περισσότερο, μέσω της καταγραφής οδηγιών για την εκτέλεσης του ΣΑΚ, ώστε να ανταποκρίνονται και σε πρακτικό – τεχνικό επίπεδο. Τέλος το Σχέδιο συμπληρώνεται από όλα τα απαραίτητα έντυπα και αρχεία.

5 Σύγχρονες τάσεις και μέτρα ανάκαμψης

5.1 Γενικά

Σε αυτό το κεφάλαιο παρατίθενται τα επικρατέστερα μέτρα τα οποία μπορεί να υιοθετήσει ένας οργανισμός προκειμένου να αντιμετωπίσει τις καταστροφές που πλήττουν τα Πληροφοριακά του Συστήματα. Τα μέτρα αυτά συνδυαζόμενα μεταξύ τους μπορούν να διαμορφώσουν τη στρατηγική αντιμετώπισης είτε για κάθε ΠΣ ξεχωριστά είτε να αποτελέσουν μια ολοκληρωμένη στρατηγική για το σύνολο των ΠΣ του οργανισμού εν όλω. Προκειμένου να εξετασθούν τα μέτρα αυτά απαιτείται αρχικά να αναλυθούν τα βασικά συστατικά στοιχεία που αποτελούν ένα τυπικό ΠΣ (Σχήμα 20) και στη συνέχεια να εξετασθούν τα διαθέσιμα μέτρα για κάθε ένα από αυτά.



Σχήμα 20: *Συστατικά στοιχεία Πληροφοριακών Συστημάτων*

Τα βασικά συστατικά ενός ΠΣ, όπως αυτά περιγράφονται και από τον ISO27031 [48] [56], συνοψίζονται στα εξής:

- **Άνθρωποι:** όλοι όσοι εμπλέκονται στη λειτουργία του ΠΣ από το επίπεδο του απλού χρήστη έως και του εξειδικευμένου επαγγελματία ο οποίος είναι υπεύθυνος για τη διαχείριση και λειτουργία του ΠΣ.
- **Εγκαταστάσεις:** οι εγκαταστάσεις στις οποίες φιλοξενούνται τα ΠΣ είτε είναι οι κύριες είτε είναι οι εναλλακτικές
- **Τεχνολογίες:** οι εφαρμοζόμενες τεχνολογίες οι οποίες αφορούν στο εξοπλισμό και τα λειτουργικά στοιχεία του ΠΣ. Αυτές μπορεί να περιλαμβάνουν το σύνολο του υλικού και λογισμικού από το οποίο αποτελείται το ΠΣ.
- **Δεδομένα:** όλα τα δεδομένα που είτε καλείται να επεξεργαστεί το ΠΣ είτε αποτελούν παράγωγο αυτής της επεξεργασίας.
- **Διαδικασίες:** όλες οι διαδικασίες-διεργασίες που αφορούν στο ΠΣ και μπορεί να σχετίζονται με τη χρήση, διαχείριση, παραμετροποίηση και αποσφαλμάτωσή τους.
- **Προμηθευτές:** όλοι οι προμηθευτές που σχετίζονται είτε με τον εξοπλισμό είτε με τις παρεχόμενες υπηρεσίες που αφορούν στο εκάστοτε ΠΣ.

Για κάθε ένα από αυτά τα συστατικά περιγράφονται τα διαθέσιμα μέτρα αντιμετώπισης και οι σύγχρονες τάσεις, όπως διαμορφώνονται σήμερα.

5.2 Άνθρωποι

Ίσως το βασικότερο συστατικό σε ένα ΠΣ αποτελούν οι άνθρωποι που εμπλέκονται σε αυτό είτε αποτελούν τους απλούς χρήστες είτε τους εξειδικευμένους διαχειριστές. Πρωταρχικό μέλημα κατά την ανάπτυξη μιας στρατηγικής αντιμετώπισης καταστροφών είναι ο καθορισμός και η απόδοση ρόλων και αρμοδιοτήτων σχετικά με την εφαρμογή του ΣΑΚ.

Στον κίνδυνο μιας ενδεχόμενης καταστροφής θα πρέπει να εξασφαλίζεται η επάρκεια των εμπλεκόμενων προσώπων τόσο αριθμητικά όσο και σε κατάρτιση ως προς την εκτέλεση των ενεργειών που απαιτούνται για την ανάκαμψη.

Οι ρόλοι-αρμοδιότητες που ορίζονται από το ΣΑΚ δε θα πρέπει να αναφέρονται σε μοναδικά πρόσωπα, καθώς υπάρχει ο κίνδυνος να μην είναι διαθέσιμα όταν θα κληθούν να αναλάβουν δράση. Η αριθμητική αυτή επάρκεια εξασφαλίζεται μέσω της αναπλήρωσης, μέσω της ανάθεσης σε τρίτους είτε μέσω της τηλεργασίας:

- **Αναπλήρωση (Redundancy):** η αναπλήρωση αφορά στον ορισμό αναπληρωτή για κάθε ρόλο που περιγράφεται στο ΣΑΚ και χρησιμοποιείται συνήθως προσωπικό του ίδιου του οργανισμού που μπορεί να του έχει αποδοθεί ήδη κάποιος ρόλος στο ΣΑΚ. Απαραίτητη προϋπόθεση αποτελεί να μην δημιουργείται πρόβλημα στην παράλληλη άσκηση των ρόλων. Αυτή η στρατηγική έχει συνήθως μικρότερο κόστος καθώς δεν αυξάνονται οι απαραίτητοι ανθρώπινοι πόροι, όμως απαιτείται η επαρκής εκπαίδευσή τους.

- **Ανάθεση σε τρίτους (Outsourcing):** όταν δεν υπάρχει επάρκεια προσωπικού ή η απαραίτητη τεχνογνωσία, τότε η ανάθεση ρόλου, ή η αναπλήρωσή του, μπορεί να πραγματοποιηθεί μέσω της ανάθεσης σε τρίτους. Η λύση αυτή, αν και συνήθως προσθέτει μεγαλύτερο κόστος, μπορεί να εξασφαλίσει την απαραίτητη τεχνογνωσία που απαιτείται για την επιτυχία του ΣΑΚ. Όταν επιλέγεται αυτή η στρατηγική θα πρέπει να δίνεται ιδιαίτερη σημασία στη διασφάλιση της εμπιστευτικότητας των δεδομένων, από τη πρόσβαση τρίτων, κατά τη διάρκεια της ανάκαμψης.

-**Τηλεργασία**: η δυνατότητα τηλεργασίας αποτελεί ένα σημαντικό μέτρο αντιμετώπισης της επάρκειας προσωπικού. Προσφέρει ευελιξία και διάθεση του απαραίτητου προσωπικού σε καλύτερους χρόνους, αλλά και ιδανικό τρόπο για την αντιμετώπιση καταστροφών, οι οποίες μπορεί να δυσχεραίνουν τη διαθεσιμότητα των ανθρώπων που εμπλέκονται στα ΠΣ, όπως μπορεί να συμβεί σε περίπτωση πανδημίας.

Όσον αφορά το σκέλος της κατάρτισης του προσωπικού αυτή εξασφαλίζεται μέσω κατάλληλης εκπαίδευσης, και μπορεί να αφορά σε:

-Βασική εκπαίδευση: η εκπαίδευση αυτή αφορά σε όλο το προσωπικό και βασικό στόχο έχει να κοινοποιήσει και να κάνει κατανοητή την πολιτική που έχει επιλέξει να ακολουθήσει ο οργανισμός σε περίπτωση καταστροφής. Μέσω της βασικής εκπαίδευσης επιδιώκεται η εξοικείωση του προσωπικού με τα οργανωτικά και τεχνικά μέτρα ανάκαμψης καθώς και η ενημέρωσή του σχετικά με τις υποχρεώσεις του, εφόσον υπάρχουν, σχετικά με τις άμεσες ενέργειες τους και τους υπεύθυνους στους οποίους θα πρέπει να απευθύνονται. Επιδιώκεται με τον τρόπο αυτό η ικανότητα του προσωπικού να προσαρμοστεί άμεσα, αν ποτέ χρειαστεί, σε περίπτωση καταστροφής.

Η βασική εκπαίδευση συνήθως διενεργείται από το προσωπικό που φέρει την ευθύνη της εκτέλεσης του ΣΑΚ και μπορεί να περιλαμβάνει από το διαμοιρασμό ενός ειδικού ενημερωτικού εντύπου έως τη διενέργεια ετήσιας παρουσίασης σεμιναριακού τύπου. Η εκπαίδευση αυτή θα πρέπει να διενεργείται τόσο κατά την πρόσληψη του προσωπικού όσο και ύστερα από κάθε σημαντική αλλαγή στην ακολουθούμενη πολιτική ή στις ακολουθούμενες στρατηγικές αντιμετώπισης.

- Εξειδικευμένη εκπαίδευση: η εξειδικευμένη εκπαίδευση αφορά στο προσωπικό που εμπλέκεται άμεσα με την εφαρμογή του ΣΑΚ. Μπορεί να περιλαμβάνει εκπαίδευση τόσο σε οργανωτικά όσο και σε τεχνικά μέτρα αντιμετώπισης. Τα οργανωτικά μέτρα μπορεί να αποτελούνται από εφαρμοζόμενα πρότυπα, νέες τάσεις και καλές πρακτικές στο πεδίο της αντιμετώπισης καταστροφών, ενώ τα τεχνικά από εφαρμογή και διαχείριση νέων τεχνολογιών. Η παραπάνω εκπαίδευση μπορεί να καλύπτεται μέσα από συμμετοχή σε συνέδρια και παρακολούθηση εξειδικευμένων σεμιναρίων.

5.3 Εγκαταστάσεις

Κρίσιμο συστατικό για τα ΠΣ αποτελούν και οι εγκαταστάσεις οι οποίες τα φιλοξενούν. Αφού διασφαλιστούν οι κύριες εγκαταστάσεις με όλα τα διαθέσιμα προληπτικά μέτρα [11] [51], θα πρέπει να ληφθεί μέριμνα ώστε σε περίπτωση που καταστραφούν να υπάρχει εναλλακτική λύση μέχρι την αποκατάστασή τους. Η διαθεσιμότητα αυτή επιτυγχάνεται με την πρόβλεψη για χρήση εναλλακτικών εγκαταστάσεων, σε απομακρυσμένο χώρο, ικανές να φιλοξενήσουν τα ΠΣ μέχρι την πλήρη αποκατάσταση των κύριων. Οι χώροι αυτοί μπορεί να είναι [7]

- **Ιδιόκτητοι**: όπου αποτελούν χώρους του ίδιου του οργανισμού ικανούς να φιλοξενήσουν τα ΠΣ για το διάστημα που απαιτείται. Εφόσον υπάρχουν τέτοιοι χώροι με κατάλληλες εγκαταστάσεις αποτελούν ιδανικό τρόπο αντιμετώπισης της διαθεσιμότητας αφού υπόκεινται στον απόλυτο διαχειριστικό έλεγχο του οργανισμού.
- **με Ανταποδοτική συμφωνία**: όπου οι χώροι κάποιου άλλου οργανισμού, οι οποίοι συνήθως φιλοξενούν τις κύριες εγκαταστάσεις του, μπορούν να διατεθούν στο πλαίσιο μιας συνεργασίας, διασφαλισμένη με τη μορφή συγκροτημένου μνημονίου

συνεργασίας, ως εναλλακτικές για τον οργανισμό. Συνήθως αυτές οι συμφωνίες είναι αμοιβαίες και ο δεύτερος αναλαμβάνει την αντίστοιχη υποχρέωση για τον πρώτο. Η λύση αυτή αποτελεί τον πλέον οικονομικό τρόπο για την εξασφάλιση εναλλακτικών εγκαταστάσεων δεδομένου ότι και οι δύο οργανισμοί διαθέτουν κύριες εγκαταστάσεις οι οποίες πληρούν τις βασικές απαιτήσεις λειτουργίας ΠΣ (υποδομές, ηλεκτρισμός, τηλεπικοινωνίες). Ιδιαίτερη προσοχή θα πρέπει να δίδεται στον τυχόν συντονισμό που απαιτείται αλλά και στις διαφορετικές απαιτήσεις ασφάλειας και τα αντίστοιχα εφαρμοζόμενα μέτρα για τα δεδομένα του κάθε οργανισμού.

- **με Εμπορική μίσθωση**: όταν κανένας από τους παραπάνω τρόπους δεν είναι διαθέσιμος, υπάρχει η δυνατότητα της εμπορικής μίσθωσης του χώρου με συνεπακόλουθο το υψηλότερο κόστος. Σήμερα υπάρχουν διαθέσιμες υπηρεσίες οι οποίες παρέχουν, κατόπιν ζήτησης (on demand), εξειδικευμένους χώρους, ειδικά διαμορφωμένους με κατάλληλες προδιαγραφές, για τη φιλοξενία εναλλακτικών εγκαταστάσεων οργανισμών σε αρκετά ανταγωνιστικές τιμές.

Κατά την επιλογή των χώρων φιλοξενίας των εναλλακτικών εγκαταστάσεων θα πρέπει να υπάρχει μέριμνα ώστε να διαθέτουν όλες τις απαραίτητες υποδομές που απαιτούνται για τη λειτουργία των ΠΣ (παροχή ηλεκτρισμού, κλιματισμού, τηλεπικοινωνιών). Θα πρέπει επίσης να λαμβάνεται υπόψη η απόσταση των εναλλακτικών εγκαταστάσεων από αυτή της κύριας. Ενώ η μεγάλη απόσταση διασφαλίζει την ανεπηρέαστη διαθεσιμότητα των εγκαταστάσεων από το ίδιο καταστροφικό γεγονός, μπορεί την ίδια στιγμή να εμποδίζει την έγκαιρη και ταχεία ανάκαμψη των συστημάτων λόγω δυσκολίας έγκαιρης μετάβασης των απαραίτητων πόρων (προσωπικού, εξοπλισμού, δεδομένων). Ως αποδεκτή ελάχιστη απόσταση μεταξύ κύριων και εναλλακτικών εγκαταστάσεων προτείνεται μεταξύ 15-80 Km ανάλογα και με τα ιδιαίτερα γεωμορφολογικά χαρακτηριστικά [57].

Ιδιαίτερη σημασία θα πρέπει να δίδεται στην διασυνδεσιμότητα μεταξύ κύριας και εναλλακτικής εγκατάστασης, ώστε να είναι σε θέση τα ΠΣ της εναλλακτικής εγκατάστασης να ανταπεξέλθουν στις ανάγκες των χρηστών.

Οι χώροι φιλοξενίας των εναλλακτικών εγκαταστάσεων μπορεί να διακρίνονται ανάλογα με το επίπεδο εξοπλισμού που διαθέτουν σε [49]:

cold sites: χώροι οι οποίοι διαθέτουν μόνο τις απαραίτητες υποδομές όπως παροχή ηλεκτρισμού, τηλεπικοινωνιών, κλιματολογικού ελέγχου. Οι χώροι αυτοί δε διαθέτουν δικό τους εξοπλισμό αλλά είναι έτοιμοι να φιλοξενήσουν τον απαραίτητο εξοπλισμό των προς αποκατάσταση ΠΣ αν χρειαστεί. Συνήθως αυτοί οι χώροι, ανάλογα και με το μέγεθος και την πολυπλοκότητα των ΠΣ, μπορούν να προσφέρουν ανάκαμψη σε διάρκεια ημερών ή εβδομάδων.

warm sites: σε αυτούς τους χώρους πέρα από τις κατάλληλες υποδομές υπάρχει και εγκατεστημένος εξοπλισμός που αφορά το απαραίτητο υλικό και λογισμικό για την λειτουργία των προς αποκατάσταση ΠΣ. Συνήθως δε διαθέτουν ούτε τις απαραίτητες εφαρμογές ούτε τα δεδομένα που απαιτούνται για να αποκατασταθούν. Μετά από μια καταστροφή και την έναρξη του ΣΑΚ, όλες οι απαραίτητες εφαρμογές και τα δεδομένα από τα αντίγραφα ασφαλείας, μεταφέρονται στο χώρο για να εγκατασταθούν και να παραμετροποιηθούν ώστε να επαναλειτουργήσουν τα ΠΣ. Οι χρόνοι ανάκτησης αυτής της λύσης είναι βελτιωμένοι και κυμαίνονται από μερικές ώρες έως μερικές μέρες.

hot sites: είναι χώροι οι οποίοι διαθέτουν τόσο τις απαραίτητες υποδομές και τον εξοπλισμό, όσο και τις εφαρμογές και τα δεδομένα έτοιμα προς λειτουργία και αντικατάσταση των κυρίως ΠΣ. Μετά από την ενεργοποίηση του ΣΑΚ απαιτείται μόνο η ανάκτηση του τελευταίου αντιγράφου ασφαλείας των δεδομένων στις εναλλακτικές εγκαταστάσεις ώστε να καταστούν παραγωγικές. Αποτελεί λύση με υψηλό κόστος αλλά προσφέρει χρόνους ανάκτησης από μερικά λεπτά σε μερικές ώρες.

Δύο παραλλαγές των παραπάνω εναλλακτικών εγκαταστάσεων αποτελούν οι παρακάτω:

Mobile sites: αφορούν κινητές εναλλακτικές εγκαταστάσεις που μπορούν να μετακινηθούν κατά βούληση. Συνήθως αποτελούνται από κοντέινερ με δυνατότητες να λάβουν ρόλο αντίστοιχο των cold, warm, hot sites τα οποία μπορούν να μεταβούν πλησίον των πληγέντων εγκαταστάσεων, εφόσον δε πρόκειται για εκτεταμένη καταστροφή, ή σε οποιαδήποτε άλλη απομακρυσμένη περιοχή.

Mirrored sites: αφορούν εγκαταστάσεις οι οποίες αποτελούν πιστά αντίγραφα των κυρίως εγκαταστάσεων όσον αφορά εξοπλισμό, εφαρμογές και δεδομένα. Είναι έτοιμα να αναπληρώσουν τη λειτουργικότητα των κυρίως ΠΣ και εφαρμόζουν τεχνολογίες

συγχρονισμού των δεδομένων σε πραγματικό χρόνο μεταξύ των δυο εγκαταστάσεων, ώστε να επιτυγχάνουν σχεδόν αδιάλειπτη λειτουργία.

5.4 Τεχνολογίες

Αναφερόμενοι στις τεχνολογίες από τις οποίες αποτελούνται τα ΠΣ εννοούμε τόσο τις πλατφόρμες και τις εφαρμογές από τις οποίες απαρτίζονται όσο και τις δικτυακές και τηλεπικοινωνιακές τεχνολογίες που χρησιμοποιούν. Τα βασικότερα μέτρα που χρησιμοποιούνται για να εξασφαλιστεί η συνέχεια της λειτουργίας τους σε περίπτωση καταστροφής αναφέρονται παρακάτω.

5.4.1 Εικονικοποίηση συστημάτων (Virtualization)

Με την εικονικοποίηση συστημάτων δίνεται η δυνατότητα να μετατραπούν όλοι οι φυσικοί εξυπηρετητές σε εικονικούς. Οι, πλέον, εικονικές μηχανές αντιμετωπίζονται ως σύνολα αρχείων-δεδομένων και ως τέτοια μπορούν να διαχειρίζονται, να συμπιέζονται και να αντιγράφονται. Επιτυγχάνεται έτσι η ανεξαρτητοποίηση της λογισμικής πλατφόρμας από την υλική πλατφόρμα (hardware) ή οποία, σε συνδυασμό με τεχνικές snapshots, καθιστούν εφικτή τη γρήγορη μετακίνηση των εικονικών μηχανών μεταξύ διαφορετικών πλατφόρμων υλικού. Παράλληλα, δίνεται η δυνατότητα στην ίδια φυσική μηχανή να φιλοξενηθούν παραπάνω εικονικές μηχανές παρέχοντας λοιπόν υψηλότερο βαθμό αξιοποίησης των υπολογιστικών πόρων. Το παραπάνω γεγονός παρόλο που οδηγεί σε μείωση του αρχικού κόστους επένδυσης, άλλα και των λειτουργικών εξόδων, εισάγει τον κίνδυνο της ταυτόχρονης κατάρρευσης των εικονικών μηχανών σε περίπτωση σφάλματος υλικού της φυσικής μηχανής που τα φιλοξενεί.

Η εικονικοποίηση προσφέρει ευελιξία, αυτοματοποίηση διαδικασιών, μεγάλες δυνατότητες φορητότητας και γρήγορους χρόνους ανάκαμψης. Επειδή όμως οι εικονικές μηχανές αντιμετωπίζονται πλέον ως αρχεία μπορεί να αυξήσουν σε σημαντικό βαθμό τον όγκο των δεδομένων που πρέπει να προστατεύεται με αντίγραφα ασφαλείας.

Η εικονικοποίηση συστημάτων δεν μπορεί να θεωρηθεί πανάκεια για την εφαρμογή ενός ΣΑΚ καθώς υπάρχουν εφαρμογές οι οποίες είτε δε μπορούν να απεξαρτηθούν από το φυσικό μηχάνημα, λόγω χρήσης εξειδικευμένων περιφερειακών, είτε δεν μπορούν να

επιτρέψουν τον διαμοιρασμό φυσικών πόρων από πολλές εικονικές μηχανές. Ενδεικτικά τέτοιες εφαρμογές μπορεί να θεωρηθούν αυτές που χειρίζονται βάσεις δεδομένων με υψηλές απαιτήσεις I/O.

5.4.2 Τεχνολογίες υπολογιστικού νέφους (Cloud computing)

Ορισμένοι πάροχοι υπηρεσιών πηγαίνοντας ένα βήμα παραπέρα την εφαρμογή τεχνολογιών εικονικοποίησης, παρέχουν ως υπηρεσία τη χρήση εικονικών υπολογιστικών πόρων με τη μορφή του υπολογιστικού νέφους με στόχο την οικονομία κλίμακας που επιτυγχάνεται από την ενοποίηση πόρων. Οι υπηρεσίες αυτές ανάλογα με το βαθμό ολοκλήρωσής τους μπορούν να διατεθούν σε τρεις μορφές [58]:

- **Software as a Service (SaaS):** όπου ο πάροχος διαχειρίζεται και διατηρεί τον έλεγχο όλης της υπολογιστικής υποδομής και παρέχει έτοιμες υπηρεσίες προς χρήση στους πελάτες. Οι πελάτες έχουν περιορισμένη διαχειριστικές δυνατότητες οι οποίες περιορίζονται στην μερική παραμετροποίηση της εφαρμογής. Χαρακτηριστικό παράδειγμα αποτελούν εφαρμογές ηλεκτρονικού ταχυδρομείου και εφαρμογών γραφείου.

- **Platform as a Service (PaaS):** σε αυτό το μοντέλο ο πάροχος διαθέτει προς χρήση πλατφόρμες εφαρμογών με κατάλληλο προγραμματιστικό περιβάλλον και με εγκατεστημένα εργαλεία ανάπτυξης λογισμικού. Ο πάροχος διατηρεί τον έλεγχο της υπολογιστικής υποδομής επιτρέποντας στον πελάτη να διαχειρίζεται το περιβάλλον ανάπτυξης και να επιλέγει ο ίδιος τις εφαρμογές που θα εγκαταστήσει. Παράδειγμα αποτελούν εφαρμογές εξυπηρετητή ιστού, διαδικτυακές βάσεις δεδομένων και εξειδικευμένες διαδικτυακές εφαρμογές.

- **Infrastructure as a Service (IaaS):** παρέχει το μικρότερο βαθμό ολοκλήρωσης, όπου ο πελάτης έχει το μέγιστο δυνατό έλεγχο στις υπολογιστικές υποδομές. Επιτρέπει την πλήρη διαχείριση των εικονικών μηχανών, δίνοντας τη δυνατότητα εγκατάστασης του επιθυμητού λειτουργικού συστήματος και εφαρμογών. Παράδειγμα αποτελούν η διάθεση αποκλειστικών εικονικών μηχανών, εξυπηρετητών, δικτυακών μέσων αποθήκευσης.

Ιδιόκτητα Συστήματα	Infrastructure as a service	Platform as a service	Software as a service
Δεδομένα	Δεδομένα	Δεδομένα	Δεδομένα
Εφαρμογές	Εφαρμογές	Εφαρμογές	Εφαρμογές
Εργαλεία Ανάπτυξης Λογισμικού	Εργαλεία Ανάπτυξης Λογισμικού	Εργαλεία Ανάπτυξης Λογισμικού	Εργαλεία Ανάπτυξης Λογισμικού
Προγραμματιστικό περιβάλλον	Προγραμματιστικό περιβάλλον	Προγραμματιστικό περιβάλλον	Προγραμματιστικό περιβάλλον
Λειτουργικό σύστημα	Λειτουργικό σύστημα	Λειτουργικό σύστημα	Λειτουργικό σύστημα
Εικονική μηχανή	Εικονική μηχανή	Εικονική μηχανή	Εικονική μηχανή
Εξυπηρετητής	Εξυπηρετητής	Εξυπηρετητής	Εξυπηρετητής
Αποθήκευση	Αποθήκευση	Αποθήκευση	Αποθήκευση
Δικτύωση	Δικτύωση	Δικτύωση	Δικτύωση

Διαχείριση από προμηθευτή
Μερική διαχείριση από πελάτη
Ολική διαχείριση από πελάτη

Πίνακας 5: *Μορφές υπολογιστικού νέφους*

Τα υπολογιστικά αυτά νέφη διακρίνονται παράλληλα ως προς το μοντέλο ανάπτυξής τους σε [58]:

- **Ιδιωτικά (Private):** όπου όλες οι διατιθέμενες υποδομές χρησιμοποιούνται αποκλειστικά από έναν οργανισμό. Αυτές μπορεί να διαχειρίζονται από τον ίδιο τον οργανισμό ή από κάποιον τρίτο, για λογαριασμό του, και μπορεί να φιλοξενούνται εντός ή εκτός των εγκαταστάσεων του οργανισμού.

- **Δημόσια (Public):** οι διατιθέμενες υποδομές μπορεί να χρησιμοποιούνται από διαφορετικούς οργανισμούς. Συνήθως ανήκουν σε κάποιον πάροχο υπηρεσιών υπολογιστικού νέφους ο οποίος και τις διαμοιράζει στο κοινό.
- **Κοινοτικά (Community):** οι διατιθέμενες υποδομές χρησιμοποιούνται από μια ομάδα οργανισμών με κοινά ενδιαφέροντα και απαιτήσεις (π.χ. επίπεδο ασφάλειας, νομικών υποχρεώσεων, επιχειρησιακών απαιτήσεων). Τα κοινοτικά νέφη μπορεί να φιλοξενούνται εντός ή εκτός των εγκαταστάσεων κάποιου μέλους της κοινότητας ή ακόμα και να βρίσκονται διαμοιρασμένα μεταξύ τους.
- **Υβριδικά (Hybrid):** οι διατιθέμενες υποδομές αποτελούν συνδυασμό των παραπάνω υλοποιήσεων. Παρόλο που οι υλοποιήσεις αυτές μπορεί να είναι διακριτές μεταξύ τους διατηρούν συνδεσιμότητα μέσω τεχνολογιών που επιτρέπει την φορητότητα δεδομένων και εφαρμογών(πχ για διαμοιρασμό φόρτου).

Αυτές οι υπηρεσίες λόγο της ευελιξίας τους και του γεγονότος ότι μπορούν να χρησιμοποιηθούν ανάλογα με τις ανάγκες του οργανισμού (on demand) μπορούν να αποτελέσουν ιδανικό τρόπο αντιμετώπισης των καταστροφών με μικρό κόστος επένδυσης. Αυτό ακριβώς το γεγονός έχει οδηγήσει στη παροχή υπηρεσιών υπολογιστικού νέφους, προσαρμοσμένες για τις ιδιαίτερες ανάγκες που απαιτεί η ανάκαμψη των ΠΣ ενός οργανισμού, γνωστές με τον όρο **Disaster Recovery as a Service (DRaaS)**.

Μια υπηρεσία DRaaS μπορεί να λάβει τη μορφή από την απλή διάθεση διαδικτυακού χώρου για την απομακρυσμένη αποθήκευσης των αντιγράφων ασφαλείας (cloud storage) ως και τη διάθεση ολοκληρωμένων εναλλακτικών διαδικτυακών εγκαταστάσεων (ως warm site ή hot site). Κάνοντας χρήση εικονικών μηχανών για τον συγχρονισμό με κρίσιμες εφαρμογές είναι σε θέση να παρέχουν τη δυνατότητα γρήγορων χρόνων ανάκαμψης, έως και 4 φορές γρηγορότερα από ότι με τις παραδοσιακές μεθόδους [59]. Παράλληλα δίνεται η δυνατότητα ακόμα και σε μικρούς οργανισμούς που δε είναι σε θέση να διαθέσουν τον απαραίτητο χώρο, εξοπλισμό και προσωπικό για αποτελεσματική εφαρμογή σχεδίων ανάκαμψης. Αυτή η αποτελεσματικότητα των υπηρεσιών DRaaS αποτυπώνεται και στη πρόβλεψη από το Gartner ότι μέχρι το 2014 το 30% των μεσαίων οργανισμών, σε αντίθεση με το 1% αυτή τη στιγμή, θα τις έχουν υιοθετήσει για να καλύψουν τις ανάγκες τους όσον αφορά την ανάκαμψη των συστημάτων τους [60].

Παρόλα τα οφέλη που προκύπτουν από τη χρήση υπηρεσιών υπολογιστικού νέφους, γίνεται άμεσα φανερό ότι ο οργανισμός θα πρέπει να δώσει ιδιαίτερη βαρύτητα στη δραματική αύξηση των απαιτήσεων για γρήγορες, αποδοτικές και αξιόπιστες συνδέσεις WAN. Ταυτόχρονα, υπεισέρχονται ζητήματα ασφάλειας και ιδιωτικότητας των δεδομένων, τα οποία, μετακινούμενα στο υπολογιστικό νέφος φεύγουν πια από το άμεσο έλεγχο του οργανισμού. Επομένως καθίσταται απαραίτητη, ιδίως στη περίπτωση νεφών δημόσιας πρόσβασης, η ύπαρξη μέτρων ασφάλεια σε επίπεδο [61] :

- Φυσικής πρόσβασης
- Δικτύου (εικονικά δίκτυα)
- Εικονικών μηχανών
- Δεδομένων(εικονικών δίσκων)

5.4.3 Συστήματα Υψηλής διαθεσιμότητας

Ως συστήματα υψηλής διαθεσιμότητας νοούνται αυτά τα οποία έχουν σχεδιαστεί και ρυθμιστεί με τέτοιο τρόπο ώστε να παραμένουν λειτουργικά σε περίπτωση καταστροφικών συμβάντων. Ως βαθμός απόδοσης της υψηλής διαθεσιμότητας, έχει επικρατήσει η έκφρασή του σε ποσοστό διαθεσιμότητας στη διάρκεια ενός έτους. Στον παρακάτω Πίνακα 6 παρουσιάζονται ορισμένα ενδεικτικά ποσοστά και ο χρόνος μη διαθεσιμότητας στον οποίο αντιστοιχούν. Για να θεωρηθεί κάποιο σύστημα ως υψηλής διαθεσιμότητας θα πρέπει να επιτυγχάνει ποσοστό μεγαλύτερο του 99,999%.

Availability %	Downtime per year	Downtime per month	Downtime per week
99.9% ("three nines")	8.76 hours	43.2 minutes	10.1 minutes
99.99% ("four nines")	52.56 minutes	4.32 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds

Πίνακας 6: *Χρόνοι υψηλής διαθεσιμότητας*

Τα συστήματα αυτά αποτελούνται από δυο ή περισσότερους κόμβους-εξυπηρετητές (server clusters), οι οποίοι συνήθως μοιράζονται τα ίδια δεδομένα και διαθέτουν τεχνολογίες αναγνώρισης και ειδοποίησης σε περίπτωση μη διαθεσιμότητας. Με τον τρόπο αυτό σε περίπτωση που κάποιος κόμβος καταστεί μη λειτουργικός αυτόματα αντικαθίσταται από κάποιον άλλον. Συνήθως οι κόμβοι βρίσκονται είτε σε διάταξη Active-Standby, οπού ο πρώτος εξυπηρετεί και ο δεύτερος είναι σε αδράνεια και έτοιμος προς χρήση, είτε σε

διάταξη Active-Active, όπου και οι δύο εξυπηρετούν παράλληλα επιτυγχάνοντας ταυτόχρονα και επιμερισμό φόρτου (load balancing). Συνήθως οι κόμβοι αυτών των συστημάτων περιορίζονται χωρικά εντός του ίδιου LAN καθώς οι δικτυακές απαιτήσεις είναι υψηλές, υπάρχουν όμως αρχιτεκτονικές (metro clusters) που δεδομένης της ύπαρξης αξιόπιστης σύνδεσης (συνήθως δικτύου οπτικής ίνας) επιτρέπουν την απομακρυσμένη εγκατάστασή τους παρέχοντας υψηλού επιπέδου ανάκαμψη (RTO, RPO σχεδόν μηδενικά). Τα συστήματα υψηλής διαθεσιμότητας απαιτούν εξειδικευμένο εξοπλισμό και τεχνογνωσία για την αποτελεσματική εφαρμογή και υποστήριξή τους.

5.4.4 Τηλεπικοινωνίες

Οι τηλεπικοινωνίες ενώ αποτελούν σημαντικό στοιχείο για τα ΠΣ ενός οργανισμού αποκτούν μια νέα διάσταση, καθώς αποτελούν κρίσιμο παράγοντα για την επιτυχή εφαρμογή ενός ΣΑΚ. Η σύνδεση LAN και WAN ενός οργανισμού αποτελεί απαραίτητο στοιχείο για την επικοινωνία των κυρίως εγκαταστάσεων με τις εναλλακτικές ιδίως όταν υιοθετούνται λύσεις υπολογιστικού νέφους, απομακρυσμένης λήψης αντιγράφων ασφαλείας ή ανάθεσης σε τρίτους. Οι κυριότεροι τρόποι διασφάλισης της διαθεσιμότητάς τους είναι η χρήση εφεδρικών αρχιτεκτονικών, η βελτιστοποίηση της απόδοσης τους, η χρήση εναλλακτικών μέσων-δικτύων μετάδοσης και η χρήση απομακρυσμένης πρόσβασης.

Αρχιτεκτονικές εφεδρείας: Με τη χρήση αρχιτεκτονικών εφεδρείας επιτυγχάνεται η υψηλή διαθεσιμότητα των στοιχείων του δικτύου και των συνδέσεων. Επομένως προτείνεται η χρήση τόσο εφεδρικού εξοπλισμού όσο και εφεδρικών συνδέσεων σε διατάξεις υψηλής διαθεσιμότητας ώστε να αποφεύγεται η ύπαρξη μοναδικών σημείων αποτυχίας (single point of failure) στα δίκτυα LAN και WAN. Ιδιαίτερα για τα WAN δίκτυα θα πρέπει να επιδιώκεται η ύπαρξη εφεδρικών συνδέσεων από διαφορετικούς παρόχους, οι οποίοι κάνουν χρήση διαφορετικών δικτύων υποδομής, και διαθέτουν υπηρεσίες εγγυημένου επιπέδου (SLAs). Αυτές οι αρχιτεκτονικές αν και είναι ιδιαίτερα αποτελεσματικές εισάγουν την ανάγκη ύπαρξης πρόσθετου εξοπλισμού και αυξάνουν την πολυπλοκότητα διαχείρισης του δικτύου.

Βελτιστοποίηση απόδοσης (Wan optimization): Με τον όρο αυτό αναφερόμαστε σε τεχνολογίες οι οποίες επιταχύνουν και αυξάνουν την αποδοτικότητα των μέσων δικτυακής επικοινωνίας. Αυτή η βελτιστοποίηση επιτυγχάνεται με τη χρήση εξειδικευμένων συσκευών οι οποίες:

- μειώνουν τον διακινούμενο όγκο μέσω του δικτύου με τεχνικές συμπίεσης
- χρησιμοποιούν πρωτόκολλα που βελτιστοποιούν τη μετάδοση δεδομένων
- ελέγχουν το εύρος ζώνης και την διαθεσιμότητα (traffic shaping-QoS) του δικτύου ανάλογα με τις ανάγκες του οργανισμού
- βελτιστοποιούν τη μετάδοση με τη δημιουργία πολλαπλών παράλληλων συνδέσεων
- απαλείφουν επαναλαμβανόμενες δομές δεδομένων και τις αντικαθιστούν (data deduplication) πριν τη μετάδοση τους, ώστε να μειώνεται ο διακινούμενος όγκος
- αποθηκεύουν τοπικά και προσωρινά (caching) δεδομένα που έχουν αυξημένη και επαναλαμβανόμενη ζήτηση ώστε να αποφεύγεται η άσκοπη αναμετάδοση τους

Η χρήση αυτών των τεχνολογιών πολλές φορές έχουν μικρότερο κόστος από τη διεύρυνση του εύρους ζώνης που απαιτείται, από τις ενδεχόμενες αυξημένες δικτυακές απαιτήσεις ενός οργανισμού, ενώ μειώνουν την καθυστέρηση (latency) που παρατηρείται στις απομακρυσμένες μεταδόσεις. Εκτιμάται ότι μπορούν να επιτύχουν από 10-100x παραπάνω μείωση στα δεδομένα κίνησης μέσω WAN, κάνοντας μια σύνδεση 24Mbps να συμπεριφέρεται σαν να ήταν 240Mbps ή και παραπάνω [62][63].

Εναλλακτικά μέσα μετάδοσης: Σήμερα για τη διαμόρφωση των δικτυακών συνδέσεων ενός οργανισμού, είτε αφορούν LAN είτε WAN, έχουν επικρατήσει οι ενσύρματες τεχνολογίες διασύνδεσης λόγω της αυξημένης αξιοπιστίας, της ταχύτητας και της ασφάλειας των δεδομένων μετάδοσης που προσφέρουν. Ταυτόχρονα, η ίδια η ενσύρματη φύση τους τα καθιστά ιδιαίτερα ευάλωτα σε περιπτώσεις καταστροφικών συμβάντων, στρέφοντας έτσι το ενδιαφέρον στη χρήση δικτύων με εναλλακτικά μέσα μετάδοσης. Τέτοια δίκτυα μπορεί να είναι τα ασύρματα δίκτυα (wifi) στην περίπτωση δικτύων LAN και τα δορυφορικά ή τα ασύρματα-κινητά (3G, 4G) για τα δίκτυα WAN. Ορισμένα από τα χαρακτηριστικά τους αποτελούν:

- **Κινητά:** αποτελούν σχετικά φθηνή λύση και εύκολη στην υλοποίηση ενώ πλέον προσφέρουν ικανοποιητικές ταχύτητες. Υστερούν ως προς το επίπεδο της διαθεσιμότητάς τους καθώς σε περίπτωση εκτεταμένων καταστροφών τείνουν να υπερκορέζονται. Εξαρτώνται από επίγειες υποδομές (base stations) οι οποίες με τη σειρά τους είναι ευάλωτες σε εκτεταμένες καταστροφές.
- **Δορυφορικά:** αποτελούν πιο ακριβή λύση λόγω του εξειδικευμένου εξοπλισμού που απαιτείται και της πολυπλοκότητας κατά την εγκατάστασή τους. Προσφέρουν

αρκετά υψηλό επίπεδο διαθεσιμότητας ξεκινώντας από 99,95 και φθάνοντας το 99,999 (χρήση C-band), καθιστώντας τα ιδανικά όταν οι απαιτήσεις διαθεσιμότητας είναι ιδιαίτερα υψηλές. Το κυριότερο αρνητικό χαρακτηριστικό αποτελεί η υψηλή καθυστέρηση (latency) που μπορεί να παρουσιάζεται κατά τη μετάδοση δεδομένων λόγω των μεγάλων αποστάσεων (Γή-δορυφόρος) [64].

Απομακρυσμένη πρόσβαση: Σε περίπτωση καταστροφής αποκτά ιδιαίτερη σημασία η δυνατότητα απομακρυσμένης πρόσβασης στα ΠΣ ενός οργανισμού. Έτσι δίδεται η δυνατότητα τόσο στους χρήστες να χρησιμοποιούν τους πληροφοριακούς πόρους από/σε εναλλακτικές εγκαταστάσεις αλλά και σε απομακρυσμένα συστήματα να επικοινωνούν μεταξύ τους, μέχρι την πλήρη ανάκαμψη των κυρίως εγκαταστάσεων. Η επικρατέστερη τεχνολογία που υπάρχει σήμερα για αυτό το σκοπό είναι η χρήση εικονικών ιδιόκτητων δικτύων (VPN), τα οποία επιτυγχάνονται με τη χρήση συμβατού λογισμικού και συσκευών και διακρίνονται κυρίως σε:

- **IPSec VPN:** αποτελεί το πλέον παραδοσιακό τρόπο σύνδεσης VPN ο οποίος υποστηρίζεται από τις περισσότερες συσκευές και απαιτεί τη χρήση κατάλληλου λογισμικού από τους χρήστες. Προτείνεται για συνδέσεις από σημείο σε σημείο (point to point) [65].
- **SSL VPN:** αποτελεί ίσως τον επικρατέστερο σύγχρονο τρόπο πρόσβασης, καθώς κάνει χρήση του πρωτοκόλλου SSL/TLS επιτρέποντας την σύνδεση από οπουδήποτε με τη χρήση ενός απλού web browser. Προτείνεται για υποστήριξη τηλεργασίας.
- **Cloud VPN:** όπου γίνεται η χρήση υπηρεσιών υπολογιστικού νέφους για την παροχή υπηρεσιών πρόσβασης σύμφωνα με τη ζήτηση (on demand), αποφεύγοντας την αγορά εξοπλισμού και πολύπλοκες παραμετροποιήσεις.

5.5 Δεδομένα

Όσον αφορά στα δεδομένα θα πρέπει να διασφαλίζεται η ύπαρξη αποτελεσματικών συστημάτων λήψης αντιγράφων ασφαλείας καθώς και η ύπαρξη αντίστοιχων πολιτικών για τη λήψη και την ανάκτησή τους. Η λήψη των αντιγράφων θα πρέπει να λαμβάνεται ανά τακτά χρονικά διαστήματα ώστε να εξασφαλίζεται η ύπαρξη αντιγράφου όλων των πρόσφατων αλλαγών. Η συχνότητα αυτή καθορίζεται βάσει των αναγκών του οργανισμού και με τρόπο ώστε να εξασφαλίζεται το απαιτούμενο RPO. Παρακάτω αναφέρονται τα μέσα

αποθήκευσης, οι μέθοδοι λήψης αντιγράφων και οι τεχνικές αντιγραφής δεδομένων που προσφέρονται για την ανάκτηση των δεδομένων σε περίπτωση καταστροφής.

5.5.1 Μέσα Αποθήκευσης

Κασέτες (Tape): αποτελεί τον πλέον παραδοσιακό και αποδοτικό, ως προς το κόστος, μέσο λήψης αντιγράφων ασφαλείας. Εισάγει σε μεγάλο βαθμό την ανάμιξη χειροκίνητων διαδικασιών τόσο κατά τη λήψη και τη μεταφορά-αποθήκευση των αντιγράφων εκτός των κυρίων εγκαταστάσεων, όσο και κατά τη διαδικασία ανάκτησης. Συνεπώς αυξάνει τη πολυπλοκότητα της διαδικασίας λήψης αντιγράφων, αυξάνει την πιθανότητα ανθρωπίνων λαθών και παρατείνει το χρόνο ανάκαμψης. Παράλληλα δημιουργεί περιορισμούς ως προς τη γεωγραφική απόσταση μεταξύ του σημείου φύλαξης (συνήθως στις εναλλακτικές εγκαταστάσεις, εφόσον υπάρχουν) και των κυρίως εγκαταστάσεων λόγω της ανάγκης φυσικής μετακίνησης του μέσου. Λόγω της μεγάλης διάρκειας ζωής των κασετών θεωρούνται ιδανικό μέσο για αρχειοθέτηση δεδομένων ειδικά σε οργανισμούς όπου υπάρχει νομική υποχρέωση διατήρησης δεδομένων (δημόσιο, υγεία, οικονομία, έρευνα).

Σκληροί δίσκοι (Hd): οι σκληροί δίσκοι ως μέσα αποθήκευσης αντιγράφων ασφαλείας παρέχουν μεγαλύτερες χωρητικότητες και ταχύτερους χρόνους λήψης και ανάκτησης αντιγράφων. Παρόλο που το κόστος τους παραμένει υψηλότερο σε σχέση με τις κασέτες παρέχουν μεγαλύτερη αυτοματοποίηση στη διαδικασία λήψης-ανάκτησης καθώς και μείωση της πολυπλοκότητας αφού δεν απαιτούνται συσκευές ανάγνωσης όπως με τις κασέτες. Χρησιμοποιούμενοι σε συστοιχίες RAID παρέχουν μέγιστη ασφάλεια από μοναδικά σημεία σφάλματος (single point of failure).

Διαδικτυακός χώρος σε υπολογιστικό νέφος (Online backup-Cloud storage): η χρήση του online backup αναφέρεται στη δυνατότητα απομακρυσμένης λήψης ή/και ανάκτησης των αντιγράφων ασφαλείας με τη χρήση δικτυακών τεχνολογιών WAN,WWW και υποδομών cloud storage. Βασικό πλεονέκτημα είναι ότι παρέχει ταυτόχρονα απομακρυσμένη φύλαξη του αντιγράφου ασφαλείας. Παράλληλα αποτελεί λύση η οποία προσαρμόζεται ανάλογα με τις πρόσκαιρες ανάγκες ως προς τη χωρητικότητα (on demand), αποφεύγοντας λάθη κατά τη διαστασιολόγηση των απαιτούμενων αναγκών τα οποία μπορεί να οδηγήσουν σε περιττό κόστος.

Η χρήση αυτού του μέσου παρόλο που παρέχει τη δυνατότητα ορθολογικότερης διαχείρισης της χωρητικότητας αποθήκευσης, μειώνοντας περιττά κόστη, εισάγει το πρόσθετο κόστος των υψηλών απαιτήσεων δικτυακής πρόσβασης που απαιτείται ως προς το εύρος ζώνης, την ταχύτητα μετάδοσης και την διαθεσιμότητα του δικτύου. Σαν μέσο αποθήκευσης κρίνεται ιδανικό όταν το μέγεθος των δεδομένων του αντιγράφου ασφαλείας είναι σχετικά μικρό και δεν υπόκεινται σε συχνές αλλαγές και υπάρχει επάρκεια δικτυακών πόρων. Χαρακτηριστικά μπορούμε να πούμε ότι όταν τα δεδομένα του αντιγράφου είναι 100GB και η σύνδεση επιτυγχάνεται με τεχνολογία DSL (24 download / 1 upload), τότε για την λήψη του πλήρους αντιγράφου τοπικά απαιτούνται τουλάχιστον 10 ώρες, εκτοξεύοντας το χρόνο ανάκαμψης.

Κατά τη χρήση αυτού του μέσου αποθήκευσης θα πρέπει να δίνεται ιδιαίτερη σημασία στην ασφάλεια των διακινούμενων δεδομένων του οργανισμού, είτε βρίσκονται αποθηκευμένα είτε σε κίνηση, καθώς διέρχονται από υποδομές οι οποίες δεν είναι στο άμεσο έλεγχο του οργανισμού. Προτείνεται λοιπόν η κρυπτογράφηση των δεδομένων πριν την αποστολή τους αλλά και η χρήση κρυπτογραφημένου καναλιού μετάδοσης (ssl).

5.5.2 Μέθοδοι λήψης αντιγράφων ασφαλείας

Οι βασικοί μέθοδοι λήψης αντιγράφων ασφαλείας είναι [53]:

Full (Πλήρες): με τη μέθοδο αυτή λαμβάνεται πλήρες αντίγραφο όλων των δεδομένων που έχουν οριστεί κάθε φορά άσχετα αν έχουν τροποποιηθεί ή όχι. Σε περίπτωση ανάκτησης απαιτείται μόνο η χρήση του τελευταίου πλήρους αντιγράφου ασφαλείας. Παρέχει ευκολία και γρήγορο χρόνο ανάκτηση καθώς όλα τα δεδομένα είναι συγκεντρωμένα στο ίδιο σημείο. Αντίθετα απαιτείται μεγαλύτερος χρόνος για τη λήψη του αντιγράφου και καταλαμβάνει μεγαλύτερο όγκο αποθήκευσης

Differential (Διαφορικό): το αντίγραφο αυτό περιλαμβάνει μόνο τα δεδομένα που έχουν τροποποιηθεί ή προστεθεί συγκριτικά με τα δεδομένα που περιέχονται στο τελευταίο πλήρες αντίγραφο (full backup). Σε περίπτωση πλήρους ανάκτησης των δεδομένων απαιτείται η χρήση του τελευταίου Διαφορικού αντιγράφου και του πλήρους αντιγράφου στο οποίο αναφέρεται. Καταλαμβάνει μικρότερο όγκο αποθήκευσης και απαιτεί μικρότερο χρόνο λήψης του αντιγράφου. Εισάγει μεγαλύτερη πολυπλοκότητα και απαιτεί περισσότερο χρόνο για την ανάκτηση δεδομένων σε σχέση με το πλήρες αντίγραφο.

Incremental (Αυξητικό): το αυξητικό αντίγραφο περιλαμβάνει τα δεδομένα που τροποποιήθηκαν ή προστέθηκαν συγκριτικά με το τελευταίο αντίγραφο ανεξάρτητα με τη μέθοδο με την οποία ελήφθη. Για να επιτευχθεί πλήρης ανάκτηση απαιτούνται πέρα από το τελευταίο πλήρες αντίγραφο ασφαλείας και όλα τα ενδιάμεσα αυξητικά αντίγραφα. Η μέθοδος αυτή απαιτεί το μικρότερο όγκο αποθήκευσης και το μικρότερο χρόνο λήψης αλλά θεωρείται ότι έχει την υψηλότερη πολυπλοκότητα και απαιτεί το περισσότερο χρόνο για ανάκτηση δεδομένων.

5.5.3 Τεχνικές αντιγραφής δεδομένων

Data Replication: αφορά σε τεχνικές αντιγραφής των δεδομένων μεταξύ δυο κόμβων. Διακρίνεται σε:

- **Synchronous replication:** όπου τα δεδομένα αντιγράφονται μεταξύ των κόμβων σε πραγματικό χρόνο παρέχοντας υψηλότατο βαθμό προστασίας (μικρό RPO σε επίπεδο δευτερολέπτου ή λεπτού). Δεν προτείνεται για απομακρυσμένα αντίγραφα λόγω του υψηλού latency που εισάγει.
- **Asynchronous replication:** όπου τα δεδομένα αντιγράφονται με μια σχετική καθυστέρηση. Με τη τεχνική αυτή απαιτείται μικρότερο εύρος ζώνης ενώ επιτυγχάνεται η αξιόπιστη μεταφορά των δεδομένων σε μεγαλύτερες αποστάσεις.

Data dedupliation: αφορά στη διαδικασία δημιουργίας αντιγράφου ασφαλείας όπου επιχειρείται η μείωση του όγκου του αντιγράφου μέσω της παράλειψης τυχόν όμοιων μπλοκ δεδομένων και χρησιμοποιείται κυρίως όταν εφαρμόζεται λήψη απομακρυσμένων αντιγράφων ασφαλείας. Αυτή η μείωση μπορεί να πραγματοποιείται είτε στο πρώτο κόμβο-αποστολέα, επιβαρύνοντας τον επεξεργαστικά αλλά αποφορτίζοντας την απαραίτητη δικτυακή μεταφορά, είτε στο δεύτερο-παραλήπτη, αντιστρέφοντας τις συνέπειες (λιγότερη επεξεργαστική επιβάρυνση παραγωγικού κόμβου και μεγαλύτερες δικτυακές απαιτήσεις).

Continuous Data Protection (CDP): αφορά μέθοδο αντιγραφής δεδομένων κατά την οποία κάθε αλλαγή που συμβαίνει στα δεδομένα του πρώτου κόμβου αυτή αμέσως καταγράφεται και αντιγράφεται στον δεύτερο. Διαφέρει με τις τεχνικές σύγχρονης αντιγραφής καθώς δίδει τη δυνατότητα διατήρησης της ιστορικότητας των αλλαγών επιτρέποντας την ανάκτηση διαφορετικών παλαιότερων εκδόσεων των δεδομένων προς ανάκτηση.

Snapshots: με τη μέθοδο αυτή τα δεδομένα του πρώτου κόμβου αντιγράφονται στο δεύτερο κατά περιοδικά διαστήματα σε επίπεδο λεπτών ή ωρών. Στην ουσία αποτελούν αντίγραφα ολόκληρου του συστήματος αρχείων όπως αυτό παρουσιαζόταν σε κάποια χρονική στιγμή άσχετα αν έχει επέλθει σε αυτό κάποια αλλαγή, καθιστώντας το ιδανική λύση για ανάκτηση εικονικών μηχανών από καταστροφή. Κατά την ανάκτηση δε μπορεί να γίνει επιλογή συγκεκριμένων δεδομένων, αλλά να ανακτηθεί ολόκληρο το σύστημα αρχείων και να ακολουθήσει η όποια διαλογή, αυξάνοντας την πολυπλοκότητα και το χρόνο της επιλεκτικής ανάκτησης.

5.6 Διαδικασίες

Οι διαδικασίες που αφορούν στα ΠΣ ενός οργανισμού αφορούν όλες τις απαραίτητες ενέργειες και οδηγίες που σχετίζονται με τη χρήση, εγκατάσταση, διαχείριση, παραμετροποίηση και αποσφαλμάτωσή τους. Αυτές μπορεί να έχουν τη μορφή εγχειριδίων, σε έντυπη ή ηλεκτρονική μορφή, τα οποία συνοδεύονται από το απαραίτητο υλικό εγκατάστασης, άδειες χρήσης, διαγράμματα αρχιτεκτονικής, συμβόλαια υποστήριξης και τα αντίστοιχα σχέδια ανάκτησης που τα αφορούν (ISCPs).

Για τη διασφάλιση των διαδικασιών από ενδεχόμενη καταστροφή μπορούν να ληφθούν μέτρα κυρίως οργανωτικής φύσης, όπως:

- Υιοθέτηση προτύπων σχετικά με διαχείριση και τυποποίηση διαδικασιών σχετικές με ΠΣ (ενδεικτικά ISO 27001, ISO 20000, ISO 24762).
- Συλλογή και ταξινόμηση τεκμηρίωσης και διαδικασιών ανά ΠΣ.
- Ορισμός υπευθύνων διατήρησης-επικαιροποίησης διαδικασιών και τεκμηρίωσης.
- Δημιουργία πολλαπλών αντιγράφων τα οποία θα φυλάσσονται σε διαφορετικές και ασφαλείς τοποθεσίες (ιδανικά στις εναλλακτικές εγκαταστάσεις εφόσον αυτές υπάρχουν).
- Διενέργεια δοκιμών εφαρμογής των διαδικασιών, για τη διασφάλιση της αποτελεσματικότητάς τους και την εμπέδωσή τους από τους εμπλεκόμενους.
- Δημιουργία προσωρινών χειροκίνητων διαδικασιών μέχρι την ανάκαμψη των ΠΣ.

5.7 Προμηθευτές

Βασικό στοιχείο στα ΠΣ αποτελούν οι προμηθευτές εξοπλισμού (λογισμικού και υλικού) και υπηρεσιών. Σε περίπτωση καταστροφής θα πρέπει να έχει εξασφαλιστεί η συνεργασία τους καθώς και η ανταπόκρισή τους στις ανάγκες του οργανισμού εντός προκαθορισμένου χρόνου (SLAs). Επομένως θα πρέπει να λαμβάνεται μέριμνα για:

5.7.1 Αντικατάσταση εξοπλισμού

Με την εμφάνιση μιας καταστροφής είναι πολύ πιθανό οι επιπτώσεις να είναι ολέθριες για τον εξοπλισμό, υλικό και λογισμικό, των ΠΣ. Θα πρέπει να υπάρχει μέριμνα για την έγκαιρη προμήθειά του, είτε για τις ανάγκες των εναλλακτικών εγκαταστάσεων είτε για την αντικατάσταση του προσβεβλημένου στις κύριες. Οι βασικοί τρόποι αντιμετώπισης αυτής της ανάγκης είναι:

- **Συμφωνία με προμηθευτές:** ο οργανισμός μπορεί να έρθει σε συμφωνία με τους βασικούς προμηθευτές του εξοπλισμού που χρησιμοποιεί έτσι ώστε, στα πλαίσια συμφωνιών παροχής υπηρεσιών εγγυημένου επιπέδου (SLAs), να μπορεί να προμηθεύεται κατά προτεραιότητα αντίστοιχο εξοπλισμό.
- **Εφεδρικός εξοπλισμός:** ο απαραίτητος εξοπλισμός μπορεί να εξασφαλιστεί με αγορά εκ των προτέρων και να χρησιμοποιηθεί στις εναλλακτικές εγκαταστάσεις (warm site, hot site). Η λύση αυτή παρέχει ταχύτερη ανταπόκριση στις απαιτήσεις αλλά εμπεριέχει υψηλότερο κόστος.
- **Υπάρχον συμβατός εξοπλισμός:** μπορεί να υπάρχει η πρόβλεψη ώστε όταν υπάρχει διαθέσιμος συμβατός εξοπλισμός στον οργανισμό να χρησιμοποιείται προσωρινά για την εξυπηρέτηση της ανάκαμψης. Συνήθως ο εξοπλισμός αυτός χρησιμοποιείται για λιγότερο κρίσιμες ανάγκες ή μπορεί να έχει αποσυρθεί λόγω αναβαθμίσεων.

5.7.2 Προγραμματισμός δαπανών

Καθοριστικής σημασίας είναι και ο κατάλληλος προγραμματισμός δαπανών και η εξασφάλιση της επάρκειάς τους, όταν αυτό καταστεί απαραίτητο. Τα κόστη αυτά, τα οποία θα πρέπει να καλύπτουν τις ανάγκες της επιλεχθείσας στρατηγικής αντιμετώπισης, αφορούν ενδεικτικά:

- Προμήθεια υπηρεσιών
- Προμήθεια εξοπλισμού (υλικού, λογισμικού)
- Έξοδα μεταφοράς/μετακίνησης

- Έξοδα εργατοωρών
- Έξοδα δοκιμών
- Έξοδα υλικών/αναλωσίμων

5.7.3 Ανάθεση σε τρίτους (Outsourcing)

Σε περιπτώσεις όπου ένας οργανισμός δεν διαθέτει κατάλληλο προσωπικό και τεχνογνωσία για τη διαχείριση της ανάκαμψης από καταστροφές, μπορεί να προσφύγει στη λύση της ανάθεσης αυτών των εργασιών σε τρίτους. Με τον τρόπο αυτό επιλέγεται η μεταφορά της ευθύνης αντιμετώπισης των κινδύνων μιας ενδεχόμενης καταστροφής με την ανάθεση είτε επιμέρους τμημάτων είτε ολόκληρου του σχεδιασμού ανάκαμψης. Επομένως μια ενδεχόμενη ανάθεση μπορεί να καλύπτει από την απλή μεταφορά και φύλαξη των αντιγράφων ασφαλείας ως την εξολοκλήρου ανάθεση της ανάκαμψης με τη μορφή παροχής υπηρεσίας “Disaster Recovery as a Service” (DRaaS) διασφαλισμένη από συμβόλαια προκαθορισμένου επιπέδου (SLAs).

Κατά την ανάθεση υπηρεσιών σε τρίτους καθίσταται σαφές ότι δημιουργούνται επιπλέον απαιτήσεις εμπιστευτικότητας, ιδίως όταν αφορά στη διαχείριση προσωπικών-ευαίσθητων δεδομένων. Παράλληλα, επειδή είναι ορατός ο κίνδυνος της λειτουργικής εξάρτησης του οργανισμού από τρίτους θα πρέπει να διασφαλίζεται ότι σε περίπτωση που καταστεί απαραίτητο, όπως είναι η παύση λειτουργίας του παρόχου, να υπάρχουν εναλλακτικές λύσεις. Ιδιαίτερη σημασία θα πρέπει να δίδεται και στο γεγονός ότι σε περίπτωση εκτεταμένης καταστροφής οι πάροχοι υπηρεσιών ανάκτησης θα πρέπει να είναι σε θέση να εξυπηρετήσουν τις ενδεχόμενες ανάγκες ανάκαμψης από πολλούς πελάτες τους ταυτόχρονα [66]. Προτείνεται για το λόγο αυτό να εξετάζεται η ευρύτητα του πεδίου δράσης καθώς και της διαθεσιμότητας πόρων και εγκαταστάσεων που διαθέτει ο πάροχος.

Πρέπει να τονιστεί ότι η τελική ευθύνη της διασφάλισης της ανάκαμψης από καταστροφές ανήκει πάντα στον ίδιο τον οργανισμό και οφείλει σε περίπτωση ανάθεσης σχετικών υπηρεσιών σε τρίτους να πιστοποιεί ότι αυτές ανταποκρίνονται στις απαιτήσεις του, διενεργώντας τακτικές δοκιμές και απαιτώντας την ύπαρξη διεθνών πιστοποιήσεων (πχ. ISO 24762).

5.8 Συγκριτική αξιολόγηση μέτρων ανάκαμψης

Όπως διαφαίνεται παραπάνω υπάρχει πληθώρα διαθέσιμων μέτρων για την εφαρμογή σχεδίων αντιμετώπισης καταστροφών. Κάθε ένα από αυτά έχει διαφορετικές απαιτήσεις για την επιτυχή εφαρμογή του, διακρίνεται από διαφορετικό βαθμό αποτελεσματικότητας και έχει διαφορετική επίπτωση τόσο στον ίδιο το σχεδιασμό όσο και στη λειτουργία του οργανισμού. Συνοψίζοντας τις παρατηρήσεις των προηγούμενων παραγράφων, επιχειρείται η συγκριτική αξιολόγηση των μέτρων αυτών.

Η σύγκριση αυτή βασίζεται στην ποιοτική αξιολόγηση 8 επιμέρους δεικτών που κατατάσσονται σε δυο κατηγορίες, σε αυτά που αφορούν τις απαιτήσεις των μέτρων και σε αυτά που αφορούν τις επιπτώσεις τους. Οι δείκτες αυτοί είναι:

Απαιτήσεις μέτρων:

- **Κόστος:** αφορά στο κόστος εφαρμογής του μέτρου και μπορεί να περιλαμβάνει το κόστος απόκτησης, λειτουργίας και συντήρησής του (TCO).
- **Χρόνος:** αφορά στο χρόνο που απαιτείται για την ανάπτυξη και πλήρη εφαρμογή του μέτρου.
- **Πόροι:** αφορά στους πόρους που απαιτούνται για την εφαρμογή του μέτρου και περιλαμβάνει τόσο τον εξοπλισμό όσο και τις απαραίτητες εργατοώρες.
- **Τεχνογνωσία:** αφορά στην τεχνογνωσία που απαιτείται για την εφαρμογή του μέτρου καθώς και τις συνεπακόλουθες απαιτήσεις εκπαίδευσης.

Επιπτώσεις μέτρων:

- **Διαθεσιμότητα:** αφορά στις επιπτώσεις στη διαθεσιμότητα των ΠΣ κατά την εμφάνιση ενός καταστροφικού συμβάντος. Ως μέτρο σύγκρισης λαμβάνεται η διάρκεια απώλειας της διαθεσιμότητας δεδομένων, η οποία μπορεί να εκφράζεται ως το άθροισμα του χρόνου RPO+RTO.
- **Εμπιστευτικότητα:** αφορά στις επιπτώσεις στην εμπιστευτικότητα των δεδομένων. Συνήθως αυτή επηρεάζεται από την απώλεια ή μη της κυριότητας των δεδομένων κατά την εφαρμογή του μέτρου.
- **Πολυπλοκότητα:** αφορά στις επιπτώσεις που επιφέρει η εφαρμογή του μέτρου στις λειτουργίες και την παραγωγικότητα του οργανισμού. Αυτές συνήθως οφείλονται στις νέες διαδικασίες που μπορεί να απαιτούνται

- **Ωριμότητα:** αφορά στο βαθμό ωριμότητας του μέτρου και την αξιοπιστία του. Λαμβάνεται υπόψη η επίδοση του συγκεκριμένου μέτρου, διαχρονικά και ιστορικά, για τον σκοπό της ανάκαμψης από καταστροφές.

Παρακάτω παρουσιάζονται σε μορφή πίνακα οι επιδόσεις κάθε μέτρου χρησιμοποιώντας ποιοτική κλίμακα 5 σημείων κατατάσσοντας τις απαιτήσεις σε:

- Πολύ υψηλές
- Υψηλές
- Μέτριες
- Χαμηλές
- Πολύ χαμηλές

και τις επιπτώσεις σε:

- Πολύ καλές
- Καλές
- Μέτριες – Ουδέτερες
- Κακές
- Πολύ κακές

		ΑΠΑΙΤΗΣΕΙΣ					ΕΠΙΠΤΩΣΕΙΣ			
		Κόστος (TCO)	**Χρόνος**	**Πόροι**	**Τεχνογνωσία**		**Διαθεσιμότητα (RPO+RTO)**	**Εμπιστευτικότητα**	**Πολυπλοκότητα**	**Ωριμότητα**
Άνθρωποι	**Αριθμ.επάρκεια**									
	Αναπλήρωση (redundancy)	Πολύ χαμηλές	Μέτριες	Πολύ χαμηλές	Υψηλές		Καλές	Πολύ καλές	Μέτριες-ουδέτερες	Καλές
	Ανάθεση (Outsourcing)	Υψηλές	Χαμηλές	Πολύ χαμηλές	Πολύ χαμηλές		Μέτριες-ουδέτερες	Κακές	Καλές	Μέτριες-ουδέτερες
	Τηλεεργασία	Πολύ χαμηλές	Πολύ χαμηλές	Μέτριες	Πολύ χαμηλές		Πολύ καλές	Μέτριες-ουδέτερες	Πολύ καλές	Καλές
	Εκπαίδευση									
	Βασική εκπαίδευση	Πολύ χαμηλές	Πολύ χαμηλές	Πολύ χαμηλές	Μέτριες		Καλές	Καλές	Καλές	Πολύ καλές
	Εξειδικευμένη εκπαίδευση	Μέτριες	Υψηλές	Μέτριες	Υψηλές		Πολύ καλές	Καλές	Πολύ καλές	Πολύ καλές
Εγκαταστάσεις	**Ιδιοκτησιακά**									
	Ιδιόκτητες	Μέτριες	Υψηλές	Πολύ υψηλές	Πολύ υψηλές		Πολύ καλές	Πολύ καλές	Κακές	Πολύ καλές
	Ανταποδοτική συμφωνία	Πολύ χαμηλές	Μέτριες	Μέτριες	Μέτριες		Καλές	Πολύ κακές	Μέτριες-ουδέτερες	Μέτριες-ουδέτερες
	Εμπορική μίσθωση	Υψηλές	Χαμηλές	Χαμηλές	Χαμηλές		Πολύ καλές	Κακές	Πολύ καλές	Καλές
	Επίπεδο εξοπλισμού									
	cold sites	Μέτριες	Χαμηλές	Μέτριες	Μέτριες		Μέτριες-ουδέτερες		Καλές	Πολύ καλές
	warm sites	Υψηλές	Υψηλές	Υψηλές	Υψηλές		Καλές		Μέτριες-ουδέτερες	Πολύ καλές
	hot sites	Πολύ υψηλές	Πολύ υψηλές	Πολύ υψηλές	Πολύ υψηλές		Πολύ καλές		Κακές	Πολύ καλές
	mobile sites	Υψηλές	Χαμηλές	Πολύ υψηλές	Πολύ υψηλές		Καλές		Κακές	Μέτριες-ουδέτερες
	mirrored sites	Πολύ υψηλές	Πολύ υψηλές	Πολύ υψηλές	Πολύ υψηλές		Πολύ καλές		Κακές	Μέτριες-ουδέτερες
Τεχνολογίες	**Πλατφόρμες-Συστήματα**									
	Συστήματα Υψηλής διαθεσιμότητας	Υψηλές	Μέτριες	Υψηλές	Υψηλές		Πολύ καλές	Μέτριες-ουδέτερες	Μέτριες-ουδέτερες	Πολύ καλές
	Εικονικοποίηση	Μέτριες	Μέτριες	Μέτριες	Υψηλές		Καλές	Μέτριες-ουδέτερες	Καλές	Καλές
	Υπολογιστικό νέφος-DRaaS	Μέτριες	Μέτριες	Χαμηλές	Πολύ χαμηλές		Καλές	Κακές	Καλές	Κακές
	Τηλεπικοινωνίες									
	Αρχιτεκτονικές εφεδρείας	Υψηλές	Μέτριες	Υψηλές	Υψηλές		Πολύ καλές	Μέτριες-ουδέτερες	Μέτριες-ουδέτερες	Πολύ καλές
	Βελτιστοποίηση απόδοσης (wan optimization)	Μέτριες	Χαμηλές	Μέτριες	Μέτριες		Καλές	Μέτριες-ουδέτερες	Μέτριες-ουδέτερες	Μέτριες-ουδέτερες
	Εναλλακτικά μέσα μετάδοσης									
	satellite	Υψηλές	Υψηλές	Υψηλές	Υψηλές		Καλές	Μέτριες-ουδέτερες	Μέτριες-ουδέτερες	Μέτριες-ουδέτερες
	mobile	Μέτριες	Μέτριες	Μέτριες	Χαμηλές		Μέτριες-ουδέτερες	Κακές	Καλές	Μέτριες-ουδέτερες
	Απομακρυσμένη πρόσβαση									
	IPSec VPN	Χαμηλές	Υψηλές	Μέτριες	Υψηλές		Καλές	Μέτριες-ουδέτερες	Μέτριες-ουδέτερες	Πολύ καλές
	SSL VPN	Μέτριες	Χαμηλές	Χαμηλές	Μέτριες		Καλές	Μέτριες-ουδέτερες	Πολύ καλές	καλή
	Cloud VPN	Χαμηλές	Πολύ χαμηλές	Πολύ χαμηλές	Χαμηλές		Καλές	Κακές	Πολύ καλές	Κακές
Δεδομένα	**Μέσα**									
	tape	Χαμηλές	Υψηλές	Υψηλές	Μέτριες		Μέτριες-ουδέτερες	Καλές	Κακές	Καλές

	hd	Υψηλές	Χαμηλές	Μέτριες	-		Πολύ καλές	Πολύ καλές	Καλές	Καλές
	online	Μέτριες	Χαμηλές	Πολύ χαμηλές	Πολύ χαμηλές		Μέτριες-ουδέτερες	Κακές	Πολύ καλές	Κακές
	Μέθοδοι									
	full	Υψηλές	Υψηλές	Πολύ υψηλές	Μέτριες		Πολύ καλές	Πολύ καλές	Πολύ καλές	Πολύ καλές
	differential	Μέτριες	Μέτριες	Υψηλές	Μέτριες		Καλές	Καλές	Μέτριες-ουδέτερες	Πολύ καλές
	incremental	Χαμηλές	Χαμηλές	Μέτριες	Μέτριες		Μέτριες-ουδέτερες	Μέτριες-ουδέτερες	Κακές	Πολύ καλές
	Τεχνικές									
	replication sync	Πολύ υψηλές	Μέτριες	Πολύ υψηλές	Μέτριες		Πολύ καλές		Μέτριες-ουδέτερες	Καλές
	replication async	Υψηλές	Μέτριες	Μέτριες	Μέτριες		Καλές		Μέτριες-ουδέτερες	Καλές
	deduplication	Μέτριες	Μέτριες	Υψηλές	Μέτριες		Μέτριες-ουδέτερες		Μέτριες-ουδέτερες	Καλές
	cdp	Πολύ υψηλές	Μέτριες	Πολύ υψηλές	Μέτριες		Πολύ καλές		Μέτριες-ουδέτερες	Καλές
	snapshot	Υψηλές	Μέτριες	Υψηλές	Μέτριες		Καλές		Μέτριες-ουδέτερες	Καλές
Διαδικασίες	**Εφαρμογή προτύπων**	Υψηλές	Υψηλές	Υψηλές	Υψηλές		Πολύ καλές	Πολύ καλές	Κακές	Πολύ καλές
	Λήψη οργανωτικών μέτρων	Πολύ χαμηλές	Χαμηλές	Χαμηλές	Χαμηλές		Καλές	Καλές	Καλές	Καλές
Προμηθευτές	**Αντικατάσταση εξοπλισμού**									
	συμφωνια με προμηθευτες (SLAs)	Χαμηλές	Χαμηλές	Πολύ χαμηλές	Χαμηλές		Μέτριες-ουδέτερες	Μέτριες-ουδέτερες	Πολύ καλές	Μέτριες-ουδέτερες
	εφεδρικός εξοπλισμός	Πολύ υψηλές	Μέτριες	Πολύ υψηλές	Μέτριες		Πολύ καλές	Μέτριες-ουδέτερες	Πολύ καλές	Πολύ καλές
	συμβατός εξοπλισμός	Πολύ χαμηλές	Πολύ χαμηλές	Μέτριες	Υψηλές		Καλές	Μέτριες-ουδέτερες	Μέτριες-ουδέτερες	Πολύ καλές
	Προγραμματισμός δαπανών	Χαμηλές	Μέτριες	Πολύ χαμηλές	Μέτριες		Πολύ καλές	Μέτριες-ουδέτερες	Πολύ καλές	Πολύ καλές
	Ανάθεση υπηρεσιών (outsourcing)	Υψηλές	Μέτριες	Πολύ χαμηλές	Πολύ χαμηλές		Καλές	Κακές	Πολύ καλές	Μέτριες-ουδέτερες

Πίνακας 7: *Συγκριτική αξιολόγηση μέτρων ανάκαμψης*

6 Μελέτη περίπτωσης σε φορέα υγείας

6.1 Εισαγωγή

Σε μια προσπάθεια εφαρμογής όσων περιγράφονται παραπάνω, σχετικά με το σχεδιασμό ανάκαμψης από καταστροφές, θα χρησιμοποιηθεί ως μελέτη περίπτωσης ο σχεδιασμός ανάκαμψης από καταστροφές για έναν υποθετικό οργανισμό που αποτελεί πρωτοβάθμιο φορέα υγείας.

Μέσα από αυτή τη μελέτη περίπτωσης θα επιχειρηθεί η εφαρμογή της μεθοδολογίας σχεδιασμού για ένα εξειδικευμένο περιβάλλον, όπως είναι αυτό του χώρου της υγείας.

Αρχικά θα περιγραφεί το μοντέλο λειτουργίας ενός τέτοιου οργανισμού καθώς και τα Πληροφοριακά Συστήματα από τα οποία συνήθως απαρτίζεται. Στη συνέχεια θα εφαρμοστεί η προτεινόμενη μεθοδολογία της §4 ώστε να αποκαλυφθούν τα βασικά συστατικά τα οποία απαιτούνται για την εφαρμογή ενός επιτυχημένου Σχεδίου Ανάκαμψης από Καταστροφές καθώς και τα ιδιαίτερα ζητήματα που ενδέχεται να ανακύψουν. Ως αποτέλεσμα επιδιώκεται ο καθορισμός της ροής σχεδιασμού της ανάκαμψης αλλά και η δημιουργία ενός πρότυπου πλάνου ΣΑΚ, για την υιοθέτηση και υλοποίησή του από μικρομεσαίους και μικρούς οργανισμούς (<100 ατόμων) στο συντομότερο δυνατό χρόνο.

6.2 Περιγραφή οργανισμού

6.2.1 Παραδοχές μελέτης περίπτωσης

Ο προς εξέταση υποθετικός οργανισμός αφορά σε φορέα παροχής υπηρεσιών πρωτοβάθμιας υγείας, του οποίου το πεδίο δράσης μπορεί να εκτείνεται σε μια ευρεία μητροπολιτική περιοχή και ο οποίος μπορεί να αποτελείται από ένα σύνολο διεσπαρμένων αλλά διασυνδεδεμένων μονάδων παροχής υπηρεσιών υγείας.

Παρακάτω παρατίθενται συγκεντρωμένες όλες οι βασικές παραδοχές που γίνονται για την μελέτη που ακολουθεί. Επομένως γίνεται δεκτό ότι ο οργανισμός προς εξέταση:

- Αποτελεί οργανισμό μικρομεσαίου μεγέθους με αριθμό προσωπικού ~100 ατόμων.

- Έχει ετήσιο κύκλο εργασιών ~2.000.000€. (Το ποσό αυτό αντιστοιχεί μόνο σε έσοδα που είναι άμεσα συνδεδεμένα με τις λειτουργίες του οργανισμού οι οποίες εξαρτώνται από τα Πληροφοριακά του Συστήματα. Παρατηρείται περιορισμένος κύκλος εργασιών ο οποίος οφείλεται σε άσκηση κοινωνικής πολιτικής)
- Έχει ετήσιο κόστος μισθοδοσίας ~3.000.000€.
- Διαθέτει ετησίως ποσό ~200.000€ για έξοδα σε Τεχνολογίες Πληροφορικής.
- Διαθέτει βασικό σχεδιασμό για συνέχιση λειτουργιών (Business continuity) σε περίπτωση απώλειας των ΠΣ, η οποία είναι σε θέση να εξασφαλίσει χειροκίνητη-χειρόγραφη λειτουργικότητα των υπηρεσιών επιτυγχάνοντας ποσοστό παραγωγικότητας προσεγγιστικά ~50%
- Έχει εμπειρία και εφαρμόζει πρότυπα ποιότητας (ISO 9001, ISO 27001)

6.2.2 Οργάνωση - Μοντέλο λειτουργίας

Ένας τυπικός φορέας παροχής υπηρεσιών πρωτοβάθμιας φροντίδας υγείας αποτελείται από τις παρακάτω υπηρεσίες οι οποίες διακρίνονται στις Ιατρικές, οι οποίες αφορούν την καθεαυτό παροχή υπηρεσιών υγείας σε ασθενείς, και στις Διοικητικές, οι οποίες αφορούν στην διεκπεραίωση των απαραίτητων λειτουργιών για την εύρυθμη λειτουργία των μονάδων. Αυτές με τη σειρά τους συνήθως διαρθρώνονται σε:

<u>Ιατρικές Υπηρεσίες</u>

- **Κλινική Φροντίδα:** η υπηρεσία αυτή αφορά στην παροχή υπηρεσιών υγείας σε ασθενείς, κατόπιν προκαθορισμένου ραντεβού και στην αντιμετώπιση επειγόντων περιστατικών.
- **Ιατρικές Απεικονίσεις:** αφορά στην διενέργεια απεικονιστικών εξετάσεων όπως ενδεικτικά είναι ο κλασικός ακτινολογικός έλεγχος, η υπερηχοτομογραφία, η μαγνητική τομογραφία και η αξονική τομογραφία.
- **Βιοπαθολογικά Εργαστήρια:** αφορά στη διενέργεια όλων των απαραίτητων μικροβιολογικών εξετάσεων για την αντιμετώπιση κοινών νοσημάτων και για την υποβοήθηση των προνοσοκομειακών ιατρικών υπηρεσιών.
- **Αποκατάσταση-Αποθεραπεία:** αφορά στην παροχή εξειδικευμένων υπηρεσιών διάγνωσης και αξιολόγησης παθήσεων καθώς και στην υλοποίησης εξατομικευμένων προγραμμάτων αποκατάστασης και αποθεραπείας. Στο ίδιο πλαίσιο μπορεί να εντάσσονται και υπηρεσίες ψυχολογικής υποστήριξης και κοινωνικής στήριξης.

Διοικητικές Υπηρεσίες

- **Διοικητικές Υπηρεσίες:** αφορά στις εν γένει διοικητικές υπηρεσίες του φορέα και μπορεί να περιλαμβάνει λειτουργίες που αφορούν στη διαχείριση του ανθρώπινου δυναμικού (τήρηση μητρώου, ωρομέτρηση παρουσίας, εκπαίδευση προσωπικού), στην εξυπηρέτηση ασθενών (διαχείριση ραντεβού, έκδοση παραστατικών) και στην εν γένει γραμματειακή υποστήριξη (τήρηση πρωτοκόλλου, διαχείριση αλληλογραφίας, γραμματειακή υποστήριξη λοιπών υπηρεσιών, πληροφόρηση και επικοινωνία).
- **Οικονομικές Υπηρεσίες:** σε αυτές υπάγονται λειτουργίες σχετικές με την οικονομική δραστηριότητα του οργανισμού. Τέτοιες μπορεί να αποτελούν η σύνταξη και ο έλεγχος εκτέλεσης του προϋπολογισμού, η έκδοση μισθοδοσίας, η είσπραξη εσόδων και αποπληρωμή εξόδων καθώς και λοιπές υπηρεσίες λογιστηρίου. Στην ίδια υπηρεσία μπορεί να συμπεριλαμβάνονται και λειτουργίες προμήθειας και διαχείρισης υλικών.
- **Τεχνικές Υπηρεσίες:** αφορά στις λειτουργίες που σχετίζονται με την υποστήριξη των υποδομών του φορέα αλλά και σε λειτουργίες που σχετίζονται με την καθαριότητα στους χώρους εργασίας και την ασφάλεια- φυσική φύλαξη των εγκαταστάσεων.
- **Υπηρεσίες Πληροφορικής:** περιλαμβάνει όλες τις λειτουργίες που αφορούν στην ορθή λειτουργία των ΠΣ του φορέα, είτε πρόκειται για την υποστήριξη συστημάτων και χρηστών είτε για την ανάπτυξη και παραμετροποίηση εξειδικευμένου λογισμικού. Εδώ περιλαμβάνονται και οι λειτουργίες που σχετίζονται με την ασφάλεια των Πληροφοριακών Συστημάτων και εν γένει των διακινούμενων πληροφοριών.
- **Υπηρεσίες Βιοϊατρικής Τεχνολογίας:** αφορά σε λειτουργίες όπως είναι η διαχείριση και υποστήριξη του ιατροτεχνολογικού εξοπλισμού και η εκπόνηση εκθέσεων και μελετών για τον εκσυγχρονισμό και την προμήθεια νέων μηχανημάτων.
- **Υπηρεσίες Ολικής Ποιότητας:** περιλαμβάνει όλες τις απαραίτητες λειτουργίες του οργανισμού για την εξασφάλιση της ποιότητας των παρεχομένων υπηρεσιών του οργανισμού.
- **Υπηρεσίες Εσωτερικού Ελέγχου:** περιλαμβάνει τις λειτουργίες που απαιτούνται για τη συμμόρφωση με τη νομοθεσία και το κανονιστικό πλαίσιο που αφορά τον οργανισμό.
- **Νομική υπηρεσία:** αφορά στη νομική υποστήριξη και εκπροσώπηση του οργανισμού.

6.2.3 Πληροφοριακά Συστήματα

Τα ΠΣ που απαντώνται σε φορείς πρωτοβάθμιας υγείας μπορούν να ταξινομηθούν σε τρεις κατηγορίες ανάλογα με τις λειτουργίες-υπηρεσίες που εξυπηρετούν. Αυτές αποτελούνται από τα Ιατρικά ΠΣ, τα οποία επικουρούν στην παροχή των υπηρεσιών υγείας του φορέα, τα Διοικητικά ΠΣ που υποστηρίζουν τις διοικητικές λειτουργίες του φορέα και τα λοιπά Υποστηρικτικά ΠΣ τα οποία εξυπηρετούν την εν γένει λειτουργία των υπολοίπων ΠΣ και λειτουργιών του οργανισμού. Παρακάτω παρατίθενται ορισμένα από τα πιο συνηθισμένα που μπορεί να συναντήσει κανείς σε ένα τέτοιο οργανισμό.

<u>Κλινικά ΠΣ</u>

- **Electronic Health Records (EHR):** Αναφέρεται συνήθως ως Ηλεκτρονικός Ιατρικός Φάκελος και χρησιμοποιείται για τη συλλογή και επεξεργασία πληροφοριών για την υγεία των ασθενών. Προσφέρεται για τη διαχείριση ιατρείων και ασθενών και την εξαγωγή στατιστικών στοιχείων και στην ουσία αποτελεί τη μεταφορά του έντυπου ιατρικού φακέλου ασθενών σε ηλεκτρονική μορφή. Όταν διασυνδέεται με άλλα ΠΣ μπορεί να περιλαμβάνει και αποτελέσματα εργαστηριακών και ακτινολογικών εξετάσεων.
- **Radiology Information System (RIS):** Είναι το ΠΣ το οποίο διασυνδέεται με τον ακτινολογικό εξοπλισμό (MRI, CT, X-rays, κοκ) και χρησιμοποιείται για την διαχείριση των ασθενών κατά τη διενέργεια ακτινολογικών εξετάσεων.
- **Picture archiving and communication system (PACS):** Είναι το ΠΣ, το οποίο διασυνδέεται με τον ακτινολογικό εξοπλισμό και το RIS, και χρησιμοποιείται για την αρχειοθέτηση και διακίνηση των εικόνων που παράγονται από τα ακτινολογικά τμήματα.
- **Laboratory Information System (LIS):** Είναι το ΠΣ των Ιατρικών Εργαστηρίων, το οποίο συνήθως είναι διασυνδεδεμένο με κατάλληλο εργαστηριακό εξοπλισμό, με σκοπό την αποθήκευση και διακίνηση αποτελεσμάτων εργαστηριακών εξετάσεων (αιματολογικών, μικροβιολογικών, βιοπαθολογικών κοκ).
- **Medical Applications:** Είναι εξειδικευμένες εφαρμογές λογισμικού που μπορεί να είναι απαραίτητες για την διαχείριση και λειτουργία λοιπού ιατροτεχνολογικού εξοπλισμού.

- **e-Health:** αποτελεί μια ευρύτερη κατηγορία ΠΣ για την οποία έχουν προταθεί πολλαπλοί ορισμοί [67]. Συνοπτικά μπορούμε να θεωρήσουμε ότι περιλαμβάνει άλλα πληροφοριακά συστήματα που δεν περιγράφονται παραπάνω και αφορούν στην εφαρμογή τεχνολογιών πληροφορικής και επικοινωνιών στην παροχή ιατρικών υπηρεσιών κυρίως μέσω της χρήσης τεχνολογιών διαδικτύου. Ως τέτοια μπορούν να θεωρηθούν διάφορα δίκτυα πληροφοριών για την υγεία, ηλεκτρονικά μητρώα υγείας, υπηρεσίες τηλεϊατρικής και ατομικά ενδυτά και φορητά επικοινωνούντα συστήματα για την παρακολούθηση και στήριξη των ασθενών, συστήματα τηλεσυμβουλευτικής (teleconsultation), πλατφόρμες ηλεκτρονικής συνταγογράφησης (ePrescribing) και ηλεκτρονικής παραπομπής (eReferral) κοκ. [68].
- **Άλλα:** μπορεί να υπάρχει πληθώρα άλλων Κλινικών ΠΣ τα οποία υποβοηθούν στις λειτουργίες μιας κλινικής όπως είναι η διαχείριση φαρμάκων ή η υποστήριξη ερευνητικού έργου (εξαγωγή και ανάλυση στατιστικών δεδομένων).

<u>Διοικητικά ΠΣ</u>

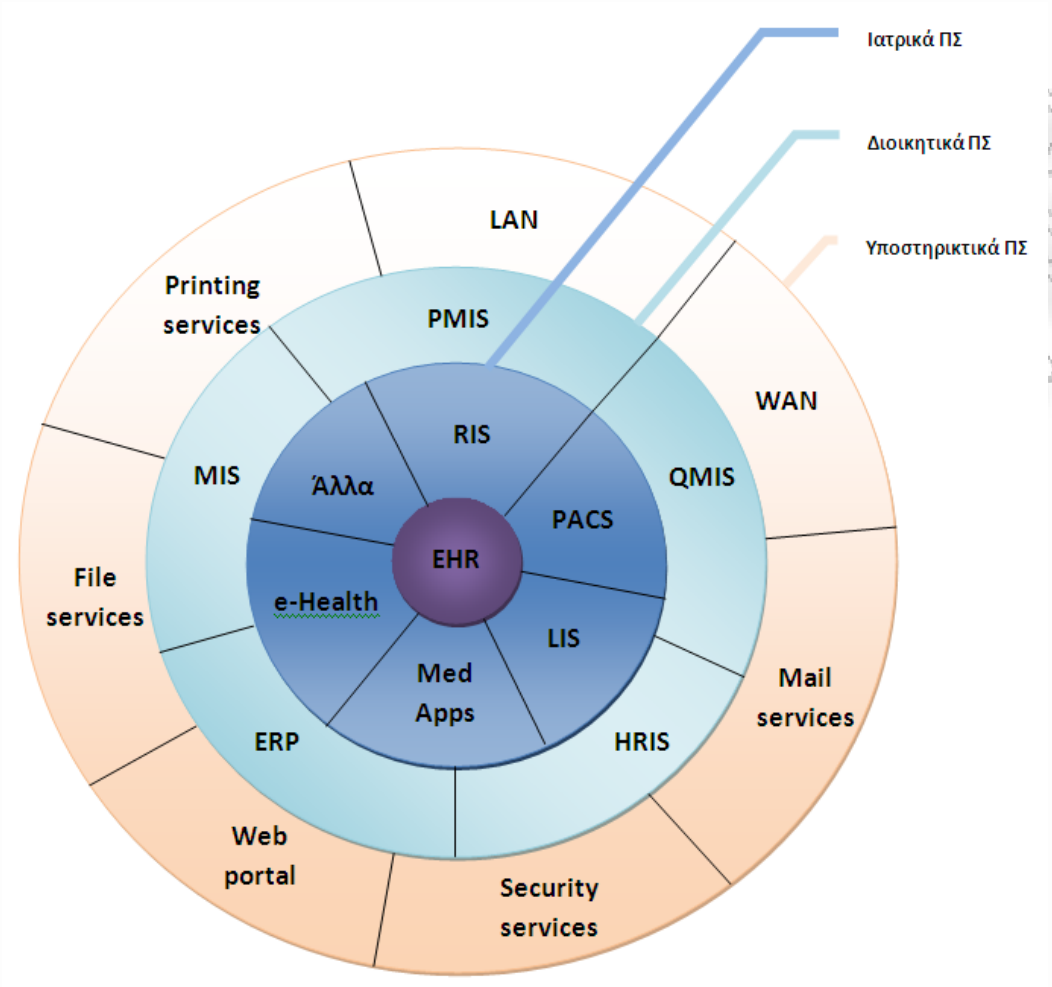
- **Payroll Management Information System (PMIS):** Είναι το ΠΣ το οποίο διαχειρίζεται τη μισθοδοσία του προσωπικού.
- **Human Resources Information System (HRIS):** Είναι το ΠΣ το οποίο χρησιμοποιείται για τη διαχείρισης ανθρωπίνων πόρων και μπορεί να περιλαμβάνει τη διαχείριση των προσωπικών δεδομένων του προσωπικού, την ωρομέτρηση της απασχόλησης, τον έλεγχο παρουσιών και αδειών, την αξιολόγηση της απόδοσης, την πρόσληψη νέου προσωπικού.
- **Quality Management Information System (QMIS):** Είναι το ΠΣ που υποβοηθά στη διαχείριση κινδύνου και στον σχεδιασμό πρόληψης και αντιμετώπισης ασυνήθιστων συμβάντων. Χρησιμοποιείται για την παρακολούθηση του συστήματος διαχείρισης ποιότητας και την παραγωγή αναφορών για την συνεχή βελτίωσή του.
- **Management Information System (MIS):** Είναι το ΠΣ το οποίο παρέχει τις απαραίτητες πληροφορίες σε κατάλληλη μορφή ώστε να βοηθά την εταιρική διαχείριση και τη λήψη αποφάσεων. Συνήθως επεξεργάζεται οικονομικές πληροφορίες συναρτήσει δεικτών μέτρησης της απόδοσης των επιχειρησιακών λειτουργιών.

- **Enterprise Resource Planning (ERP):** Είναι το ΠΣ το οποίο χρησιμοποιείται για τη διαχείριση των οικονομικών στοιχείων, λογαριασμών και συναλλαγών του οργανισμού. Είναι απαραίτητο για τη διαχείριση των εσόδων-εξόδων του οργανισμού, τη λειτουργία των υπηρεσιών λογιστηρίου και μπορεί να ενσωματώνει και άλλες λειτουργίες όπως η διαχείριση υλικού και προμηθειών.

Υποστηρικτικά ΠΣ

- **Intranet access or Local Area Network (LAN):** αφορά στον εξοπλισμό και τις υπηρεσίες οι οποίες εξυπηρετούν τη λειτουργία των τοπικών δικτύων.
- **Internet access or Wide Area Network (WAN):** αφορά στον εξοπλισμό και τις υπηρεσίες οι οποίες εξυπηρετούν τη λειτουργία και επικοινωνία με δίκτυα πέραν του τοπικού και με τον παγκόσμιο ιστό.
- **Printing services:** αφορά στον εξοπλισμό και τις υπηρεσίες που χρησιμοποιούνται για εκτυπωτικές εργασίες.
- **File services:** αφορά στον εξοπλισμό και τις υπηρεσίες που χρησιμοποιούνται για το διαμοιρασμό αρχείων.
- **Mail services:** αφορά στον εξοπλισμό και τις υπηρεσίες που χρησιμοποιούνται για τη διακίνηση μηνυμάτων ηλεκτρονικού ταχυδρομείου.
- **Security services:** αφορά στον εξοπλισμό και τις υπηρεσίες που χρησιμοποιούνται για τη διασφάλιση των διακινούμενων δεδομένων.
- **Web portal:** αφορά την ηλεκτρονική διαδικτυακή πύλη του οργανισμού μέσω της οποίας μπορεί να πραγματοποιείται η ενημέρωση του κοινού, η ανταλλαγή πληροφοριών και η πρόσβαση σε υπηρεσίες ηλεκτρονικής υγείας.

Τα παραπάνω ΠΣ ενός φορέα υγείας μπορεί να διασυνδέονται, να συνεργάζονται ή και να συγχωνεύονται μεταξύ τους έτσι ώστε πολλές φορές να συντελούν προς την κατεύθυνση της δημιουργίας ενός Ολοκληρωμένου Πληροφοριακού Συστήματος Υγείας (HIS-Hospital Information System).



Σχήμα 21: *Πληροφοριακά συστήματα τυπικού φορέα πρωτοβάθμιας υγείας*

6.3 Εργαλεία συλλογής δεδομένων

Για την συλλογή των απαραίτητων δεδομένων και πληροφοριών, με στόχο την εφαρμογή της μεθοδολογίας σχεδιασμού του πλάνου ανάκαμψης χρησιμοποιούνται κυρίως οι εξής ερευνητικές μέθοδοι-εργαλεία:

- **Βιβλιογραφική έρευνα**: έρευνα που αφορά πληροφορίες και βέλτιστες πρακτικές από μελέτες, βιβλία, διαδικτυακή έρευνα.
- **Συνέντευξη με πρόσωπα κλειδιά**: διενέργεια συνεντεύξεων από πρόσωπα σε εξειδικευμένες θέσεις εργασίας.
- **Αρχειακή έρευνα-ανασκόπηση**: έλεγχος έντυπων διαδικασιών, αποθηκευμένων δεδομένων και καταγεγραμμένων συμβάντων για εξαγωγή πληροφοριών και έλεγχο ιστορικότητας.

- **Παρατήρηση**: επιτόπια επίσκεψη σε συγκεκριμένους χώρους για τον έλεγχο λειτουργιών και διαδικασιών.
- **Ερωτηματολόγια**: χρήση ερωτηματολογίων με στοχευμένες ερωτήσεις για την εξαγωγή πληροφοριών.
- **Πρακτική εμπειρία**: χρήση εμπειρίας από εφαρμογή κοινών βέλτιστων πρακτικών

Ως προς την αξιολόγηση των δεδομένων γίνεται χρήση κυρίως ποιοτικών αναλύσεων με χρήση κλίμακας (καθόλου-λίγο-πολύ, χαμηλό-μέσο-υψηλό), λόγω της ευκολίας και της ταχύτητας εφαρμογής που προσφέρει έναντι της ποσοτικής ανάλυσης.

6.4 Αξιολόγηση υπάρχουσας κατάστασης

6.4.1 Προκαταρκτικός έλεγχος

Μια από τις πρωταρχικές ενέργειες που πρέπει να πραγματοποιηθούν αποτελεί η αξιολόγηση του επιπέδου προστασίας των ΠΣ του οργανισμού καθώς και της επάρκειας των μέτρων ανάκαμψης, εφόσον αυτά υφίστανται, μέσα από μια αρχική και γενική επισκόπηση.

Στόχος είναι η αποκάλυψη των αδύνατων σημείων του οργανισμού σχετικά με τη δυνατότητα ανάκαμψης από καταστροφές αλλά και η ανάδειξη της αναγκαιότητας σχεδιασμού και εφαρμογής ενός ολοκληρωμένου πλάνου αντιμετώπισης-ανάκαμψης από καταστροφές.

Για να το επιτύχουμε αυτό χρησιμοποιείται ένα σύνολο από 10 ερωτήσεις-σημεία ελέγχου, οι οποίες επιχειρούν να διερευνήσουν την ύπαρξη των βασικότερων συστατικών, όπως περιγράφηκαν παραπάνω, που απαιτούνται για τον αποτελεσματικού σχεδιασμό ανάκαμψης από καταστροφές. Ως κλίμακα αξιολόγησης για κάθε σημείο ελέγχου χρησιμοποιείται η παρακάτω:

Κλίμακα Βαθμού Ικανοποποίησης	
1	**Δεν ικανοποιείται**
2	**Μερική ικανοποίηση**
3	**Ικανοποιείται**

Το αποτέλεσμα του ελέγχου, και κατά συνέπεια η διερεύνηση της αποτελεσματικότητας της αντιμετώπισης καταστροφών, ταξινομείται ως εξής:

Κατάσταση	
✗	**Βαθμός: (10-20) Μη ικανοποιητική**
!	**Βαθμός: (20-25) Μερική ικανοποίηση (Χρήζει βελτίωσης)**
✓	**Βαθμός: (26-30) Ικανοποιητική**

Σύμφωνα με τα παραπάνω, παρατίθεται το παρακάτω ερωτηματολόγιο με την ενδεικτική αξιολόγηση που προκύπτει για τη παρούσα μελέτη περίπτωσης:

Α/Α	Σημείο Ελέγχου	Βαθμός Ικανοποίησης	Παρατηρήσεις
1	Υπάρχει πολιτική για Σχέδιο Ανάκαμψης από Καταστροφές στον οργανισμό; Εκφράζεται με επίσημο τρόπο από τη Διοίκηση;	2	Υπάρχει πολιτική ασφαλείας κατ' έφαρμογή των απαιτήσεων του ISO27001, χωρίς όμως να γίνεται ιδιαίτερη αναφορά σε Σχέδιο Ανάκαμψης από Καταστροφές.
2	Έχουν αναγνωριστεί οι κρίσιμες λειτουργίες του οργανισμού και τα ΠΣ που τις εξυπηρετούν; Έχουν προτεραιοποιηθεί ακολουθώντας μια επίσημη διαδικασία;	2	Έχει πραγματοποιηθεί μια αρχική αποτίμηση και αξιολόγηση των ΠΣ και των κινδύνων, χωρίς όμως να υπάρχει ξεκάθαρη προτεραιοποίηση.
3	Έχουν αναγνωριστεί οι πόροι οι οποίο απαρτίζουν το κάθε ΠΣ; Τηρείται η συστηματική καταγραφή τους;	2	Έχει πραγματοποιηθεί μερική καταγραφή των πόρων, χωρίς να περιλαμβάνει όλα τα συστατικά τους όπως τους εμπλεκόμενους ανθρώπους και προμηθευτές.
4	Έχουν ληφθεί προληπτικά μέτρα; Δοκιμάζονται για την αποτελεσματικότητά τους σε τακτά χρονικά διαστήματα;	3	Εφαρμόζονται προληπτικά μέτρα, τα οποία και δοκιμάζονται.
5	Υπάρχουν καθορισμένες στρατηγικές για την πρόληψη και αντιμετώπιση των επιπτώσεων ενδεχόμενων καταστροφών που	2	Υπάρχουν, χωρίς όμως συστηματική εφαρμογή.
6	Έχουν τεθεί συγκεκριμένοι στόχοι για την ανάκαμψη των ΠΣ;	2	Υπάρχουν στόχοι, χωρίς όμως να είναι αποτέλεσμα κάποιας τεκμηριωμένης και συστηματικής διαδικασίας.
7	Υπάρχουν εναλλακτικές εγκαταστάσεις διαμορφωμένες κατάλληλα και με διαθέσιμο τον εξοπλισμό που απαιτείται για την ανάκαμψη;	1	Υπάρχουν εναλλακτικές εγκαταστάσεις, χωρίς κατάλληλη διαμόρφωση και εξοπλισμό.
8	Υπάρχει οργανωμένο Σχέδιο Ανάκαμψης από Καταστροφές; Είναι άρτια συντεταγμένο περιγράφοντας ρόλους και αρμοδιότητες τόσο σε οργανωτικό όσο και σε λειτουργικό επίπεδο; Περιγράφει με επάρκεια τις ενέργειες που πρέπει να πραγματοποιηθούν και τις διαδικασίες που πρέπει να ακολουθηθούν; Περιλαμβάνει όλες τις απαραίτητες πληροφορίες; (αρχεία,οδηγίες,λίστες,εντυπα)	2	Υπάρχει Σχέδιο Ανάκαμψης, το οποίο όμως παρουσιάζει σημαντικές ελλείψεις.
9	Έχει δοκιμαστεί πρόσφατα η αποτελεσματικότητα του Σχεδίου Ανάκαμψης από Καταστροφές; (εντός των τελευταίων 12 μηνών)	1	Δεν πραγματοποιούνται συστηματικές δοκιμές.
10	Το Σχέδιο Ανάκαμψης επικαιροποιείται τακτικά; Υπάρχει συγκεκριμένο πλάνο επικαιροποίησης που ακολουθείται;	1	Δεν υπάρχει συγκεκριμένο πλάνο επικαιροποίησης.
	Συνολική Βαθμολογία: ✗	**18**	

Πίνακας 8: *Ερωτηματολόγιο προκαταρκτικού ελέγχου δυνατοτήτων ανάκαμψης*

6.4.2 Αναγνώριση και αξιολόγηση πιθανότητας καταστροφών

Σε αυτό το στάδιο επιχειρείται η αναγνώριση των πιθανών καταστροφών και των επιπτώσεων που μπορεί να έχουν στα ΠΣ του οργανισμού. Γίνεται αξιολόγηση τόσο σε γενικό επίπεδο, σε δεδομένα που αφορούν τη συχνότητα εμφάνισης καταστροφών στον ελλαδικό χώρο, όσο και σε ειδικό, σε δεδομένα από καταγεγραμμένα παρόμοια περιστατικά στον οργανισμό ή την εγγύς περιοχή. Για την εκτίμηση τόσο της πιθανότητας εμφάνισης όσο και των ενδεχόμενων επιπτώσεων γίνεται χρήση ποιοτικής κλίμακας ως εξής:

Για την πιθανότητα ((P)ossibility) εμφάνισης μιας καταστροφής:

Βαθμός	Πιθανότητα (P)	Περιγραφή
1	ΠΟΛΥ ΧΑΜΗΛΗ	Εμφάνιση σχεδόν ποτέ
2	ΧΑΜΗΛΗ	Εμφάνιση σπάνια (μεμονωμένα περιστατικά και σε βάθος χρόνου)
3	ΜΕΣΗ	Αυξημένος κίνδυνος εμφάνισης (παρόλο που μπορεί να μην έχει αναφερθεί σχετικά πρόσφατο περιστατικό, κρίνεται πιθανή η εμφάνισή του)
4	ΥΨΗΛΗ	Εμφάνιση συχνά (μια φορά το χρόνο)
5	ΠΟΛΥ ΥΨΗΛΗ	Εμφάνιση πολύ συχνά (περισότερο από μια φορά το χρόνο)

Για την εκτίμηση των πιθανών επιπτώσεων ((I)mpact) στα ΠΣ:

Βαθμός	Επίπτωση (I)	Περιγραφή
1	ΧΑΜΗΛΗ	Σύντομη διακοπή ΠΣ
2	ΜΕΣΗ	Μερική καταστροφή ΠΣ
3	ΥΨΗΛΗ	Πλήρης καταστροφή ΠΣ

Για κάθε καταστροφή υπολογίζεται το επίπεδο επικινδυνότητας ((R)isk) για τον οργανισμό, ως το γινόμενο της πιθανότητας εμφάνισης με τις ενδεχόμενες συνέπειες:

$$R=P*I$$

Προκύπτει έτσι μια κλίμακα από το 1-15, η οποία χρησιμοποιείται για την προτεραιοποίηση των καταστροφών που πρέπει να ληφθούν υπόψη κατά τη λήψη μέτρων, είτε προληπτικών είτε αντιμετώπισης-ανάκαμψης. Ως αποτέλεσμα προκύπτει ο Πίνακας 9.

6.4.3 Αξιολόγηση προληπτικών μέτρων

Για κάθε μια από τις παραπάνω πιθανές καταστροφές καταγράφονται τα προληπτικά μέτρα που εφαρμόζονται ήδη από τον οργανισμό και γίνεται ποιοτική αξιολόγηση της επάρκειας τους ως προς τη δυνατότητα ανίχνευσης, αντιμετώπισης και πρόληψης των καταστροφών με χρήση της παρακάτω κλίμακας:

Βαθμός	Επάρκεια	Περιγραφή
1	ΧΑΜΗΛΗ	Παρέχουν κυρίως δυνατότητα έγκαιρης ανίχνευσης
2	ΜΕΣΗ	Παρέχουν δυνατότητες μερικής αντιμετώπισης των επιπτώσεων
3	ΥΨΗΛΗ	Παρέχουν δυνατότητες πρόληψης, αποτρέποντας την εμφάνιση της αιτίας

Όπως ήταν αναμενόμενο, και σύμφωνα με τα όσα προκύπτουν από τον Πίνακα 9, υπάρχουν καταστροφές που δεν μπορούν να αντιμετωπιστούν με μέτρα προληπτικού χαρακτήρα. Στην περίπτωση που εξετάζουμε, αυτές είναι κυρίως όσες οφείλονται σε φυσικά αίτια (σεισμοί, πλημμύρες, πυρκαγιές) και σε τεχνολογικά (δυσλειτουργία εξοπλισμού, λάθη συστήματος). Για τις καταστροφές αυτές το μόνο μέτρο αντιμετώπισης φέρεται να είναι ένα σχέδιο ανάκαμψης.

Είδος Καταστροφής	Πιθανότητα Εμφάνισης (P)	Επιπτώσεις (I)	Επικινδυνότητα (R=P*I)	Προληπτικά Μέτρα	Επάρκεια Προληπτικών Μέτρων	Παρατηρήσεις
Φυσικές καταστροφές						
σεισμοί	3	3	9			
πυρκαγιές	3	3	9	χρήση ανιχνευτών, συστήματα πυρόσβεσης	2	
πλημμύρες	3	3	9	χρήση ανιχνευτών	1	
τυφώνες	1	2	2			
κατολισθήσεις	1	3	3			
ηφαίστεια	1	3	3			
ακραία καιρικά φαινόμενα	2	2	4			
Ανθρώπινα λάθη						
ατυχήματα	3	2	6	εφαρμογή OHSAS 18001:2007	3	
διαρροή επικίνδυνων ουσιών/μόλυνση	3	1	3	εφαρμογή ISO14001:2004	3	
Ανθρώπινος δόλος:						
τρομοκρατικές ενέργειες	1	3	3	υπηρεσίες φύλαξης	3	
hacking	3	2	6	εξοπλισμός προστασίας	3	
κλοπή υλικού/δεδομένων	4	2	8	υπηρεσίες φύλαξης, συστήματα έλεγχος πρόσβασης, εφαρμογή ISO27001:2005	3	
εξεγέρσεις/κοινωνικές αναταραχές	1	1	1	υπηρεσίες φύλαξης	1	
Τεχνολογικά:						
δυσλειτουργία εξοπλισμού	5	2	10	εφεδρικά συστήματα	2	
λάθη συστήματος	5	2	10	αντίγραφα ασφαλείας	2	
πτώση/απώλεια ενέργειας	5	1	5	εφεδρικά συστήματα (UPS, H/Z)	3	
απώλεια επικοινωνιών	5	1	5			
Άλλες						
πανδημίες	2	1	2			
οικονομική κατάρρευση	2	1	2			

Πίνακας 9: *Αξιολόγηση πιθανών καταστροφών και προληπτικών μέτρων*

6.4.4 Σύνοψη συμπερασμάτων

Τα αποτελέσματα των παραπάνω αξιολογήσεων μπορούμε να τα συνοψίσουμε και να τα εκφράσουμε με την παρακάτω μήτρα SWOT [69], η οποία αποκαλύπτει τα βασικά σημεία σχετικά με την δυνατότητα του οργανισμού να εφαρμόσει αποτελεσματικά ένα Σχέδιο Ανάκαμψης από Καταστροφές των ΠΣ του. Τα σημεία αυτά αφορούν είτε στο εσωτερικό περιβάλλον, που αποτελούνται από πλεονεκτήματα και αδυναμίες, είτε στο εξωτερικό περιβάλλον, που αποτελούνται από ευκαιρίες και απειλές. Όπου:

- Πλεονεκτήματα, θεωρούνται τα δυνατά σημεία του οργανισμού σχετικά με τη δυνατότητα ανάκαμψης από καταστροφές, τα οποία θα πρέπει να αξιοποιηθούν και να διατηρηθούν.
- Αδυναμίες, θεωρούνται τα αδύνατα σημεία του οργανισμού σχετικά με τη δυνατότητα ανάκαμψης από καταστροφές, τα οποία θα πρέπει είτε να διορθωθούν είτε να βελτιωθούν.
- Ευκαιρίες, θεωρούνται τα στοιχεία εκείνα του οργανισμού και του εξωτερικού περιβάλλοντος, τα οποία μπορούν να συνεισφέρουν θετικά και θα πρέπει να αξιοποιηθούν κατά τον επαναπροσδιορισμό της στρατηγικής της ανάκαμψης.

- Απειλές, θεωρούνται τα στοιχεία εκείνα του οργανισμού και του εξωτερικού περιβάλλοντος, τα οποία απειλούν την επιτυχή ανάκαμψη και θα πρέπει να λαμβάνονται υπόψη κατά τον σχεδιασμό και να αντιμετωπίζονται στο μέτρο του δυνατού.

	ΔΥΝΑΤΑ ΣΗΜΕΙΑ (STRENGTHS)	ΑΔΥΝΑΤΑ ΣΗΜΕΙΑ (WEAKNESSES)
ΕΣΩΤΕΡΙΚΟ ΠΕΡΙΒΑΛΛΟΝ	Υπάρχουν βασικές διαδικασίες, απαραίτητες για την ανάκαμψη, που τηρούνται στα πλαίσια εφαρμογής του προτύπου ISO270001.	Το παρόν ΣΑΚ δεν αποτελεί συντεταγμένο σχέδιο και παρατηρούνται οργανωσιακά ελλείματα.
	Υπάρχουν ιδιόκτητες εναλλακτικές εγκαταστάσεις.	Δεν πραγματοποιούνται οι απαραίτητες δοκιμές και δεν υπάρχει συστηματική επικαιροποίηση.
	ΕΥΚΑΙΡΙΕΣ (OPPORTUNITIES)	**ΑΠΕΙΛΕΣ (THREATS)**
ΕΞΩΤΕΡΙΚΟ ΠΕΡΙΒΑΛΛΟΝ	Εμπειρία και εξοικείωση του προσωπικού στην τήρηση διαδικασιών, λόγω εφαρμογής διαφόρων προτύπων ποιότητας.	Έλλειψεις προσωπικου.
	Ύπαρξη νέων τεχνολογιών και μέσων ανάκαμψης σε προσιτή τιμή.	Έλλειψεις οικονομικών πόρων.

Πίνακας 10: *Μήτρα ανάλυσης SWOT δυνατότητας εφαρμογής ΣΑΚ*

Η παραπάνω μήτρα SWOT παρουσιάζει τους βασικότερους άξονες, πάνω στους οποίους θα πρέπει να κινηθεί ο στρατηγικός σχεδιασμός της ανάκαμψης των ΠΣ από καταστροφές.

6.5 Εφαρμογή μεθοδολογίας σχεδιασμού πλάνου

Σε αυτό το κεφάλαιο θα επιχειρηθεί η εφαρμογή της μεθοδολογίας για τον σχεδιασμό του πλάνου ανάκαμψης όπως αυτή παρουσιάζεται στο §4.

6.5.1 Δήλωση πολιτικής

Πρώτο βήμα αποτελεί ο καθορισμός της πολιτικής του οργανισμού σχετικά με την ανάκαμψη των ΠΣ του από καταστροφή. Προτείνεται η υιοθέτηση ενός πρότυπου κειμένου, το οποίο να δηλώνει τη σχετική δέσμευση του οργανισμού, ως παρακάτω:

« Η Διοίκηση του οργανισμού όντας ευαισθητοποιημένη για τους κινδύνους από απρόβλεπτα γεγονότα και ακραίες καταστάσεις που μπορούν να επηρεάσουν τη λειτουργία

του και το επίπεδο παροχής υπηρεσιών, δεσμεύεται να λάβει κάθε απαραίτητο μέτρο για τον περιορισμό των επιπτώσεων.

Για το λόγο αυτό εγκρίνει την κατάρτιση και εφαρμογή Σχεδίου Ανάκαμψης από Καταστροφές (ΣΑΚ) για τα Πληροφοριακά Συστήματα του οργανισμού. Το Σχέδιο αυτό αναγνωρίζει τις κρίσιμες λειτουργίες του οργανισμού και τα πληροφοριακά συστήματα που τις υποστηρίζουν, περιγράφει διαδικασίες και στρατηγικές απαραίτητες για την αντιμετώπιση καταστροφών και αναθέτει ρόλους και αρμοδιότητες. Το προσωπικό του οργανισμού είναι εκπαιδευμένο κατάλληλα για την επιτυχή εφαρμογή του. Το Σχέδιο ελέγχεται, δοκιμάζεται και επικαιροποιείται σε τακτά χρονικά διαστήματα, καθώς και εκτάκτως μετά από κάθε αλλαγή που μπορεί να επηρεάσει την αποτελεσματικότητά του.»

6.5.2 Ανάλυση επιχειρησιακών επιπτώσεων

Στο στάδιο αυτό πραγματοποιείται η ανάλυση των επιπτώσεων, από την ενδεχόμενη καταστροφή των ΠΣ. Οι επιπτώσεις αυτές αξιολογούνται και στη συνέχεια προτεραιοποιείται η ανάκτηση των πόρων που απαιτούνται για την άμεση αποκατάσταση των ΠΣ.

Για την αξιολόγηση των επιπτώσεων επιλέγεται η χρήση κυρίως της ποιοτικής ανάλυσης ώστε να επιτευχθεί οικονομία χρόνου αλλά και μεγαλύτερη προσαρμοστικότητα της ίδιας της διαδικασίας αξιολόγησης σε άλλους ομοειδής οργανισμούς.

- ***Αναγνώριση και αξιολόγηση κρίσιμων λειτουργιών***

Κατά την αναγνώριση των κρίσιμων λειτουργιών και την αξιολόγηση των διαφορετικών επιπτώσεων που μπορεί να έχει μια ενδεχόμενη διακοπή τους για τον οργανισμό γίνεται χρήση ερωτηματολογίου το οποίο συμπληρώνεται από κάθε οργανωτική μονάδα του οργανισμού (βλέπε ΠΑΡΑΡΤΗΜΑ).

Στόχος του ερωτηματολογίου είναι:

- Η αναγνώριση όλων των λειτουργιών του οργανισμού που βασίζονται σε ΠΣ
- Η αναγνώριση των ΠΣ στα οποία βασίζεται κάθε λειτουργία

- Η εκτίμηση του μέγιστου ανεκτού χρόνου συνέχισης των λειτουργιών (MTD) χωρίς τα απαραίτητα ΠΣ, και μετά το πέρας του οποίου αναμένεται να εμφανιστούν οι επιπτώσεις
- Η αναγνώριση και αξιολόγηση των επιπτώσεων μετά το πέρας του παραπάνω χρόνου
- Η αναγνώριση του μέγιστου ανεκτού χρόνου απώλειας δεδομένων (RPO)
- Η αναγνώριση τυχών αλληλεξαρτήσεων ορισμένων λειτουργιών

Για τη διευκόλυνση της συμπλήρωσης του ερωτηματολογίου καθορίζουμε:

Α. την κλιμάκωση του χρόνου MTD σε τέσσερις κατηγορίες, ως εξής:

- ≤ 4 ώρες
- ≤ 1 ημέρα
- ≤ 3 ημέρες
- ≤ 1 εβδομάδα

Β. την κλιμάκωση του χρόνου RPO σε τρείς κατηγορίες, ως εξής:

- ≤ 1 ώρα
- ≤ 1 ημέρα
- ≤ 1 εβδομάδα

Γ. Αντίστοιχα για την αξιολόγηση των επιπτώσεων παρατίθεται ο Πίνακας 11, ο οποίος περιλαμβάνει την προτεινόμενη κλίμακα ποιοτικής αξιολόγησης ανά θεματική κατηγορία επίπτωσης. Αυτός ο πίνακας βοηθά στο χαρακτηρισμό και την κατηγοριοποίηση της κάθε επίπτωσης ως χαμηλής, μέσης ή υψηλής.

Επιπτώσεις δυσλειτουργίας ΠΣ	ΧΑΜΗΛΗ	ΜΕΣΗ	ΥΨΗΛΗ
Νομικές-Κανονιστικές	Δεν προκύπτει αθέτηση νομικών ή κανονιστικών υποχρεώσεων. Δεν υπάρχει κίνδυνος για πρόστιμα. Δεν υπάρχει κίνδυνος για αγωγές και νομικές κυρώσεις. Δεν προκύπτει αιτία για διεξαγωγή εισαγγελικής έρευνας. (συνήθως αφορούν σε απλά δεδομένα)	Προκύπτει αθέτηση κυρίως κανονιστικών υποχρεώσεων. Κίνδυνος για ελάχιστα πρόστιμα. Περιορισμένος κίνδυνος για αγωγές και νομικές κυρώσεις. Δεν προκύπτει αιτία για διεξαγωγή εισαγγελικής έρευνας, αλλά μπορεί να υπάρξει κλήση για απολογία από επίσημη αρχή. (συνήθως αφορούν σε προσωπικά δεδομένα)	Προκύπτει αθέτηση νομικών ή κανονιστικών υποχρεώσεων. Υπάρχει κίνδυνος για υψηλά πρόστιμα. Υπάρχει κίνδυνος για αγωγές και νομικές κυρώσεις. Προκύπτει αιτία για διεξαγωγή εισαγγελικής έρευνας. (συνήθως αφορούν σε ευαίσθητα δεδομένα)
Οικονομικές	Ελάχιστη εως ανύπαρκτη στιγμιαία οικονομική απώλεια. Ελάχιστες επιπτώσεις στο λειτουργικό κόστος του οργανισμού. Ελάχιστη εως μηδενική απώλεια εσόδων. Αμελητέα επίδραση στα έσοδα του οργανισμού. Καμία επίπτωση στην οικονομική σταθερότητα.	Στιγμιαία οικονομική απώλεια. Αισθητές επιπτώσεις στο λειτουργικό κόστος του οργανισμού. Μερική απώλεια εσόδων. Αισθητή επίδραση στα έσοδα του οργανισμού.Αμελητέα επίπτωση στην οικονομική σταθερότητα.	Μεγάλη στιγμιαία οικονομική απώλεια. Έντονες επιπτώσεις στο λειτουργικό κόστος του οργανισμού. Υψηλή απώλεια εσόδων. Σημαντική επίπτωση στην οικονομική σταθερότητα του οργανισμού.
Λειτουργικές-Παραγωγικές	Ελάχιστη εως καθόλου επίπτωση στην παραγωγικότητα του οργανισμού. Χαμηλή εξάρτηση λειτουργιών από ΠΣ. Δυνατότητα απρόσκοπτης συνέχισης των λειτουργιών του οργανισμού με εναλλακτικό τρόπο (χειροκίνητα, χειρόγραφα).	Μερική επίπτωση στην παραγωγικότητα του οργανισμού. Υψηλή εξάρτηση λειτουργιών από ΠΣ. Δυνατότητα συνέχισης των λειτουργιών του οργανισμού με εναλλακτικό τρόπο (χειροκίνητα, χειρόγραφα) αλλά με υψηλή καθυστέρηση.	Καθοριστική επίπτωση στην παραγωγικότητα του οργανισμού. Υψηλή εξάρτηση λειτουργιών από ΠΣ. Αδυναμία συνέχισης των λειτουργιών του οργανισμού σε ανεκτό επίπεδο.
Υπόληψη-Υστεροφημία	Ελάχιστες επιπτώσεις. Απαιτειται ελάχιστη εως καθόλου προσπάθεια ανάκτησής της. Ελάχιστες ως μηδενικές απώλειες πελατών.	Μέτριες επιπτώσεις. Απαιτείται προσπάθεια για την ανάκτησή της. Μερική απώλεια πελατών.	Υψηλές επιπτώσεις. Η ανάκτησή της μπορεί να είναι μη αναστρέψιμη. Μαζική απώλεια πελατών.
Υγιεινή & Ασφάλεια	Δεν υπάρχει αξιόλογος κίνδυνος για τη ζωή, υγιεινή και ασφάλεια πελατών και προσωπικού.	Υπάρχει έμμεσος και περιορισμένος κίνδυνος για τη ζωή, υγιεινή και ασφάλεια πελατών και προσωπικού.	Υπάρχει άμεσος και ορατός κίνδυνος για τη ζωή, υγιεινή και ασφάλεια πελατών και προσωπικού.
Άλλες	Χαμηλή επίπτωση	Μέση επίπτωση	Υψηλή επίπτωση

Πίνακας 11: *Κλίμακα αξιολόγησης επιπτώσεων*

Μετά τη συμπλήρωση των ερωτηματολογίων ακολουθεί η επεξεργασία των δεδομένων που προέκυψαν ώστε να εκτιμηθεί η κρισιμότητα των λειτουργιών του οργανισμού. Για να το επιτύχουμε αντιστοιχούμε τον χαρακτηρισμό των επιπτώσεων από χαμηλή, μέση, υψηλή στην ποσοτική κλίμακα 1, 2, 3 κατά αντιστοιχία.

Κάνοντας την παραδοχή ότι οι επιπτώσεις είναι ισοβαρής άσχετα από την θεματική κατηγορία στην οποία ανήκουν μπορούμε, αθροίζοντας τις επιμέρους αξιολογήσεις, να εξάγουμε την κρισιμότητα των λειτουργιών με τη μορφή ενός δείκτη κρισιμότητας (Criticality Indicator - CI) ο οποίος στο συγκεκριμένο παράδειγμα κυμαίνεται στη κλίμακα από 5-15.

Έχουμε πλέον διερευνήσει για κάθε λειτουργία του οργανισμού το δείκτη κρισιμότητας (CI), τον μέγιστο ανεκτό χρόνο δυσλειτουργίας (MTD) και τον μέγιστο ανεκτό χρόνο απώλειας δεδομένων (RPO) σύμφωνα με τις ανάγκες και τις απαιτήσεις κάθε οργανωτικής μονάδας. Τα αποτελέσματα αυτά φαίνονται συγκεντρωτικά στον Πίνακα 12.

Οργανωτικές Μονάδες	Λειτουργίες ανά Μονάδα	ΚΛΙΝΙΚΑ ΠΣ					ΔΙΟΙΚΗΤΙΚΑ ΠΣ					ΥΠΟΣΤΗΡΙΚΤΙΚΑ ΠΣ							Επιπτώσεις από δυσλειτουργία-απώλεια						Μέγιστος ανεκτός χρόνος δυσλειτουργίας(MTD				Μέγιστος ανεκτός χρόνος απώλειας δεδομένων(RPO)			Εξάρτηση από άλλες λειτουργίες	Παρατηρήσεις
		EHR	LIS	RIS/PACS	Medical Applications	e-Health	PMIS	HRIS	QMIS	MIS	ERP	mail services	file services	printing services	web-portal	internet access (WAN)	intranet access (LAN)	Security services	Νομικές-Κανονιστικές	Οικονομικές	Λειτουργικές-Παραγωγικές	Υπόληψη-Υστεροφημία	Υγιεινή & Ασφάλεια	Δείκτης Κρισιμότητας (CI)	4Ω	1H	3H	1E	1Ω	1H	1E		
Κλινική Φροντίδα	Υπηρεσιες υγείας	X		X	X	X								X		X	X		Y	Y	Y	Y	Y	15		X			X				
Ιατρικές Απεικονίσεις	Υπηρεσιες υγείας			X										X			X		Y	Y	Y	Y	Y	15		X			X				
Αποκατάσταση-Αποθεραπεία	Υπηρεσιες υγείας	X			X	X								X			X		Y	Y	Y	Y	Y	15		X			X				
Βιοπαθολογικά Εργαστήρια	Διενέργεια εργαστηριακών εξετάσεων		X											X			X		Y	Y	Y	Y	Y	15		X			X				
Διοικητικές Υπηρεσίες	Διαχείριση Ανθρωπίνου Δυναμικού						X	X				X	X	X			X		M	X	Y	X	X	8				X			X		
	Γραμματειακή υποστήριξη											X	X	X	X		X		X	X	M	X	X	6				X			X		
	Κλείσιμο ραντεβού	X										X			X		X		M	Y	M	M	X	10		X			X				
Οικονομικές Υπηρεσίες	Σχεδιασμός-Εκτέλεση προϋπολογισμού									X	X		X	X			X		Y	Y	M	X	X	10				X			X		
	Έκδοση μισθοδοσίας						X							X			X		X	X	X	X	X	5				X			X		
	Υπηρεσίες Λογιστηρίου (Τιμολόγηση)										X			X			X		Y	Y	M	M	X	11			X			X			
	Προμήθεια και διαχείριση υλικού										X	X					X		M	X	X	M	M	8				X			X		
Υπηρεσίες Πληροφορικής	Υποστήριξη ΠΣ												X	X		X	X		M	M	Y	X	M	10		X					X		
	Ασφάλεια ΠΣ-Πληροφοριών																X	X	Y	X	X	Y	M	12		X				X			
Υπηρεσίες Βιοϊατρικής Τεχνολογίας	Υποστήριξη Βιοιατρικού εξοπλισμού								X			X	X			X	X		M	X	X	M	M	8			X				X		
Τεχνικές Υπηρεσίες	Υποστήριξη Υποδομών								X			X	X			X	X		M	X	X	X	M	7				X			X		
Υπηρεσίες Ολικής Ποιότητας	Έλεγχος Συστήματος Ποιότητας								X								X		M	X	X	M	M	8				X			X		
Νομικές Υπηρεσίες	Νομικές Υπηρεσίες												X				X		M	X	X	X	X	6				X			X		
Υπηρεσίες Εσωτερικού Ελέγχου	Εσωτερικός Έλεγχος								X				X				X	X	M	x	x	X	X	6				X			X		

Πίνακας 12: *Σύνοψη αποτελεσμάτων ανάλυσης επιχειρησιακών επιπτώσεων*

- ***Αντιστοίχιση λειτουργιών με ΠΣ και προτεραιοποίηση ανάκαμψης***

Παρατηρούμε ότι κατόπιν και της αντιστοιχίας των λειτουργιών του οργανισμού με τα απαραίτητα ΠΣ (Πίνακας 12), μπορούμε κατά συνέπεια να αντιστοιχίσουμε και τους σχετικούς δείκτες (CI, MTD, RPO) σε αυτά τα ΠΣ. Σε περίπτωση που σε κάποιο ΠΣ αντιστοιχούν περισσότερες τιμές για κάθε δείκτη, επιλέγουμε αυτόν που δηλώνει την υψηλότερη απαίτηση, ήτοι:

- Για τον CI, τη μεγαλύτερη τιμή
- Για το MTD, τη μικρότερη
- Για το RPO, τη μικρότερη

Με τον τρόπο αυτό μπορούμε πλέον να εξάγουμε την κρισιμότητα (CI) και τις απαιτήσεις (MTD, RPO) για τα ΠΣ και να τα ιεραρχήσουμε βάσει αυτών λαμβάνοντας υπόψη πρωτίστως την τιμή του δείκτη MTD και δευτερευόντως την τιμή του CI. Βάσει αυτών προκύπτει η παρακάτω ταξινόμηση, η οποία υποδεικνύει και την προτεραιότητα βάσει της οποίας θα πρέπει να σχεδιαστεί η ανάκαμψή τους:

Α/Α	ΠΛΗΡΟΦΟΡΙΑΚΟ ΣΥΣΤΗΜΑ	MTD	CI	RPO
1	**Intranet (LAN)**	1H	15	1H
2	**printing services**	1H	15	1H
3	**EHR**	1H	15	1H
4	**Internet (WAN)**	1H	15	1H
5	**RIS/PACS**	1H	15	1H
6	**e-Health**	1H	15	1H
7	**LIS**	1H	15	1H
8	**MED APPS**	1H	15	1H
9	**security services**	1H	12	1H
10	**file services**	1H	10	1E
11	**mail services**	1H	10	1H
12	**web portal**	1H	10	1E
13	**ERP**	3H	11	1H
14	**QMIS**	3H	8	1E
15	**MIS**	1E	10	1E
16	**HRIS**	1E	8	1E
17	**PMIS**	1E	5	1E

Πίνακας 13: *Προτεραιοποίηση και απαιτήσεις ανάκαμψης ΠΣ*

- ***Αναγνώριση πόρων ΠΣ και καθορισμός απαιτήσεων ανάκαμψης***

Έχοντας καθορίσει τις απαιτήσεις των λειτουργιών του οργανισμού καταφέραμε να καθορίσουμε και τις απαιτήσεις των ΠΣ που τις υποστηρίζουν. Απομένει λοιπόν να καθοριστούν και οι απαιτήσεις των αντίστοιχων πόρων που απαρτίζουν το κάθε ΠΣ. Πρωταρχικό μέλημα αποτελεί η αναγνώριση και καταγραφή αυτών των πόρων (άνθρωποι-εγκαταστάσεις- τεχνολογίες-δεδομένα-διαδικασίες-προμηθευτές) για κάθε ΠΣ, το οποίο μπορεί να επιτευχθεί με τη συμπλήρωση κατάλληλης αναγνωριστικής καρτέλας (βλέπε ΠΑΡΑΡΤΗΜΑ-ΣΑΚ:Έντυπο ISCPs). Η καρτέλα αυτή συμπληρώνεται από το εξειδικευμένο προσωπικό (τεχνικό, διοικητικό) το οποίο ασχολείται με τα εν λόγω ΠΣ (συνήθως από τις Υπηρεσίες Πληροφορικής).

Βάσει του δείκτη MTD κάθε ΠΣ πρέπει να καθοριστεί ο επιδιωκόμενος χρόνος ανάκτησης (RTO) για κάθε πόρο, με τέτοιο τρόπο ώστε το σύνολο των RTO των πόρων που απαρτίζουν το εκάστοτε ΠΣ, να μην ξεπερνούν συνδυαστικά τον συνολικό χρόνο MTD του ΠΣ.

6.5.3 Καθορισμός προληπτικών ενεργειών

Η ύπαρξη προληπτικών μέτρων έχει ήδη εξετασθεί στην §6.4.3. Σε κάθε περίπτωση προτείνεται η εφαρμογή αναγνωρισμένων προτύπων για τη διασφάλιση των ΠΣ ενός οργανισμού, όπως χαρακτηριστικά αποτελεί το Σύστημα Διαχείρησης Ασφάλειας Πληροφοριών κατά ISO 27001:2005 και τα μέτρα που προτείνονται από το ISO 27002:2005.

6.5.4 Επιλογή Στρατηγικών

Για την αποτελεσματική χάραξη της ακολουθούμενης στρατηγικής, όσον αφορά το σχεδιασμό ανάκαμψης από καταστροφές των ΠΣ, θα πρέπει αρχικά να αποφασιστεί ο επιδιωκόμενος χρόνος ανάκαμψης και το διατιθέμενο οικονομικό ποσό. Βάσει αυτών των απαιτήσεων μπορεί ακολούθως να επιλεχθεί η κατάλληλη στρατηγική.

- ***Καθορισμός Χρόνου ανάκαμψης***

Λόγω της ιδιαίτερης φύσης του οργανισμού, ως πάροχος υπηρεσιών υγείας, προκύπτει η λογική κατάταξη των ΠΣ σε αυτά που υποστηρίζουν αμιγώς Κλινικές Υπηρεσίες (Κλινικά ΠΣ),

σε αυτά που υποστηρίζουν Διοικητικές Υπηρεσίες (Διοικητικά ΠΣ) και σε αυτά που υποστηρίζουν την εν γένει λειτουργία του οργανισμού (Υποστηρικτικά ΠΣ). Παρατηρούμε ότι στα Κλινικά και στα Υποστηρικτικά ΠΣ, τα οποία διαχειρίζονται κυρίως ευαίσθητα δεδομένα ασθενών, απαιτείται εστίαση στις νομικές-κανονιστικές επιπτώσεις ως προς τον καθορισμό των χρόνων ανάκαμψης ενώ αντίστοιχα στα Διοικητικά ΠΣ, τα οποία διαχειρίζονται οικονομικά δεδομένα, απαιτείται εστίαση κυρίως στις οικονομικές επιπτώσεις. Ως αποτέλεσμα προκύπτει η διαφοροποίηση στις χρονικές απαιτήσεις για την ανάκαμψη κάθε κατηγορίας, η οποία αποτυπώνεται και στην ανάλυση των επιχειρησιακών επιπτώσεων. Σύμφωνα με αυτή τα περισσότερα ΠΣ (κυρίως τα Κλινικά και τα Υποστηρικτικά) θα πρέπει να έχουν ανακάμψει εντός 1 Ημέρας (24 ώρες) και ορισμένα, μικρότερης κρισιμότητας (κυρίως τα Διοικητικά), εντός 3 Ημερών ή 1 Εβδομάδας.

Συνεπώς κατά το σχεδιασμό του ΣΑΚ θα μπορούσε να επιλεχθεί με ασφάλεια ως επιδιωκόμενος χρόνος ανάκαμψης ο ελάχιστος απαιτούμενος, δηλαδή 1 ημέρα, ώστε να καλυφθούν όλες οι απαιτήσεις. Έχοντας όμως ως στόχο τον περιορισμό του κόστους ανάκαμψης στο ελάχιστο δυνατό, προτείνεται η υιοθέτηση των επιδιωκόμενων χρόνων ανάκαμψης διακριτά για τα επιμέρους ΠΣ, όπως αυτοί προκύπτουν ως μέγιστοι ανεκτοί χρόνοι δυσλειτουργίας από τον Πίνακα 13. Παράλληλα μπορούμε να ορίσουμε ως μέγιστο ανεκτό χρόνο ανάκαμψης για το σύνολο των ΠΣ τη **1 Εβδομάδα** (ήτοι 5 εργάσιμες).
Ιδιαίτερη σημασία κατά τον καθορισμό του χρόνου ανάκαμψης πρέπει να δοθεί και στο χρονικό που μεσολαβεί από την εκδήλωση της καταστροφής μέχρι και την έναρξη του Σχεδίου Ανάκαμψης. Στο ίδιο χρονικό διάστημα πρέπει να διερευνηθεί και να αποφασιστεί η αναγκαιότητα σχετικά με το κατά πόσο απαιτείται η χρήση εναλλακτικών εγκαταστάσεων στα πλαίσια εφαρμογής του ΣΑΚ, λαμβάνοντας υπόψη ότι μια τέτοια απόφαση συνεπάγεται αρκετά υψηλότερο κόστος. Για τη περίπτωση που μελετάμε επιλέγεται ως μέγιστος χρόνος για τη λήψη της παραπάνω απόφασης οι **4 Ώρες**. Παράλληλα τίθεται ως χρονικό διάστημα-στόχος για τη δυνατότητα φιλοξενίας των ΠΣ στις εναλλακτικές εγκαταστάσεις οι **2 εβδομάδες**, στη διάρκεια του οποίου θα πρέπει να έχουν αποκατασταθεί οι κυρίως εγκαταστάσεις και να είναι σε θέση να φιλοξενήσουν και πάλι τα ΠΣ.

Ο καθορισμός του μέγιστου χρόνου στον οποίο αφορά η απώλεια δεδομένων όπως προκύπτει από τον Πίνακα 13 καθορίζεται στη 1 Ημέρα.

- ***Προσδιορισμός κόστους μη διαθεσιμότητας και εκτίμηση κόστους ανάκαμψης***

Για να προσδιορίσουμε το ποσό που πρέπει να διατεθεί για την ανάκαμψη θα πρέπει αρχικά να προσδιορίσουμε το κόστος που προκαλεί μια ενδεχόμενη καταστροφή των ΠΣ συναρτήσει του χρόνου που αυτά είναι μη διαθέσιμα (CoRI).

Για να το επιτύχουμε αυτό υιοθετούμε την προσέγγιση που περιγράφεται στην §3.4.6, σύμφωνα με την οποία ισχύει:

$$CoRI_{MTD} = (T_{RT} + T_{RP}) \times (Hr + Pr)$$

όπου:

T_{RT} : Διάρκεια μέχρι την ανάκαμψη

T_{RP} : Διάρκεια απώλειας δεδομένων βάσει RPO

Hr : **Κόστος/ημέρα από εργατοώρες** λόγω αδράνειας του προσωπικού

Pr : Κόστος/ημέρα από **απώλεια εσόδων**

Βάσει των παραδοχών που έγιναν για τη συγκεκριμένη περίπτωση (§6.2.1), ισχύει ότι ο κύκλος εργασιών του οργανισμού είναι ~2.000.000€ και το κόστος μισθοδοσίας ~3.000.000€, τα οποία ανάγοντας τα σε ημερήσια κλίμακα, θεωρώντας ότι ένα εργασιακό έτος έχει 300 εργάσιμες ημέρες, προκύπτει ότι:

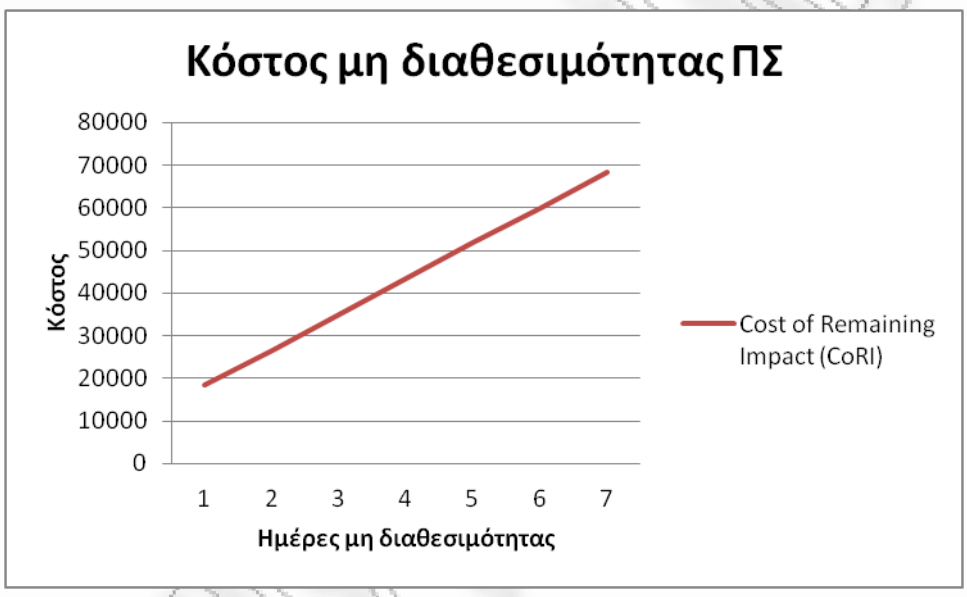
- Έσοδα: 2.000.000/300= 6.700€ ανά ημέρα, οπότε Pr =6.700€
- Κόστος μισθοδοσίας: 3.000.000/300=10.000€ ανά ημέρα, οπότε Hr=10.000€
- T_{RT} : κατά την οποία εκτιμούμε ότι επέρχεται μείωση της παραγωγικότητας (απώλεια εσόδων και αδράνεια προσωπικού) κατά 50% (λόγω ύπαρξης σχεδίου επιχειρησιακής συνέχειας, η οποία επιτρέπει διατήρηση παραγωγικότητας 50%, βλέπε §6.2.1)
- T_{RP} : η οποία όπως είδαμε αντιστοιχεί σε 1 Ημέρα και εκτιμούμε ότι προκαλεί ελάχιστη έως μηδενική απώλεια στα έσοδα (εφόσον εισπράττονται κατά την παροχή της υπηρεσίας) και ολική (100%) αδράνεια προσωπικού, καθώς θα πρέπει να απασχοληθεί το προσωπικό για το ίδιο χρονικό διάστημα ώστε να επαναληφθούν οι εργασίες στις οποίες αφορούν τα απολεσθέντα δεδομένα.

Επομένως το κόστος της καταστροφής συναρτήσει του χρόνου εκφράζεται από τη παρακάτω σχέση και το αντίστοιχο γράφημα:

$$CoRI_{MTD} = (T_{RT} + T_{RP}) \times (Hr + Pr) = (T_{RT} \times (Hr + Pr)) + (T_{RP} \times (Hr + Pr)) = (T_{RT} \times 50\% \times (Hr + Pr)) + (T_{RP} \times 100\% \times (Hr + Pr))$$

$$= (T_{RT} \times 50\% \times (10000 + 6700)) + (1 \times 10000)$$

$$= (T_{RT} \times 8350) + 10000$$



Σχήμα 22: *Κόστος μη διαθεσιμότητας ΠΣ*

Το παραπάνω διάγραμμα (Σχήμα 22) μπορεί να χρησιμοποιηθεί έτσι ώστε να υπάρχει μια άμεση εκτίμηση του κόστους της μη διαθεσιμότητας, συναρτήσει του χρόνου που αυτή διαρκεί. Επομένως κατά την αξιολόγηση των στρατηγικών και των λύσεων ανάκαμψης, μπορεί να συγκριθεί το κόστος τους με το κόστος των επιπτώσεων, για το αντίστοιχο χρονικό διάστημα της ανάκαμψης που υπόσχονται, ώστε να κριθεί κατά πόσο είναι αποδοτικά από οικονομική σκοπιά.

Όπως περιγράφεται και στην §3.4.5, το διατιθέμενο ποσό για την ανάκαμψη θα πρέπει να αντιστοιχεί στην τάξη μεγέθους του κόστους της μη διαθεσιμότητας για να μπορεί να χαρακτηριστεί ως «αποδοτικό» με αυστηρά οικονομικά κριτήρια. Επομένως για την περίπτωση που μελετάμε όπου οι απαιτήσεις ανάκαμψης κυμαίνονται από 1-5 ημέρες, και

το αντίστοιχο κόστος της μη διαθεσιμότητας κυμαίνεται αντίστοιχα από **20.000-50.000 €**. Για να διατηρηθεί η παραπάνω ισορροπία θα πρέπει και το συνολικό κόστος των μέτρων ανάκαμψης να κυμαίνεται στο ίδιο επίπεδο (δηλαδή CoR=CoRI). Δε θα πρέπει να παραβλέπεται σε αυτό το σημείο ότι οι ιδιαίτερες απαιτήσεις ενός οργανισμού, πέρα από τις οικονομικές, μπορεί να αυξήσουν κατά πολύ αυτό το ποσό.

Σύμφωνα με μελέτη που έγινε σε δείγμα 1700 επιχειρήσεων [70], η κοινή πρακτική που παρουσιάστηκε όσον αφορά το ποσό που διατίθεται για έξοδα που σχετίζονται με το σχεδιασμό και τη λήψη μέτρων ανάκαμψης από καταστροφές κυμαίνεται στο 26% του ετήσιου διατιθέμενου ποσού για έξοδα πληροφορικής. Το συμπέρασμα αυτό σε συνδυασμό με τις παραδοχές που αναφέρονται για τη συγκεκριμένη περίπτωση (§6.2.1), όπου το διατιθέμενο ετήσιο ποσό για έξοδα πληροφορικής κυμαίνεται στα 200.000€, μας οδηγεί στην εκτίμηση ότι ένα πιθανό ποσό που θα μπορούσε να εγκριθεί για τη σχεδίαση του ΣΑΚ θα προσέγγιζε τα **52.000€**. Παρατηρούμε ότι το ποσό αυτό κυμαίνεται στα ίδια επίπεδα με αυτό που προκύπτει και από την αντιστοιχία με το κόστος της μη διαθεσιμότητας, καθιστώντας το ποσό αυτό ως μια ρεαλιστική εκτίμηση του ολικού ποσού που πρέπει να διατεθεί για την ανάκαμψη.

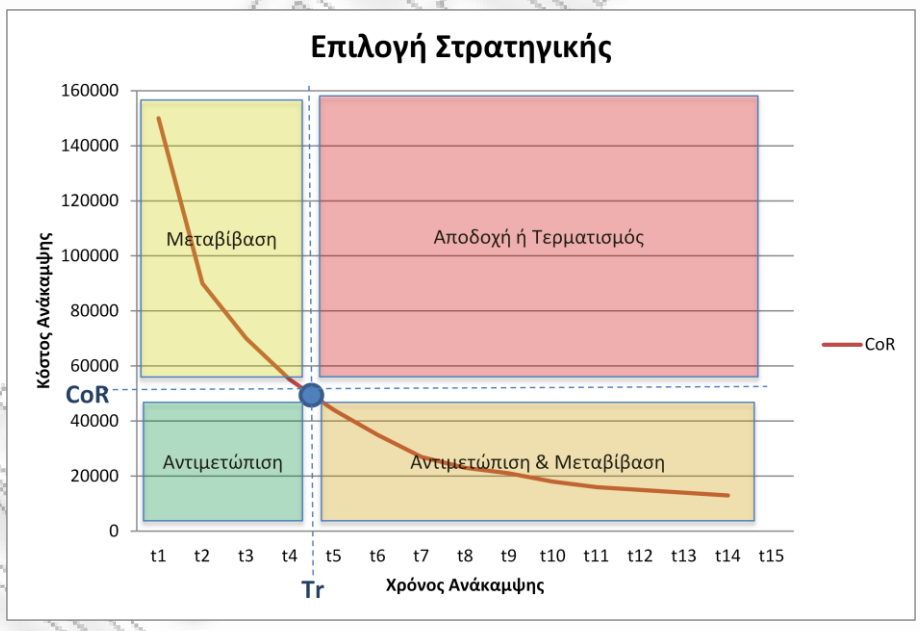
Συμπερασματικά μπορούμε να παρατηρήσουμε ότι τόσο οι απαιτήσεις της ανάκαμψης όσο και τα διατιθέμενα ποσά είναι άρρηκτα συνδεδεμένα με τον κύκλο εργασιών του οργανισμού. Συνεπώς θα πρέπει σε τακτική βάση και σε κάθε σημαντική αυξομείωση του, να αναθεωρούνται και να προσαρμόζονται ανάλογα, ώστε να διατηρείται η απόδοση του ΣΑΚ, με οικονομικούς όρους.

- ***Καθορισμός και επιλογή στρατηγικών αντιμετώπισης***

Έχοντας προσδιορίσει τις χρονικές απαιτήσεις ανάκαμψης (T_r) και το μέγιστο κόστος (CoR) το οποίο απαιτείται, έχουμε πλέον στη διάθεσή μας τα απαραίτητα μεγέθη για την αξιολόγηση και την επιλογή των στρατηγικών αντιμετώπισης και των σχετικών με αυτές μέτρων-λύσεων. Όπως είδαμε στην §4.4.1, οι διαθέσιμες αυτές στρατηγικές αντιμετώπισης αποτελούνται από την Αντιμετώπιση, τον Τερματισμό, τη Μεταβίβαση και την Αποδοχή.

Επομένως για κάθε λύση ανάκαμψης που χαρακτηρίζεται από το κόστος της και το χρόνο ανάκαμψης που υπόσχεται (CoR(ι), t_r(ι)) μπορούμε να επιλέξουμε την εκάστοτε στρατηγικής σύμφωνα με τα κάτωθι (Σχήμα 23):

- Αντιμετώπιση (Treat), εφαρμόζοντας τα προτεινόμενα μέτρα, όταν το κόστος τους και ο χρόνος ανάκαμψης που προσφέρουν είναι σε ανεκτά επίπεδα. (CoR(ι) < CoR και t_r(ι) < T_r)
- Μεταβίβαση (Transfer), όταν το κόστος τους υπερβαίνει το επιθυμητό μέγιστο κόστος ανάκαμψης, που επιτυγχάνεται συνήθως μέσω outsourcing. (CoR(ι) > CoR και t_r(ι) < T_r)
- Αντιμετώπιση και Μεταβίβαση (Treat and Transfer), όταν το κόστος τους είναι ανεκτό αλλά δεν πληρούν τις χρονικές απαιτήσεις. Στην περίπτωση αυτή γίνεται εφαρμογή των μέτρων με παράλληλη μερική μεταφορά της ευθύνης, συνήθως μέσω ρητρών σε συμβόλαια εγγυημένου επιπέδου υπηρεσίας (SLAs) και μέσω ασφαλιστικών συμβολαίων. (CoR(ι) < CoR και t_r(ι) > T_r)
- Αποδοχή ή τερματισμός (Tolerate or Terminate), όταν το κόστος των μέτρων είναι υψηλότερο από το επιθυμητό μέγιστο κόστος και δεν πληρούνται οι χρονικές απαιτήσεις της ανάκαμψης. (CoR(ι) > CoR και t_r(ι) > T_r)



Σχήμα 23: *Επιλογή στρατηγικής αντιμετώπισης ανάκαμψης*

Ακολουθώντας αυτούς τους κανόνες και λαμβάνοντας υπόψη τα ιδιαίτερα χαρακτηριστικά του κάθε ΠΣ μπορούμε να επιλέξουμε την ακολουθούμενη κάθε φορά στρατηγική, όπως παρουσιάζεται στον παρακάτω Πίνακα 14.

Α/Α	ΠΛΗΡΟΦΟΡΙΑΚΟ ΣΥΣΤΗΜΑ	MTD	CI	RPO	ΣΤΡΑΤΗΓΙΚΗ ΑΝΑΚΑΜΨΗΣ				ΠΕΡΙΓΡΑΦΗ
					Treat	Transfer	Treat & Transfer	Tolerate or Terminate	
1	Intranet (LAN)	1H	15	1Ω			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
2	printing services	1H	15	1Ω			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
3	EHR	1H	15	1Ω			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
4	Internet (WAN)	1H	15	1Ω			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
5	RIS/PACS	1H	15	1Ω			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
6	e-Health	1H	15	1Ω				X	Αφορά κρατικές υπηρεσίες ηλεκτρονικής συνταγογράφησης και ηλεκτρονικής διάγνωσης/παραμπομπής τα οποία ανήκουν σε εξωτερικούς φορείς. Ως στρατηγική αντιμετώπισης προτείνεται η εφαρμογή χειροκίνητων διαδικασιών μέχρι την ανάκαμψη του ΠΣ.
7	LIS	1H	15	1Ω			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
8	MED APPS	1H	15	1Ω			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
9	security services	1H	12	1Ω			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
10	file services	1H	10	1E			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
11	mail services	1H	10	1Ω		X			Παρέχεται ως υπηρεσία από εξωτερικό οργανισμό. Μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
12	web portal	1H	10	1E		X			Παρέχεται ως υπηρεσία από εξωτερικό οργανισμό. Μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
13	ERP	3H	11	1H			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
14	QMIS	3H	8	1E			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
15	MIS	1E	10	1E			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
16	HRIS	1E	8	1E	X				Λήψη απαραίτητων μέτρων
17	PMIS	1E	5	1E	X				Λήψη απαραίτητων μέτρων

Πίνακας 14: *Επιλογή στρατηγικών αντιμετώπισης ανά ΠΣ*

6.5.5 Ανάπτυξη Σχεδίου Ανάκαμψης από Καταστροφές

Επόμενο βήμα αποτελεί η καταγραφή σε ένα περιεκτικό οδηγό-πλάνο των ενεργειών που απαιτούνται για την ανάκαμψη των Πληροφοριακών Συστημάτων. Στο ΠΑΡΑΡΤΗΜΑ παρατίθεται ένα προτεινόμενο πρότυπο για αυτό το πλάνο (IT DRP), ενώ παρακάτω περιγράφονται τα βασικότερα από τα επιμέρους στοιχεία που το αποτελούν (βλέπε και §4.5).

i. Καταγραφή στοιχείων

Γίνεται καταγραφή των βασικότερων στοιχείων που αφορούν στο ίδιο το πλάνο και τον οργανισμό εν γένει, σύμφωνα με όσα περιγράφονται στην §4.5.1.

ii. Θέσπιση στόχων ανάκαμψης

Γίνεται παράθεση των αποτελεσμάτων που προέκυψαν από τη διενέργεια της ανάλυσης των επιχειρησιακών επιπτώσεων (§6.5.2) και κατά την επιλογή των στρατηγικών ανάκαμψης (§6.5.4). Για τον καθορισμό τους γίνεται χρήση των δεικτών CI, MTD, RTO, RPO.

Σε περίπτωση που αποφασιστεί η μετάβαση στις εναλλακτικές εγκαταστάσεις ισχύουν οι ίδιες απαιτήσεις ανάκαμψης. Αν η καταστροφή των κυρίως εγκαταστάσεων είναι εκτεταμένη, οι εναλλακτικές θα πρέπει να έχουν τη δυνατότητα να φιλοξενήσουν τα ΠΣ για χρονικό διάστημα ίσο με 2 Εβδομάδες, εντός του οποίου θα πρέπει να έχουν αποκατασταθεί εκ νέου οι κύριες.

iii. Ανάπτυξη στρατηγικών και επιλογή μέτρων ανάκαμψης

- ***Στρατηγικές***

Σχετικά με τις ακολουθούμενες στρατηγικές επισυνάπτεται ο Πίνακας 14 όπως προέκυψε στην §6.5.4.

- ***Πολιτική αντιγράφων ασφαλείας***

Κάνοντας χρήση του δείκτη RPO, από την ανάλυση επιχειρησιακών επιπτώσεων, καθορίζεται και η πολιτική λήψης αντιγράφων ασφαλείας για τα δεδομένα κάθε ΠΣ. Η πολιτική αυτή εκφράζεται με τη μορφή πίνακα και προβλέπει τη φύλαξη των αντιγράφων

είτε τοπικά, επιτυγχάνοντας μεγαλύτερη ταχύτητα ανάκτησης, είτε απομακρυσμένα, επιτυγχάνοντας μεγαλύτερη προστασία από το καταστροφικό συμβάν.

- ***Επιλογή και εφαρμογή μέτρων***

Κατά την επιλογή των μέτρων ανάκαμψης για τα συστατικά στοιχεία των ΠΣ, λαμβάνοντας υπόψη και τις απαιτήσεις του Πίνακα 13 (ανά ΠΣ), γίνεται χρήση του συγκριτικού Πίνακα 7 (§5.8). Μεταξύ των μέτρων που πληρούν τις απαιτήσεις χρόνου και κόστους για την ανάκαμψη (CoR και T_r), θα χρησιμοποιηθεί ο δείκτης RORI (§3.4.5), ώστε να επιλεχθεί η βέλτιστη οικονομικά λύση. Συνεπώς θα συγκρίνουμε, για κάθε λύση, το άθροισμα του κόστους της και του εναπομείναντος κόστους από τη μη διαθεσιμότητα, για το δεδομένο χρόνο ανάκαμψης που αυτή προσφέρει, δηλαδή:

$$RORI(i) = TCD_{MTD}(i) = CoR(i) + CoRI(i)$$

Έτσι, ως παράδειγμα, σε περίπτωση που έχουμε να επιλέξουμε μεταξύ του μέτρου Α και του μέτρου Β όταν:

- A($CoR_{(A)}$=20000,$tr_{(A)}$=1) και B($CoR_{(B)}$=2000, $tr_{(B)}$=3), επειδή $TCD_{(A)}$=40000 και $TCD_{(B)}$=37000 προτιμάται το μέτρο Β.
- A($CoR_{(A)}$=18000,$tr_{(A)}$=1) και B($CoR_{(B)}$=9000, $tr_{(B)}$=3), επειδή $TCD_{(A)}$=38000 και $TCD_{(B)}$=44000 προτιμάται το μέτρο Α.

Έχοντας υπόψη τα παραπάνω μπορούμε να επιλέξουμε τα κατάλληλα μέτρα για κάθε συστατικό στοιχείο, όπως αυτά παρουσιάζονται στον Πίνακα 15. Ο πίνακας αυτός περιέχει τόσο βασικές παρατηρήσεις για τα επιλεχθέντα μέτρα όσο και εκτίμηση του κόστους εφαρμογής τους. Παρατηρούμε ότι η επιλογή των μέτρων είναι τέτοια ώστε το συνολικό κόστος τους (~46.000€) να καλύπτεται από το μέγιστο διατιθέμενο ποσό (<50.000€) που τέθηκε στην §6.5.4 για τα μέτρα ανάκαμψης.

Η εφαρμογή των επιλεχθέντων μέτρων εκφράζεται μέσα από τη συμπλήρωση των αντίστοιχων Πλάνων Αντιμετώπισης Καταστροφής (ISCPs) για κάθε ΠΣ χωριστά. Το πρότυπο του αντίστοιχου εντύπου παρατίθεται στο Παράρτημα του ΣΑΚ (βλέπε ΠΑΡΑΡΤΗΜΑ-ΣΑΚ:Έντυπο ISCPs). Το έντυπο αυτό συμπληρώνεται από το εξειδικευμένο προσωπικό (τεχνικό, διοικητικό) το οποίο ασχολείται με τα εν λόγω ΠΣ.

		ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ																				
	ΣΤΡΑΤΗΓΙΚΗ	Treat & Transfer	Treat & Transfer	Treat & Transfer	Treat & Transfer	Treat & Transfer	tolerate	Treat & Transfer	Treat & Transfer	Treat & Transfer	Treat & Transfer	transfer	transfer	Treat & Transfer	Treat & Transfer	Treat & Transfer	Treat	Treat				
	ΜΕΤΡΑ	Intranet (LAN)	printing services	EHR	Internet (WAN)	RIS/PACS	e-Health	LIS	MED APPS	security services	file services	mail services	web portal	ERP	QMIS	MIS	HRIS	PMIS	ΠΑΡΑΤΗΡΗΣΕΙΣ	ΚΟΣΤΟΣ	ΠΕΡΙΓΡΑΦΗ ΚΟΣΤΟΥΣ
Άνθρωποι	**Αριθμ.επάρκεια**																				
	Αναπλήρωση (redundancy)	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	Η αναπλήρωση αυτή αφορά κυρίως το ρόλο του διαχειριστή και του κύριου χρήστη. Εφαρμόζεται για όλα τα ΠΣ εκτός από αυτά που φιλοξενούνται και διαχειρίζονται εξ' ολοκλήρου από εξωγενείς παράγοντες	0	Καλύπτεται από υπάρχον προσωπικό
	Ανάθεση (Outsouring)	X	X	X	X	X		X	X	X	X			X	X	X	X	X	Ανάθεση σε εξειδικευμένους εξωτερικούς συνεργάτες για συνεργασία με υπάρχον προσωπικό. Σύναψη συμβολαίων παροχής υπηρεσιών, ιδίως για τα κρίσιμα ΠΣ.	2000	Εργατοώρες (~20)
	Τηλεεργασία	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	Δυνατότητα τηλεεργασίας για όλα τα ΠΣ.	500	Συνδέσεις πρόσβασης σε διαδίκτυο
	Εκπαίδευση																				
	Βασική εκπαίδευση	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Βασική εκπαίδευση και ενημέρωση προσωπικού για εφαρμοζόμενες στρατηγικές.	0	
	Εξειδικευμένη εκπαίδευση	X	X	X	X	X		X	X	X	X								Εκπαίδευση εξειδικευμένου προσωπικού του οργανισμού για κρίσιμα συστήματα.	2000	Τεχνικά σεμινάρια
Εγκαταστάσεις	**Ιδιοκτησιακά**																				
	Ιδιόκτητες	X	X	X	X	X		X	X	X	X			X	X	X	X	X	Χρήση ιδιόκτητων εναλλακτικών εγκαταστάσεων.	0	
	Ανταποδοτική συμφωνία																			0	
	Εμπορική μίσθωση																			0	
	Επίπεδο εξοπλισμού																				
	cold sites																				
	warm sites	X	X	X	X	X		X	X	X	X			X	X	X	X	X	Υπαρξη κατάλληλων υποδομών και εξοπλισμού προς χρήση.	5000	Διαμόρφωση υπάρχοντος χώρου και υποδομών (ups, acecss control, cooling).
	hot sites																			0	
	mobile sites																			0	
	mirrored sites																			0	
Τεχνολογίες	**Πλατφόρμες-Συστήματα**																				
	Συστήματα Υψηλής διαθεσιμότητας			X				X		X	X								Χρήση σε κρίσιμα συστήματα και όπου είναι εφικτό.	0	
	Εικονικοποίηση		X	X		X		X	X	X	X			X	X	X	X	X	Χρήση κυρίως για επιτάχυνση της εγκατάστασης σε εναλλακτικές εγκαταστάσεις.	1500	Εργατοώρες για μετατροπή εξυπηρετητών σε εικονικές μηχανές(~15).
	Υπολογιστικό νέφος-DRaaS																			0	
	Τηλεπικοινωνίες																				
	Αρχιτεκτονικές εφεδρείας	X			X														Χρήση σε τοπολογία δικτύου κυρίως εγκαταστάσεων.	500	Κόστη καλωδίωσης.
	Βελτιστοποίηση απόδοσης (wan optimization)				X														Χρήση σε WAN και σε διασύνδεση με εναλλακτικές εγκαταστάσεις.	0	
	Εναλλακτικά μέσα μετάδοσης																				
	satellite																			0	
	mobile				X														Χρήση σε WAN και σε διασύνδεση με εναλλακτικές εγκαταστάσεις.	1000	Σύνδεση για mobile Internet (2 εβδομάδες) για κύριες εγκαταστάσεις
	Απομακρυσμένη πρόσβαση																				
	IPSec VPN	X	X	X	X	X		X	X	X	X			X	X	X	X	X	Χρήση για απομακρυσμένη υποστήριξη.	200	Συνδέσεις mobile Internet για απομακρυσμένη πρόσβαση προσωπικού.
	SSL VPN																			0	
	Cloud VPN																			0	
Δεδομένα	**Μέσα**																				
	tape			X		X		X	X	X	X			X	X		X	X	Αφορά σε εβδομαδιαίο πλήρες αντίγραφο ασφαλείας που αποστέλλεται στις εναλλακτικές εγκαταστάσεις.	100	Υπάρχει ήδη εξοπλισμός. Αφορά σε αναλλακτικά.
	hd			X		X		X	X	X	X			X	X		X	X	Αφορά σε ημερήσιο διαφορικό αντίγραφο ασφαλείας	500	Υπάρχει ήδη εξοπλισμός. Αφορά σε αναλλακτικά.
	online			X		X		X	X	X				X					Αφορά σε ημερήσιο διαφορικό αντίγραφο που αποστέλλεται online στις εναλλακτικές εγκαταστάσεις	0	
	Μέθοδοι																				
	full			X		X		X	X	X	X			X	X		X	X	Αφορά σε εβδομαδιαίο πλήρες αντίγραφο ασφαλείας.	0	
	differential			X		X		X	X	X	X			X	X		X	X	Αφορά σε ημερήσιο διαφορικό αντίγραφο ασφαλείας	0	
	incremental																			0	
	Τεχνικές																				
	replication sync																			0	
	replication async																			0	
	deduplication			X		X		X	X	X	X			X	X	X	X	X		0	
	cdp																			0	
	snapshot																			0	
Διαδικασίες	**Εφαρμογή προτύπων**	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Υιοθέτηση προτύπων (ISO27001,δυνητικά και ISO24762)	5000	Υπηρεσίες συμβουλευτικής και πιστοποίησης.
	Λήψη οργανωτικών μέτρων	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Ενημέρωση, Διαδικασίες, Δοκιμές	5000	Κόστος διεξαγωγής δοκιμών (υπερωρίες, υλικά-αναλώσιμα).
Προμηθευτές	**Αντικατάσταση εξοπλισμού**																				
	συμφωνια με προμηθευτες (SLAs)					X				X									Συμφωνία με προμηθευτές λόγω εξειδικευμένου εξοπλισμού.	2000	Συμβόλαια παροχής υπηρεσιών με αντικατάσταση εξοπλισμού και ρήτρες.
	εφεδρικός εξοπλισμός		X	X				X	X		X			X	X	X	X	X	Χρήση εφεδρικού εξοπλισμού ο οποίος βρίσκεται στις εναλλακτικές εγκαταστάσεις.	16000	Αγορά εφεδρικού εξοπλισμού (εξυπηρετητές, σταθμοί εργασίας, φορητοί σταθμοί,εκτυπωτές). Περιλαμβάνει και επικουρικό εξοπλισμό (κινητά τηλέφωνα, σκληροί δίσκοι, λοιπά εργαλεία)
	συμβατός εξοπλισμός	X			X															0	
	Προγραμματισμός δαπανών	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Το ποσό που προκύπτει από τον προγραμματισμό θα πρέπει να είναι εξασφαλισμένο και πάντα διαθέσιμο σε τραπεζικό λογαριασμό.	3000	Λειτουργικές δαπάνες (Υπερωρίες, Έξοδα μετακίνησης/μεταφοράς, αναλώσιμα, λοιπά).
	Ανάθεση υπηρεσιών (outsourcing)					X													Συμφωνία με προμηθευτές λόγω εξειδικευμένου εξοπλισμού.	2000	Συμβόλαια παροχής υπηρεσιών ανάκαμψης με ρήτρες.
																			ΣΥΝΟΛΟ	**46300**	

Πίνακας 15: *Επιλογή μέτρων ανάκαμψης*

iv. Καθορισμός Ρόλων-Αρμοδιοτήτων

Για την αποτελεσματικότερη εφαρμογή του ΣΑΚ προτείνεται η ανάθεση των ρόλων-αρμοδιοτήτων να ακολουθήσει όσο το δυνατόν πιο πιστά την υπάρχουσα οργανωτική δομή του οργανισμού και να γίνει η ανάθεσή τους στα ήδη υπάρχοντα τμήματα. Παράλληλα λόγω του μικρού μεγέθους του οργανισμού επιβάλλεται η ανάθεση παράλληλων αρμοδιοτήτων στις ίδιες ομάδες-τμήματα.

Στις υποομάδες αντιμετώπισης της καταστροφής προτείνεται η συμμετοχή και ενός εξωτερικού συνεργάτη, ώστε να συνεισφέρει στις αυξημένες απαιτήσεις τεχνογνωσίας και φόρτου εργασίας.

Στον παρακάτω πίνακα παρατίθεται η εφαρμογή των παραπάνω η οποία καταλήγει στην αξιοποίηση 10 ατόμων από το προσωπικό και 5 εξωτερικών συνεργατών.

Ρόλος κατά την εφαρμογή του ΣΑΚ	**Ανάθεση**	**Άτομα**
Υπεύθυνοι		
Υπεύθυνος Συντονισμού	Προϊστάμενος Πληροφορικής	1
Υπεύθυνος Επικοινωνίας	Προϊστάμενος Τμήματος Προσωπικού	1
Υπεύθυνος Επικαιροποίησης	Προϊστάμενος Πληροφορικής	
Υπεύθυνος Νομικών ενεργειών	Νομικός Σύμβουλος	1
Υπεύθυνος Εκπαίδευσης	Προϊστάμενος Πληροφορικής	
Ομάδα Αντιμετώπισης Καταστροφής		
Υποομάδα Υποδομών	Τμήμα Τεχνικό	2
Υποομάδα Συστημάτων και Περιφερειακών	Τμήμα Πληροφορικής-Ομάδα Α	1+(1)
Υποομάδα Εξυπηρετητών και Εφαρμογών	Τμήμα Πληροφορικής-Ομάδα Β	1+(1)
Υποομάδα Τηλεπικοινωνιών και δικτύων	Τμήμα Πληροφορικής-Ομάδα Γ	1+(1)
Υποομάδα Ανάκτησης δεδομένων	Τμήμα Πληροφορικής-Ομάδα Β	
Υποομάδα Ενημέρωσης και υποστήριξης χρηστών	Τμήμα Πληροφορικής-Ομάδα Α	
Ομάδα Προμηθειών και Μεταφοράς	Τμήμα Προμηθειών	2
Ομάδα Φυσικής ασφάλειας	(Εξωτερικοί συνεργάτες)	(2)
	ΣΥΝΟΛΟ:	**10+(5)**

Πίνακας 16: *Κατανομή ρόλων και ομάδων*

Το ΣΑΚ συμπληρώνεται με το απαραίτητο οργανόγραμμα αλλά και τη σύνοψη των ρόλου και των αρμοδιοτήτων κάθε υπεύθυνου και κάθε ομάδας.

v. Περιγραφή ενεργειών δράσης

Η περιγραφή της ροής των ενεργειών που πρέπει να γίνουν κατά τις τρεις φάσεις του κύκλου ζωής ενός περιστατικού (Ειδοποίηση/Ενεργοποίηση, Ανάκαμψη, Ανασύσταση/Επαναφορά) πρέπει να γίνεται με τον πλέον κατανοητό και προσιτό τρόπο. Για το λόγο αυτό επιλέγεται η παράθεσή τους με τη μορφή λογικών διαγραμμάτων ροής.

vi. Καθορισμός συνοδευτικών εντύπων

Για την ολοκλήρωση του ΣΑΚ ως συνοδευτικά έντυπα προτείνονται τα παρακάτω:

- ***Λίστες***
    - Στοιχεία επικοινωνίας
    - Κωδικοί πρόσβασης διαχειριστών
    - Συμβόλαια με τρίτους
    - Απαραίτητοι πόροι για ανάκαμψη
    - Ανάλυση επιχειρησιακών επιπτώσεων (BIA)
    - Στρατηγικές ανάκαμψης ανά ΠΣ

- ***Έντυπα***
    - Πλάνο αντιμετώπισης καταστροφών για κάθε ΠΣ(ISCPs)
    - Καταγραφή περιστατικού-αναφορά παρατηρήσεων

6.5.6 Δοκιμές και Εκπαίδευση

Σύμφωνα και με την πολιτική του οργανισμού και λαμβάνοντας υπόψη την αναγκαιότητα διεξαγωγής ασκήσεων-εκπαιδεύσεων συναρτήσει του κόστους διεξαγωγής τους, προτείνεται η παρακάτω συχνότητα εφαρμογής:

Είδος	Επί Χάρτου	Προσομοίωσης
Ανάκαμψη μεμονωμένων συστημάτων στις κύριες εγκαταστάσεις (Έλεγχος αποτελεσματικότητας ISCPs)	6 μήνες	1 έτος
Ανάκαμψη μεμονωμένων συστημάτων σε εναλλακτικές εγκαταστάσεις (Έλεγχος ετοιμότητας εναλλακτικών εγκαταστάσεων για εφαρμογή ISCPs)	1 έτος	2 έτη
Έλεγχος παρόχων υπηρεσιών (Έλεγχος επιπέδου παροχής υπηρεσιών και τήρησης δεσμεύσεων)	1 έτος	**2 έτη**
Ανάκαμψη πλήρους κλίμακας σε εναλλακτικές εγκαταστάσεις (Έλεγχος πλήρους εφαρμογής ΣΑΚ)	1 έτος	**3 έτη**

Πίνακας 17: *Προγραμματισμός δοκιμών*

6.5.7 Συντήρηση και Επικαιροποίηση

Σε συμφωνία με την «Δήλωση Πολιτικής» του οργανισμού και όσα περιγράφονται στην §4.7, προτείνεται η τακτική επικαιροποίηση του ΣΑΚ, **σε ετήσια βάση**, καθώς και εκτάκτως μετά από κάθε αλλαγή που μπορεί να επηρεάσει την αποτελεσματικότητά του.

7 Συμπεράσματα

Στη παρούσα εργασία εξετάσθηκε το θεματικό πεδίο του σχεδιασμού ανάκαμψης των ΠΣ ενός οργανισμού, σε περίπτωση καταστροφής. Επιχειρήθηκε να γίνει μελέτη του θέματος στο μεγαλύτερο δυνατό εύρος άλλα και να δοθεί έμφαση σε ιδιαίτερα ζητήματα, όπως κυρίως οικονομικής και νομικής φύσης, στα οποία μέχρι σήμερα μοιάζει να μην υπάρχουν ικανοποιητικές απαντήσεις. Παράλληλα αναλύθηκαν οι απαιτήσεις για την επιτυχή εφαρμογή ενός ΣΑΚ σε διοικητικό, οργανωτικό, αλλά και τεχνικό επίπεδο καθώς και τα μέσα με τα οποία μπορούν αυτές να ικανοποιηθούν.

Αρχικά, αναλύοντας την ιστορικότητα των καταστροφών και τις πολύπλευρες επιπτώσεις από την καταστροφή των ΠΣ ενός οργανισμού, διαπιστώθηκε η αναγκαιότητα επιστάμενης λήψης μέτρων για την αντιμετώπισή τους, καθώς παρατηρείται ραγδαία αύξηση τους τα τελευταία έτη, ιδιαίτερα στον ελλαδικό χώρο. Αν αναλογιστούμε ότι το πεδίο δράσης των οργανισμών μπορεί σήμερα να είναι παγκόσμιο, βασιζόμενο κυρίως στις τεχνολογίες πληροφορικής και επικοινωνιών, τότε ο Σχεδιασμός Ανάκαμψης από Καταστροφές των ΠΣ κρίνεται απαραίτητος. Ιδιαίτερα δε, στα σύγχρονα μεταβαλλόμενα οικονομικά περιβάλλοντα αποκτά προστιθέμενη αξία καθώς μπορεί να χρησιμοποιηθεί ως εργαλείο ταχείας μεταφοράς της επιχειρηματικής δραστηριότητας, σε πιο ασφαλή περιβάλλοντα, προσδίδοντας και «επιχειρησιακή ευελιξία».

Εξετάζοντας το νομικό πλαίσιο στην ΕΕ, και τον τρόπο που ενσωματώνεται στην ελληνική νομοθεσία, διαπιστώθηκε η ύπαρξη νομικών και κανονιστικών υποχρεώσεων για φορείς που διαχειρίζονται προσωπικά δεδομένα ή παρέχουν υπηρεσίες ηλεκτρονικών επικοινωνιών στο κοινό, σχετικά με τη διαφύλαξη της διαθεσιμότητας και ακεραιότητας των δεδομένων που επεξεργάζονται. Αυτές οι υποχρεώσεις αναφέρονται στη λήψη μέτρων προστασίας μέσα από μια γενικότερη έννοια, χωρίς να δηλώνουν ρητά ή/και να αναφέρονται ειδικότερα στη λήψη μέτρων ανάκαμψης, με αποτέλεσμα να έγκειται στη διακριτική ευχέρεια του φορέα η επιλογή και εφαρμογή συγκεκριμένων στρατηγικών-μέτρων ανάκαμψης από καταστροφές. Επομένως με το παρόν νομοθετικό πλαίσιο δεν υπάρχει ξεκάθαρη υποχρέωση ύπαρξης διαδικασιών και μέτρων ανάκαμψης, ούτε διασφαλίζεται η αποτελεσματικότητα τους, όταν αυτά υπάρχουν, η οποία είναι και το ζητούμενο. Μια ενδεχόμενη υποχρέωση εφαρμογής ενός οργανωμένου Σχεδίου Ανάκαμψης από Καταστροφές (ΣΑΚ), ακολουθώντας το παράδειγμα της υποχρέωσης κατάρτισης Σχεδίων Ασφαλείας της Λειτουργίας των Ευρωπαϊκών Υποδομών Ζωτικής

Σημασίας (Οδηγία 2008/114/ΕΚ [26] και ενσωμάτωση με Π.Δ.39/2011 [27]), ίσως να αντιμετώπιζε αποτελεσματικά το παραπάνω νομοθετικό έλλειμμα.

Σχετικά με τον τρόπο που θα πρέπει να σχεδιάζεται και να εφαρμόζεται αποτελεσματικά η ανάκαμψη των ΠΣ από καταστροφές, αναφέρθηκαν τα κυριότερα πρότυπα και οδηγίες που υπάρχουν σήμερα. Μελετώντας τα, συμπεραίνουμε την αυξητική τους τάση και τη σχετικά υψηλή ταχύτητα με την οποία αναθεωρούνται, ακολουθώντας με τον τρόπο αυτό τόσο τις τεχνολογικές εξελίξεις όσο και τις αυξημένες απαιτήσεις στο θεματικό πεδίο της ανάκαμψης από καταστροφές.

Κατά τη μελέτη του κόστους που πρέπει να έχει ο σχεδιασμός ανάκαμψης από καταστροφές ώστε να είναι αποδοτικός, διαπιστώνεται μεγάλη δυσκολία προσδιορισμού του. Για να επιτευχθεί απαιτείται η σύγκριση της σχέση κέρδους – κόστους του ΣΑΚ, όπου το μεν κόστος μπορεί να είναι μετρήσιμο ποσοτικά, το δε κέρδος για να είναι ρεαλιστικό θα απαιτούσε και την ποσοτικοποίηση που αφορά σε οφέλη πέραν των αμιγώς οικονομικών (νομικά-κανονιστικά, λειτουργικά, εμπιστοσύνη πελατών, υγιεινή&ασφάλεια). Για το λόγο αυτό χρησιμοποιείται ένας νέος δείκτης ο RORI (Return On Recovery Investment) ως μετεξέλιξη και προσαρμογή του δείκτη ROSI (Return On Security Investment). Ο δείκτης αυτός αντί για το κέρδος λαμβάνει υπόψη το εναπόμειναν οικονομικό κόστος μέχρι την ανάκαμψη των ΠΣ από τα ληφθέντα μέτρα, με την προϋπόθεση ότι η διάρκεια είναι τέτοια που δεν επιτρέπει να εκδηλωθούν άλλου τύπου επιπτώσεις πέραν των οικονομικών. Σε κάθε περίπτωση το κόστος του ΣΑΚ φέρεται να είναι άρρηκτα συνδεδεμένο με τον κύκλο εργασιών του οργανισμού, στον οποίο αφορά, και συνεπώς θα πρέπει να αναθεωρείται με κάθε αυξομείωσή του ώστε να διατηρείται σε αποδοτικό οικονομικά μέγεθος.

Σήμερα υπάρχει πληθώρα μέτρων, με διαφορετικά χαρακτηριστικά και δυνατότητες, τα οποία ενσωματώνοντας τις νέες τεχνολογικές εξελίξεις, μπορούν να προσφέρουν ταχύτατη δυνατότητα ανάκαμψης και σε αρκετά χαμηλότερο κόστος, με χαρακτηριστικότερα παραδείγματα το υπολογιστικό νέφος και τα κινητά δίκτυα 4^{ης} γενιάς. Δίδεται λοιπόν η δυνατότητα σε έναν οργανισμό να αξιοποιήσει αυτά που ταιριάζουν περισσότερο στις ανάγκες του και στον προϋπολογισμό του. Στο 5^{ο} κεφάλαιο παρατίθεται ένας συγκριτικός πίνακας αυτών των μέτρων, ο οποίος αξιολογεί ποιοτικά τα επιμέρους χαρακτηριστικά τους.

Τέλος, μέσα από τη μελέτη μιας περίπτωσης, παρουσιάστηκε η δυνατότητα εφαρμογής των βασικών σημείων της διαδικασίας σχεδιασμού της ανάκαμψης με γρήγορο και αποδοτικό τρόπο. Ως αποτέλεσμα προέκυψε ένα Σχέδιο Ανάκαμψης από Καταστροφές, το οποίο

μπορεί να χρησιμοποιηθεί ως βάση, και με τις απαραίτητες προσαρμογές να αξιοποιηθεί από μικρούς/μικρομεσαίους οργανισμούς. Πάραυτα, θα πρέπει να σημειωθεί ότι δε μπορεί να υπάρξει ένα σχέδιο-πρότυπο, το οποίο να χρησιμοποιείται ως πανάκεια και να αποτελέσει μόνιμη λύση για την ανάκαμψη από καταστροφές. Ο Σχεδιασμός Ανάκαμψης από Καταστροφές αποτελεί διαδικασία η οποία θα πρέπει προσαρμόζεται στις ιδιαίτερες ανάγκες και τα χαρακτηριστικά του κάθε οργανισμού, καθώς και να εξελίσσεται συνεχώς ώστε να επιτυγχάνεται το βέλτιστο αποτέλεσμα.

Βιβλιογραφία

[1] Emerson Network Power. State of the data center 2011. http://www.emersonnetworkpower.com/en-US/About/NewsRoom/Pages/2011DataCenterState.aspx (Accessed June 2012)

[2] Caralli, R. et al. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Processoctave allegro. May 2007.

[3] Enisa. IT Business Continuity Management: An approach for Small Medium Sized Organizations. Enisa, January 2010.

[4] European Parliament. Directive 89/391/EEC on the introduction of measures to encourage improvements in the safety and health of workers at work**.** European Parliament , 12 June 1989.

[5] Centre for Research on the Epidemiology of Disasters (CRED). EM-DAT: The International Disaster Database. http://www.emdat.be/ (Accessed June 2012)

[6] Centre for Research on the Epidemiology of Disasters (CRED). http://www.cred.be/ (Accessed June 2012)

[7] Swanson, M. et al. NIST Special Publication 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems. NIST, May 2010.

[8] Moen, R. and Norman, C. "Evolution of the PDCA Cycle". August 2009.

[9] AFCOM. State of the Data Center. AFCOM, March 2011. http://www.afcom.com

[10] ENISA. BCM & Resilience. http://www.enisa.europa.eu/activities/risk-management/current-risk/bcm-resilience (Accessed June 2012)

[11] National Institute of Standards and Technology (NIST). Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199). NIST, February 2004.

http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[12] Schreider, T. White paper-The Legal issues of disaster recovery planning. Disaster Rcovery Journal, June 1996.
http://www.drj.com/new2dr/model/schr.htm

[13] Γραφείο Αντιπροέδρου Κυβερνήσεως. Αναλυτικός πίνακας Οδηγιών. Ελληνική Κυβέρνηση, Μάρτιος 2012.
http://antiproedros.gov.gr/wp-content/uploads/2012/03/%CE%91%CE%9D%CE%91%CE%9B%CE%A5%CE%A4%CE%99%CE%9A%CE%9F%CE%A3-%CE%A0%CE%99%CE%9D%CE%91%CE%9A%CE%91%CE%A3-%CE%9F%CE%94%CE%97%CE%93%CE%99%CE%A9%CE%9D.pdf
(Accessed June 2012)

[14] European Parliament. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. European Parliament, 24 October 1995.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EL:HTML

[15] Πρόεδρος Ελληνικής Δημοκρατίας. Νόμος 2472: Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Εφημερίδα της Κυβερνήσεως, 10 Απριλίου 1997.

[16] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ). ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ, ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΣΧΕΔΙΟ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΕΣ.
http://www.dpa.gr/pls/portal/url/ITEM/B6F5DCC88FD8EC4AE040A8C07C24572A
(Accessed June 2012)

[17] European Parliament. Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. European Parliament, 18 December 2000.

[18] European Parliament. Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive). European Parliament, 7 March 2002.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:EL:HTML

[19] European Parliament. Directive 2009/136/EC amending Directive 2002/22/EC, Directive 2002/58/EC and Regulation (EC) No 2006/2004. European Parliament, 25 November 2009.

[20] Πρόεδρος Ελληνικής Δημοκρατίας. Νόμος 3431: Περί Ηλεκτρονικών Επικοινωνιών και άλλες διατάξεις. Εφημερίδα της Κυβερνήσεως, 3 Φεβρουαρίου 2006.

[21] Πρόεδρος Ελληνικής Δημοκρατίας. Νόμος 4070: Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις. Εφημερίδα της Κυβερνήσεως, 10 Απριλίου 2012.

[22] European Parliament. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). European Parliament, 12 July 2002. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EL:HTML

[23] Πρόεδρος Ελληνικής Δημοκρατίας. Νόμος 3471: Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997. Εφημερίδα της Κυβερνήσεως, 28 Ιουνίου 2006.

[24] European Parliament. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. European Parliament, 15 March 2006. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EL:PDF

[25] Πρόεδρος Ελληνικής Δημοκρατίας. Νόμος 3917: Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις. Εφημερίδα της Κυβερνήσεως, 21 Φεβρουαρίου 2011.

[26] European Parliament. Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. European Parliament, 8 December 2008. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EL:PDF

[27] Πρόεδρος Ελληνικής Δημοκρατίας. Προεδρικό Διάταγμα υπ΄αριθμ.39: Προσαρμογή της ελληνικής νομοθεσίας προς τις διατάξεις της Οδηγίας 2008/114/ΕΚ του Συμβουλίου της 8ης Δεκεμβρίου 2008 «σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την

αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους». Εφημερίδα της Κυβερνήσεως, 6 Μαΐου 2011.

[28] Κέντρο Μελετών Ασφάλειας (ΚΕ.ΜΕ.Α.). http://www.kemea.gr

[29] Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Council of Europe, Strasbourg 1981. http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

[30] U.S. Department of Commerce in consultation with the European Commission. U.S.-EU Safe Harbor Framework. July 2000. http://export.gov/safeharbor/eu/eg_main_018476.asp

[31] OECD. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD, September 1980. http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html

[32] UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files. UN General Assembly, 14 December 1990. http://www.unhcr.org/refworld/publisher,UNGA,THEMGUIDE,3ddcafaac,0.html

[33] OECD. Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. OECD, 25 July 2002. http://www.oecd.org/dataoecd/16/22/15582260.pdf

[34] Botchkarev, A. and Andru, P. A Return on Investment as a Metric for Evaluating Information Systems: Taxonomy and Application. Interdisciplinary Journal of Information, Knowledge, and Management Volume 6, 2011.

[35] Kirwin, B. and Mieritz, L. Defining Gartner Total Cost of Ownership. Gartner, 8 December 2005.

[36] Investopedia. Return on investment – ROI. http://www.investopedia.com/terms/r/returnoninvestment.asp (Accessed June 2012)

[37] Shneier, B. Schneier on Security: Security ROI. September 2, 2008. https://www.schneier.com/blog/archives/2008/09/security_roi_1.html (Accessed June 2012)

[38] Sonnenreich, W. et al. Return On Security Investment (ROSI) – A Practical Quantitative

Model. Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February 2006.
http://sonnenreich.com/wes/return_on_security_investment.pdf

[39] ENISA. Economics of Security: Facing the Challenges.ENISA, 2012.
http://www.enisa.europa.eu/activities/risk-management/files/EoS%20Final%20report

[40] Hand, L. UNITED STATES et al. v. CARROLL TOWING CO., Inc., et al. UNITED STATES CIRCUIT COURT OF APPEALS, SECOND CIRCUIT, January 1947.
http://www.learnedhand.com/

[41] Buffington, J. Data protection for virtual data centers. Sybex, August 2010.

[42] Senate and House of Representatives of the United States of America in Congress. Sarbanes-Oxley Act of 2002. Corporate responsibility. July 2002.
http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/html/PLAW-107publ204.htm

[43] Senate and House of Representatives of the United States of America in Congress. Health Insurance Portability and Accountability Act of 1996. August 1996.
http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm

[44] International Organization for Standardization (ISO). ISO/IEC 27001:2005 Information security management systems. ISO, October 2008.
http://www.iso.org/iso/catalogue_detail?csnumber=42103

[45] British Standards Institution (BSI). BS 25999: Business Continuity Management. BSI 2006-2007.

[46] International Organization for Standardization (ISO). ISO 22301:2012 Business continuity management systems. ISO, May 2012.
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50038

[47] British Standards Institution (BSI). BS 25777:2008 Information and communications technology continuity management. Code of practice. December 2008.

[48] International Organization for Standardization (ISO). ISO/IEC 27031:2011 Guidelines for Information and Communications Technology Readiness for Business Continuity. ISO, March 2011.
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374

[49] International Organization for Standardization (ISO). ISO/IEC 24762:2008 Guidelines for Information and Communications Technology Disaster Recovery Services. ISO, April 2011. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=41532

[50] National Institute of Standards and Technology (NIST). NIST Special Publication 800-53 Rev. 3: Recommended Security Controls for Federal Information Systems and Organizations. NIST, August 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[51] International Organization for Standardization (ISO). ISO/IEC 27002:2005 Code of practice for information security management. ISO, April 2008. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50297

[52] Bundesamt für Sicherheit in der Informationstechnik. BSI-Standard 100-3: Risk analysis based on IT-Grundschutz. BSI, 2008. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile

[53] EC-Council. Disaster Recovery. EC-Council|Press, 2011.

[54] National Institute of Standards and Technology (NIST). NIST Special Publication 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. NIST, September 2006. http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf

[55] ENISA. Good Practice Guide on National Exercises. ENISA, December 2009. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/exercises/national-exercise-good-practice-guide

[56] Sy, P. Infocomm Technology Readiness for Business Continuity-The International Standardisation Effort on ICT Continuity. Synthesis Journal, 2009. http://www.itsc.org.sg/pdf/synthesis09/Four_ICT.pdf

[57] Kirvan, P. Building a DR site vs. outsourcing disaster recovery. SearchDisasterRecovery, April 2012. http://searchdisasterrecovery.techtarget.com/podcast/Building-a-DR-site-vs-outsourcing-disaster-recovery

[58] National Institute of Standards and Technology (NIST). NIST Special Publication 800-145: The NIST Definition of Cloud Computing. NIST, September 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[59] Csaplar, D. Small and Mid-Sized Organizations Gain Disaster Recovery Advantages Using Cloud Storage. Aberdeen Group, December 2011. http://www.aberdeen.com/aberdeen-library/6827/RA-disaster-recovery-cloud.aspx

[60] Gartner. Gartner Says 30 Percent of Midsize Companies Will Use Recovery-as-a-Service by 2014. Gartner, November 2011. https://www.gartner.com/it/page.jsp?id=1841114

[61] ENISA. Security and Resilience in Governmental Clouds. ENISA, January 2011. http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/

[62] Stouffer, C. WAN acceleration: Enabling successful disaster recovery. SearchDataCenter, July 2006. http://searchdatacenter.techtarget.com/tip/WAN-acceleration-Enabling-successful-disaster-recovery

[63] NATA Systems. WAN Optimization. http://natasystems.com/en/wan (Accessed June 2012)

[64] Frost & Sullivan. Satellite-based Continuity and Recovery. http://www.myservicestar.com/myservicestar/White%20Papers/tct_whitepapers/spacenet/Frost_and_Sullivan-BC.pdf (Accessed June 2012)

[65] AbdelNasir, A. and Takamichi, S. A Technical Comparison of IPSec and SSL. Tokyo University of Technology, 2004. http://www.tresw.com/v6/_PDF/en/A%20Technical%20Comparison%20of%20IPSec%20and%20SSL.pdf

[66] Wood, T. et al. Disaster Recovery as a Cloud Service: Economic Benefits & Deployment Challenges. USENIX HotCloud 10, 2010. http://static.usenix.org/event/hotcloud10/tech/full_papers/Wood.pdf

[67] Jadad, A. et al. What Is eHealth (3): A Systematic Review of Published Definitions. J Med Internet Res., 2005 Jan-Mar. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1550636/

(Accessed June 2012)

[68] European Commision. eHealth. http://ec.europa.eu/health-eu/care_for_me/e-health/index_el.htm (Accessed June 2012)

[69] Humphrey, A. "SWOT Analysis for Management Consulting". SRI Alumni Newsletter (SRI International), December 2005.

[70] Symantec. 2010 Symantec Disaster Recovery Study. Symantec, November 2010. http://www.slideshare.net/symantec/symantec-2010-disaster-recovery-study (Accessed June 2012)

ΠΑΡΑΡΤΗΜΑ

Ερωτηματολόγιο Ανάλυσης Επιχειρησιακών Επιπτώσεων

Ερωτηματολόγιο Ανάλυσης Επιχειρησιακών Επιπτώσεων

Ημερομηνία	
Επώνυμο	
Όνομα	
Ειδικότητα-Θέση	

Γενικά στοιχεία	
Συμπληρώστε τα βασικά στοιχεία που αφορούν στην οργανωτική μονάδα-τμήμα στην οποία ανήκετε.	
Οργανωτική μονάδα - Τμήμα	
Περιγραφή ρόλου μονάδας-τμήματος στον οργανισμό	

Λειτουργίες που επιτελεί η οργανωτική μονάδα

Περιγράψτε τις λειτουργίες τις οποίες επιτελεί η μονάδα σας, οι οποίες κάνουν χρήση οποιουδήποτε από τα ΠΣ του οργανισμού για να έρθουν εις πέρας.(Πίνακας 1-Περιγραφή ΠΣ οργανισμού)

Α/Α	Τίτλος	Περιγραφή
1	<Λειτουργία 1>	
2	<Λειτουργία 2>	
3	<Λειτουργία 3>	
4	<Λειτουργία 4>	
5	<Λειτουργία 5>	

Χρησιμοποιούμενα ΠΣ

Για κάθε λειτουργία που συμπληρώσατε παραπάνω επιλέξτε τα ΠΣ που χρησιμοποιούνται από τη μονάδα σας για την εκτέλεσή της.

Α/Α	Λειτουργία	EHR	LIS	RIS/PACS	Medical Applications	e-Health	PMIS	HRIS	QMIS	MIS	ERP	mail services	file services	printing services	web-portal	internet access (WAN)	intranet access (LAN)	Security services	Άλλο
1	<Λειτουργία 1>																		
2	<Λειτουργία 2>																		
3	<Λειτουργία 3>																		
4	<Λειτουργία 4>																		
5	<Λειτουργία 5>																		

Ανεκτός χρόνος μη διαθεσιμότητας και απώλειας δεδομένων

Για κάθε λειτουργία δώστε τον μέγιστο ανεκτό χρόνο μη λειτουργίας των ΠΣ που την υποστηρίζουν. Ο χρόνος αυτός αντιστοιχεί στο χρονικό διάστημα μη δυνατότητας χρήσης των ΠΣ, μετά την πάροδο του οποίου είτε δε μπορεί να ολοκληρωθεί η λειτουργία είτε καθίσταται άκρως δυσχερής. (Επιλογές: ≤ 4 ώρες, ≤ 1 ημέρα, ≤ 3 ημέρες, ≤ 1 εβδομάδα)

Για κάθε λειτουργία δώστε τη μέγιστη ανεκτή απώλεια στα δεδομένα των ΠΣ που την υποστηρίζουν. Η απώλεια αυτή εκφράζεται ως το χρονικό διάστημα, στο οποίο αφορούν τα απωλεσθέντα δεδομένα, για το οποίο τα δεδομένα είτε μπορούν να επανεισαχθούν χειροκίνητα είτε η απώλειά τους δεν επιφέρει σημαντικές επιπτώσεις στην ίδια τη λειτουργία. (Επιλογές: ≤ 1 ώρα, ≤ 1 ημέρα, ≤ 1 εβδομάδα)

Α/Α	Λειτουργία		Μέγιστος ανεκτός χρόνος δυσλειτουργίας(MTD)					Μέγιστος ανεκτός χρόνος απώλειας δεδομένων(RPO)		
			4Ω	1Η	3Η	1Ε		1Ω	1Η	1Ε
1	<Λειτουργία 1>		☐	☐	☐	☐		☐	☐	☐
2	<Λειτουργία 2>		☐	☐	☐	☐		☐	☐	☐
3	<Λειτουργία 3>		☐	☐	☐	☐		☐	☐	☐
4	<Λειτουργία 4>		☐	☐	☐	☐		☐	☐	☐
5	<Λειτουργία 5>		☐	☐	☐	☐		☐	☐	☐

Επιπτώσεις μη διαθεσιμότητας

Για κάθε λειτουργία αξιολογείστε τις επιπτώσεις που ενδεχομένως να προκύψουν για τον οργανισμό από την παρατεταμένη μη διαθεσιμότητα (μεγαλύτερη από το μέγιστο ανεκτό χρόνο που δόθηκε παραπάνω) των ΠΣ που την υποστηρίζουν. (Επιλογές: Χ-χαμηλή, Μ-μέση, Υ-υψηλή σύμφωνα με Πίνακα 2- Κλίμακα επιπτώσεων)

		Νομικές-Κανονιστικές		Οικονομικές		Λειτουργικές-Παραγωγικές		Υπόληψη-Υστεροφημία		Υγιεινή και Ασφάλεια		Άλλες	
Α/Α	Λειτουργία	Επίπτωση	Περιγραφή	Επίπτωση	Περιγραφή	Επίπτωση	Περιγραφή	Επίπτωση	Περιγραφή	Επίπτωση	Περιγραφή	Επίπτωση	Περιγραφή
1	<Λειτουργία 1>												
2	<Λειτουργία 2>												
3	<Λειτουργία 3>												
4	<Λειτουργία 4>												
5	<Λειτουργία 5>												

Ανεκτός χρόνος μη διαθεσιμότητας και απώλειας δεδομένων

Για κάθε μια από τις λειτουργίες καταγράψτε την τυχόν εξάρτηση της από άλλες λειτουργίες, αυτής ή άλλης οργανωτικής μονάδας-τμήματος του οργανισμού.

Α/Α	Λειτουργία	Εξάρτηση από άλλες λειτουργίες	Περιγραφή
1	<Λειτουργία 1>		
2	<Λειτουργία 2>		
3	<Λειτουργία 3>		
4	<Λειτουργία 4>		
5	<Λειτουργία 5>		

	Πληροφοριακό Σύστημα	Περιγραφή
ΙΑΤΡΙΚΑ	**Electronic Health Records (EHR)**	Αναφέρεται συνήθως ως Ηλεκτρονικός Ιατρικός Φάκελος και χρησιμοποιείται για τη συλλογή και επεξεργασία πληροφοριών για την υγεία των ασθενών. Προσφέρεται για τη διαχείριση ιατρείων και ασθενών και την εξαγωγή στατιστικών στοιχείων και στην ουσία αποτελεί τη μεταφορά του έντυπου ιατρικού φακέλου ασθενών σε ηλεκτρονική μορφή. Όταν διασυνδέεται με άλλα ΠΣ μπορεί να περιλαμβάνει και αποτελέσματα εργαστηριακών και ακτινολογικών εξετάσεων
	Laboratory Information System (LIS)	Είναι το ΠΣ των Ιατρικών Εργαστηρίων, το οποίο συνήθως είναι διασυνδεδεμένο με κατάλληλο εργαστηριακό εξοπλισμό, με σκοπό την αποθήκευση και διακίνηση αποτελεσμάτων εργαστηριακών εξετάσεων (αιματολογικών, μικροβιολογικών, βιοπαθολογικών κοκ)
	Picture archiving and communication system (PACS)	Είναι το ΠΣύστημα, το οποίο διασυνδέεται με τον ακτινολογικό εξοπλισμό και το PACS, και χρησιμοποιείται για την αρχειοθέτηση και διακίνηση των εικόνων που παράγονται από τα ακτινολογικά τμήματα
	Medical Applications(Med Apps)	Είναι εξειδικευμένες εφαρμογές λογισμικού που μπορεί να είναι απαραίτητες για την διαχείριση και λειτουργία λοιπού ιατροτεχνολογικού εξοπλισμού
	e-Health	Συνοπτικά μπορούμε να θεωρήσουμε ότι περιλαμβάνει άλλα πληροφοριακά συστήματα που δεν περιγράφονται παραπάνω και αφορούν στην εφαρμογή τεχνολογιών πληροφορικής και επικοινωνιών στην παροχή ιατρικών υπηρεσιών κυρίως μέσω της χρήσης τεχνολογιών διαδικτύου. Ως τέτοια μπορούν να θεωρηθούν διάφορα δίκτυα πληροφοριών για την υγεία, ηλεκτρονικά μητρώα υγείας, υπηρεσίες τηλεϊατρικής και ατομικά ενδυτά και φορητά επικοινωνούντα συστήματα για την παρακολούθηση και στήριξη των ασθενών, συστήματα τηλεσυμβουλευτικής (teleconsultation),πλατφόρμες ηλεκτρονικής συνταγογράφησης (e-syntagografisi) και ηλεκτρονικής παραπομπής (e-diagnosis) κοκ.
ΔΙΟΙΚΗΤΙΚΑ	**Payroll Management Information System (PMIS)**	Είναι το ΠΣ το οποίο διαχειρίζεται τη μισθοδοσία του προσωπικού
	Human Resources Information System (HRIS)	Είναι το ΠΣ το οποίο χρησιμοποιείται για τη διαχείρισης ανθρωπίνων πόρων και μπορεί να περιλαμβάνει τη διαχείριση των προσωπικών δεδομένων του προσωπικού, την ωρομέτρηση της απασχόλησης, τον έλεγχο παρουσιών και αδειών, την αξιολόγηση της απόδοσης, την πρόσληψη νέου προσωπικού
	Quality Management Information System (QMIS)	Είναι το ΠΣ που υποβοηθά στη διαχείριση κινδύνου και στον σχεδιασμό πρόληψης και αντιμετώπισης ασυνήθιστων συμβάντων. Χρησιμοποιείται για την παρακολούθηση του συστήματος διαχείρισης ποιότητας και την παραγωγή αναφορών για την συνεχή βελτίωσή του
	Management Information System (MIS)	Είναι το ΠΣ το οποίο παρέχει τις απαραίτητες πληροφορίες σε κατάλληλη μορφή ώστε να βοηθά την εταιρική διαχείριση και τη λήψη αποφάσεων. Συνήθως επεξεργάζεται οικονομικές πληροφορίες συναρτήσει δεικτών μέτρησης της απόδοσης των επιχειρησιακών λειτουργιών
	Enterprise Resource Planning (ERP)	Είναι το ΠΣ το οποίο χρησιμοποιείται για τη διαχείριση των οικονομικών στοιχείων, λογαριασμών και συναλλαγών του οργανισμού. Είναι απαραίτητο για τη διαχείριση των εσόδων-εξόδων του οργανισμού, τη λειτουργία των υπηρεσιών λογιστηρίου και μπορεί να ενσωματώνει και άλλες λειτουργίες όπως η διαχείριση υλικού και προμηθειών
ΥΠΟΣΤΗΡΙΚΤΙΚΑ	**mail services**	Αφορά στον εξοπλισμό και τις υπηρεσίες που χρησιμοποιούνται για τη διακίνηση μηνυμάτων ηλεκτρονικού ταχυδρομείου
	file services	Αφορά στον εξοπλισμό και τις υπηρεσίες που χρησιμοποιούνται για το διαμοιρασμό αρχείων
	printing services	Αφορά στον εξοπλισμό και τις υπηρεσίες που χρησιμοποιούνται για εκτυπωτικές εργασίες
	web-portal	Αφορά την ηλεκτρονική διαδικτυακή πύλη του οργανισμού μέσω της οποίας μπορεί να πραγματοποιείται η ενημέρωση του κοινού, η ανταλλαγή πληροφοριών και η πρόσβαση σε υπηρεσίες ηλεκτρονικής υγείας
	Internet access or Wide Area Network (WAN)	Αφορά στον εξοπλισμό και τις υπηρεσίες οι οποίες εξυπηρετούν τη λειτουργία και επικοινωνία με δίκτυα πέραν του τοπικού και με τον παγκόσμιο ιστό
	Intranet access or Local Area Network (LAN)	Αφορά στον εξοπλισμό και τις υπηρεσίες οι οποίες εξυπηρετούν τη λειτουργία των τοπικών δικτύων
	Security software	Αφορά στον εξοπλισμό και τις υπηρεσίες που χρησιμοποιούνται για τη διασφάλιση των διακινούμενων δεδομένων

Πίνακας 1- Περιγραφή Πληροφοριακών Συστημάτων οργανισμού

Επιπτώσεις δυσλειτουργίας ΠΣ	ΧΑΜΗΛΗ	ΜΕΣΗ	ΥΨΗΛΗ
Νομικές-Κανονιστικές	Δεν προκύπτει αθέτηση νομικών ή κανονιστικών υποχρεώσεων. Δεν υπάρχει κίνδυνος για πρόστιμα. Δεν υπάρχει κίνδυνος για αγωγές και νομικές κυρώσεις. Δεν προκύπτει αιτία για διεξαγωγή εισαγγελικής έρευνας. (συνήθως αφορούν σε απλά δεδομένα)	Προκύπτει αθέτηση κυρίως κανονιστικών υποχρεώσεων. Κίνδυνος για ελάχιστα πρόστιμα. Περιορισμένος κίνδυνος για αγωγές και νομικές κυρώσεις. Δεν προκύπτει αιτία για διεξαγωγή εισαγγελικής έρευνας, αλλά μπορεί να υπάρξει κλήση για απολογία από επίσημη αρχή. (συνήθως αφορούν σε προσωπικά δεδομένα)	Προκύπτει αθέτηση νομικών ή κανονιστικών υποχρεώσεων. Υπάρχει κίνδυνος για υψηλά πρόστιμα. Υπάρχει κίνδυνος για αγωγές και νομικές κυρώσεις. Προκύπτει αιτία για διεξαγωγή εισαγγελικής έρευνας. (συνήθως αφορούν σε ευαίσθητα δεδομένα)
Οικονομικές	Ελάχιστη εως ανύπαρκτη στιγμιαία οικονομική απώλεια. Ελάχιστες επιπτώσεις στο λειτουργικό κόστος του οργανισμού. Ελάχιστη εως μηδενική απώλεια εσόδων. Αμελητέα επίδραση στα έσοδα του οργανισμού. Καμία επίπτωση στην οικονομική σταθερότητα.	Στιγμιαία οικονομική απώλεια. Αισθητές επιπτώσεις στο λειτουργικό κόστος του οργανισμού. Μερική απώλεια εσόδων. Αισθητή επίδραση στα έσοδα του οργανισμού.Αμελητέα επίπτωση στην οικονομική σταθερότητα.	Μεγάλη στιγμιαία οικονομική απώλεια. Έντονες επιπτώσεις στο λειτουργικό κόστος του οργανισμού. Υψηλή απώλεια εσόδων. Σημαντική επίπτωση στην οικονομική σταθερότητα του οργανισμού.
Λειτουργικές-Παραγωγικές	Ελάχιστη εως καθόλου επίπτωση στην παραγωγικότητα του οργανισμού. Χαμηλή εξάρτηση λειτουργιών από ΠΣ. Δυνατότητα απρόσκοπτης συνέχισης των λειτουργιών του οργανισμού με εναλλακτικό τρόπο (χειροκίνητα, χειρόγραφα).	Μερική επίπτωση στην παραγωγικότητα του οργανισμού. Υψηλή εξάρτηση λειτουργιών από ΠΣ. Δυνατότητα συνέχισης των λειτουργιών του οργανισμού με εναλλακτικό τρόπο (χειροκίνητα, χειρόγραφα) αλλά με υψηλή καθυστέρηση.	Καθοριστική επίπτωση στην παραγωγικότητα του οργανισμού. Υψηλή εξάρτηση λειτουργιών από ΠΣ. Αδυναμία συνέχισης των λειτουργιών του οργανισμού σε ανεκτό επίπεδο.
Υπόληψη-Υστεροφημία	Ελάχιστες επιπτώσεις. Απαιτειται ελάχιστη εως καθόλου προσπάθεια ανάκτησής της. Ελάχιστες ως μηδενικές απώλειες πελατών.	Μέτριες επιπτώσεις. Απαιτείται προσπάθεια για την ανάκτησή της. Μερική απώλεια πελατών.	Υψηλές επιπτώσεις. Η ανάκτησή της μπορεί να είναι μη αναστρέψιμη. Μαζική απώλεια πελατών.
Υγιεινή & Ασφάλεια	Δεν υπάρχει αξιόλογος κίνδυνος για τη ζωή, υγιεινή και ασφάλεια πελατών και προσωπικού.	Υπάρχει έμμεσος και περιορισμένος κίνδυνος για τη ζωή, υγιεινή και ασφάλεια πελατών και προσωπικού.	Υπάρχει άμεσος και ορατός κίνδυνος για τη ζωή, υγιεινή και ασφάλεια πελατών και προσωπικού.
Άλλες	Χαμηλή επίπτωση	Μέση επίπτωση	Υψηλή επίπτωση

Πίνακας 2- Κλίμακα επιπτώσεων

Σχέδιο Ανάκαμψης από Καταστροφές Πληροφοριακών Συστημάτων (IT DRP)

<Όνομα Οργανισμού>

Ιστορικό Εκδόσεων

ΕΚΔΟΣΗ	ΗΜΕΡΟΜΗΝΙΑ	ΣΥΝΤΑΞΗ	ΕΓΚΡΙΣΗ	ΠΕΡΙΓΡΑΦΗ
1.0 Αρχική				

Περιεχόμενα

1. Γενικά στοιχεία

1.1 Πλάνο Ανάκαμψης

1.1.1 Σκοπός και πεδίο εφαρμογής

Σκοπός του παρόντος πλάνου αποτελεί η ανάκαμψη των Πληροφοριακών Συστημάτων του οργανισμού με την επωνυμία <……..> σε περίπτωση που αυτά προσβληθούν από κάποιο καταστροφικό γεγονός. Το πλάνο ορίζει όλα τα εμπλεκόμενα πρόσωπα, καθορίζει τις αρμοδιότητες τους, περιέχει όλες τις απαραίτητες πληροφορίες και περιγράφει τις ενέργειες που πρέπει να ακολουθηθούν για την αποτελεσματική ανάκαμψη των Πληροφοριακών Συστημάτων.

Το πεδίο εφαρμογής του παρόντος πλάνου ορίζεται στην ανάκαμψη των Πληροφοριακών Συστημάτων που φιλοξενούνται στις υποδομές του οργανισμού καθώς και στην ανάκτηση της πρόσβασης σε Πληροφοριακά Συστήματα που φιλοξενούνται σε εξωτερικές υποδομές, αλλά κρίνονται απαραίτητα για τις καθημερινές λειτουργίες του οργανισμού και τη διατήρηση της επιχειρησιακής συνέχειας.

1.1.2 Υπεύθυνος Συντονισμού

Ο <Υπεύθυνος ΣΑΚ> μαζί με την <ομάδα ΣΑΚ> είναι οι μόνοι αρμόδιοι για την ενεργοποίηση και τον συντονισμό των διαδικασιών που περιγράφονται στο παρόν πλάνο.

Ρόλος	Όνομα	Τηλ.Κινητού	Τηλ.Σπιτιού	Τηλ.Εργασίας	E-mail
Υπεύθυνος ΣΑΚ					

1.1.3 Άμεσες ενέργειες

Με την εμφάνιση ενός καταστροφικού γεγονότος ή μιας δυσλειτουργίας στα ΠΣ, η οποία έχει γενικευμένη μορφή και δεν αποτελεί δυσλειτουργία ρουτίνας, θα πρέπει να ενημερώνεται άμεσα ο <*Υπεύθυνος ΣΑΚ*>.

Με την ενεργοποίηση του παρόντος, όλοι όσοι έχουν ενεργό ρόλο στο σχέδιο ανάκαμψης θα πρέπει να μεταβούν στους παρακάτω προκαθορισμένους χώρους ανάλογα με τις συνθήκες που επικρατούν.

Κατάσταση	Χώρος Συγκέντρωσης	Περιγραφή	Χρόνος συγκέντρωσης
Το αίτιο της καταστροφής δεν έχει παρέλθει. Καταστροφή με περιορισμένη επίπτωση στις κύριες εγκαταστάσεις, η οποία τις καθιστά μη προσβάσιμες ή με κίνδυνο τραυματισμού.	Κύριες εγκαταστάσεις (εκτός)	*<ΧΩΡΟΣ Α>*	ΑΜΕΣΑ
Το αίτιο της καταστροφής έχει παρέλθει. Καταστροφή με περιορισμένη επίπτωση στις κύριες εγκαταστάσεις.	Κύριες εγκαταστάσεις (εντός)	*<ΑΙΘΟΥΣΑ Α>*	<2 Ώρες
Μεγάλη επίπτωση στις κύριες εγκαταστάσεις και στην ευρύτερη περιοχή, καθιστώντας τες μη προσβάσιμες και μη λειτουργικές.	Εναλλακτικές εγκαταστάσεις	*<ΑΙΘΟΥΣΑ Β>*	<4 Ώρες

1.1.4 Εναλλακτικές εγκαταστάσεις

Σε περίπτωση που η καταστροφή δεν επιτρέπει την άμεση χρήση των κυρίως εγκαταστάσεων και υποδομών (παροχή ηλεκτρισμού, δομημένη καλωδίωση, τηλεπικοινωνίες) του κέντρου ελέγχου των ΠΣ, τότε η ανάκαμψη λαμβάνει χώρα σε εναλλακτικές εγκαταστάσεις. Αυτές οι εναλλακτικές εγκαταστάσεις ορίζονται στον παρακάτω πίνακα και είναι τύπου **WARM Site**. (Διατίθενται κατάλληλες υποδομές και ο απαραίτητος εξοπλισμός ώστε να χρησιμοποιηθούν, ύστερα από απαραίτητες ρυθμίσεις και με ανάκτηση δεδομένων από αντίγραφα ασφαλείας. Διατίθεται λίστα πόρων στο ΠΑΡΑΡΤΗΜΑ.)

Εγκατάσταση	Τύπος	Περιοχή	Διεύθυνση	Υπεύθυνος Επικοινωνίας	Τηλέφωνο	Παρατηρήσεις
Κυρίως Εγκαταστάσεις	MAIN Site					
Εναλλακτικές Εγκαταστάσεις	WARM Site					

1.1.5 Τόπος φύλαξης Σχεδίου Ανάκαμψης

Αντίγραφα του παρόντος σχεδίου τηρούνται τόσο στις κύριες εγκαταστάσεις όσο και στις εναλλακτικές σε διασφαλισμένο χώρο.

Εγκαταστάσεις	Χώρος φύλαξης
Κύριες εγκαταστάσεις	*<ΑΙΘΟΥΣΑ Α>*
Εναλλακτικές εγκαταστάσεις	*<ΑΙΘΟΥΣΑ Β>*

1.2 Οργανισμός

1.2.1 Περιγραφή οργανισμού

Ο οργανισμός με την επωνυμία <……> αποτελεί φορέα παροχής υπηρεσιών πρωτοβάθμιας υγείας, του οποίου το πεδίο δράσης εκτείνεται στην ευρύτερη μητροπολιτική περιοχή στην οποία βρίσκονται οι εγκαταστάσεις του. Στόχος του είναι η αδιάλειπτη παροχή υπηρεσιών υγείας στους πολίτες και η ενσωμάτωση σύγχρονων τεχνολογιών Πληροφορικής και Επικοινωνιών για την εκσυγχρονισμένη και αποτελεσματικότερη διεκπαιρέωσή τους.

Τα εφαρμοζόμενα ΠΣ κρίνονται καίριας σημασίας για την λειτουργία του οργανισμού καθώς επιτρέπουν τη λειτουργία του στο μοντέλο του ψηφιακού νοσοκομείου (paperless/ filmless hospital) καθώς και επιτρέπουν την εφαρμογή υπηρεσιών ηλεκτρονικής υγείας (eHealth).

1.2.2 Περιγραφή Πληροφοριακών Συστημάτων

Το Ολοκληρωμένο Πληροφοριακό Σύστημα του οργανισμού απαρτίζεται από διακριτά υποσυστήματα σύμφωνα με τον παρακάτω πίνακα. Για ευκολία ταξινομούνται σε Κλινικά (όσα υποστηρίζουν υπηρεσίες υγείας), Διοικητικά (όσα υποστηρίζουν διοικητικές λειτουργίες) και λοιπά Υποστηρικτικά (όσα υποστηρίζουν λοιπές λειτουργίες).

	Πληροφοριακό Σύστημα	Περιγραφή
ΙΑΤΡΙΚΑ	**Electronic Health Records (EHR)**	Αναφέρεται συνήθως ως Ηλεκτρονικός Ιατρικός Φάκελος και χρησιμοποιείται για τη συλλογή και επεξεργασία πληροφοριών για την υγεία των ασθενών. Προσφέρεται για τη διαχείριση ιατρείων και ασθενών και την εξαγωγή στατιστικών στοιχείων και στην ουσία αποτελεί τη μεταφορά του έντυπου ιατρικού φακέλου ασθενών σε ηλεκτρονική μορφή. Όταν διασυνδέεται με άλλα ΠΣ μπορεί να περιλαμβάνει και αποτελέσματα εργαστηριακών και ακτινολογικών εξετάσεων
	Laboratory Information System (LIS)	Είναι το ΠΣ των Ιατρικών Εργαστηρίων, το οποίο συνήθως είναι διασυνδεδεμένο με κατάλληλο εργαστηριακό εξοπλισμό, με σκοπό την αποθήκευση και διακίνηση αποτελεσμάτων εργαστηριακών εξετάσεων (αιματολογικών, μικροβιολογικών, βιοπαθολογικών κοκ)
	Picture archiving and communication system (PACS)	Είναι το ΠΣ, το οποίο διασυνδέεται με τον ακτινολογικό εξοπλισμό και το PACS, και χρησιμοποιείται για την αρχειοθέτηση και διακίνηση των εικόνων που παράγονται από τα ακτινολογικά τμήματα
	Medical Applications(Med Apps)	Είναι εξειδικευμένες εφαρμογές λογισμικού που μπορεί να είναι απαραίτητες για την διαχείριση και λειτουργία λοιπού ιατροτεχνολογικού εξοπλισμού
	e-Health	Συνοπτικά μπορούμε να θεωρήσουμε ότι περιλαμβάνει άλλα πληροφοριακά συστήματα που δεν περιγράφονται παραπάνω και αφορούν στην εφαρμογή τεχνολογιών πληροφορικής και επικοινωνιών στην παροχή ιατρικών υπηρεσιών κυρίως μέσω της χρήσης τεχνολογιών διαδικτύου. Ως τέτοια μπορούν να θεωρηθούν διάφορα δίκτυα πληροφοριών για την υγεία, ηλεκτρονικά μητρώα υγείας, υπηρεσίες τηλεϊατρικής και ατομικά ενδυτά και φορητά επικοινωνούντα συστήματα για την παρακολούθηση και στήριξη των ασθενών, συστήματα τηλεσυμβουλευτικής (teleconsultation), πλατφόρμες ηλεκτρονικής συνταγογράφησης (e-syntagografisi) και ηλεκτρονικής παραπομπής (e-diagnosis) κοκ.
ΔΙΟΙΚΗΤΙΚΑ	**Payroll Management Information System (PMIS)**	Είναι το ΠΣ το οποίο διαχειρίζεται τη μισθοδοσία του προσωπικού
	Human Resources Information System (HRIS)	Είναι το ΠΣ το οποίο χρησιμοποιείται για τη διαχείρισης ανθρωπίνων πόρων και μπορεί να περιλαμβάνει τη διαχείριση των προσωπικών δεδομένων του προσωπικού, την ωρομέτρηση της απασχόλησης, τον έλεγχο παρουσιών και αδειών, την αξιολόγηση της απόδοσης, την πρόσληψη νέου προσωπικού
	Quality Management Information System (QMIS)	Είναι το ΠΣ που υποβοηθά στη διαχείριση κινδύνου και στον σχεδιασμό πρόληψης και αντιμετώπισης ασυνήθιστων συμβάντων. Χρησιμοποιείται για την παρακολούθηση του συστήματος διαχείρισης ποιότητας και την παραγωγή αναφορών για την συνεχή βελτίωσή του
	Management Information System (MIS)	Είναι το ΠΣ το οποίο παρέχει τις απαραίτητες πληροφορίες σε κατάλληλη μορφή ώστε να βοηθά την εταιρική διαχείριση και τη λήψη αποφάσεων. Συνήθως επεξεργάζεται οικονομικές πληροφορίες συναρτήσει δεικτών μέτρησης της απόδοσης των επιχειρησιακών λειτουργιών
	Enterprise Resource Planning (ERP)	Είναι το ΠΣ το οποίο χρησιμοποιείται για τη διαχείριση των οικονομικών στοιχείων, λογαριασμών και συναλλαγών του οργανισμού. Είναι απαραίτητο για τη διαχείριση των εσόδων-εξόδων του οργανισμού, τη λειτουργία των υπηρεσιών λογιστηρίου και μπορεί να ενσωματώνει και άλλες λειτουργίες όπως η διαχείριση υλικού και προμηθειών
ΥΠΟΣΤΗΡΙΚΤΙΚΑ	**Mail services**	Αφορά στον εξοπλισμό και τις υπηρεσίες που χρησιμοποιούνται για τη διακίνηση μηνυμάτων ηλεκτρονικού ταχυδρομείου
	File services	Αφορά στον εξοπλισμό και τις υπηρεσίες που χρησιμοποιούνται για το διαμοιρασμό αρχείων
	Printing services	Αφορά στον εξοπλισμό και τις υπηρεσίες που χρησιμοποιούνται για εκτυπωτικές εργασίες
	Web-portal	Αφορά την ηλεκτρονική διαδικτυακή πύλη του οργανισμού μέσω της οποίας μπορεί να πραγματοποιείται η ενημέρωση του κοινού, η ανταλλαγή πληροφοριών και η πρόσβαση σε υπηρεσίες ηλεκτρονικής υγείας
	Internet access or Wide Area Network (WAN)	Αφορά στον εξοπλισμό και τις υπηρεσίες οι οποίες εξυπηρετούν τη λειτουργία και επικοινωνία με δίκτυα πέραν του τοπικού και με τον παγκόσμιο ιστό
	Intranet access or Local Area Network (LAN)	Αφορά στον εξοπλισμό και τις υπηρεσίες οι οποίες εξυπηρετούν τη λειτουργία των τοπικών δικτύων
	Security software	Αφορά στον εξοπλισμό και τις υπηρεσίες που χρησιμοποιούνται για τη διασφάλιση των διακινούμενων δεδομένων

1.2.3 Πιθανοί κίνδυνοι

Στον παρακάτω πίνακα παρουσιάζονται οι κυριότερες καταστροφές από τις οποίες απειλούνται τα ΠΣ και κατανέμονται ως προς το βαθμό επικινδυνότητας σε κλίμακα 1-15. Το παρόν σχέδιο εστιάζει στην αντιμετώπιση καταστροφών με **βαθμό επικινδυνότητας >7**.

Είδος Καταστροφής	Πιθανότητα Εμφάνισης (P)	Επιπτώσεις (I)	Επικινδυνότητα (R=P*I)	Προληπτικά Μέτρα	Επάρκεια Προληπτικών Μέτρων	Παρατηρήσεις
Φυσικές καταστροφές						
σεισμοί	3	3	**9**			
πυρκαγιές	3	3	**9**	χρήση ανιχνευτών, συστήματα πυρόσβεσης	2	
πλημμύρες	3	3	**9**	χρήση ανιχνευτών	1	
τυφώνες	1	2	2			
κατολισθήσεις	1	3	3			
ηφαίστεια	1	3	3			
ακραία καιρικά φαινόμενα	2	2	4			
Ανθρώπινα λάθη						
ατυχήματα	3	2	6	εφαρμογή OHSAS 18001:2007	3	
διαρροή επικίνδυνων ουσιών/μόλυνση	3	1	3	εφαρμογή ISO14001:2004	3	
Ανθρώπινος δόλος:						
τρομοκρατικές ενέργειες	1	3	3	υπηρεσίες φύλαξης	3	
hacking	3	2	6	εξοπλισμός προστασίας	3	
κλοπή υλικού/δεδομένων	4	2	**8**	υπηρεσίες φύλαξης, συστήματα έλεγχος πρόσβασης, εφαρμογή ISO27001:2005	3	
εξεγέρσεις/κοινωνικές αναταραχές	1	1	1	υπηρεσίες φύλαξης	1	
Τεχνολογικά:						
δυσλειτουργία εξοπλισμού	5	2	**10**	εφεδρικά συστήματα	2	
λάθη συστήματος	5	2	**10**	αντίγραφα ασφαλείας	2	
πτώση/απώλεια ενέργειας	5	1	5	εφεδρικά συστήματα (UPS, H/Z)	3	
απώλεια επικοινωνιών	5	1	5			
Άλλες						
πανδημίες	2	1	2			
οικονομική κατάρρευση	2	1	2			

Όπου:

Βαθμός	Πιθανότητα (P)	Περιγραφή
1	ΠΟΛΥ ΧΑΜΗΛΗ	Εμφάνιση σχεδόν ποτέ
2	ΧΑΜΗΛΗ	Εμφάνιση σπάνια (μεμονωμένα περιστατικά και σε βάθος χρόνου)
3	ΜΕΣΗ	Αυξημένος κίνδυνος εμφάνισης (παρόλο που μπορεί να μην έχει αναφερθεί σχετικά πρόσφατο περιστατικό, κρίνεται πιθανή η εμφάνισή του)
4	ΥΨΗΛΗ	Εμφάνιση συχνά (μια φορά το χρόνο)
5	ΠΟΛΥ ΥΨΗΛΗ	Εμφάνιση πολύ συχνά (περισσότερο από μια φορά το χρόνο)

Βαθμός	Επίπτωση (I)	Περιγραφή
1	ΧΑΜΗΛΗ	Σύντομη διακοπή ΠΣ
2	ΜΕΣΗ	Μερική καταστροφή ΠΣ
3	ΥΨΗΛΗ	Πλήρης καταστροφή ΠΣ

1.2.4 Εφαρμοζόμενα προληπτικά μέτρα

Τα προληπτικά μέτρα που εφαρμόζονται για την αντιμετώπιση των καταστροφών αναφέρονται στον προηγούμενο πίνακα και αξιολογούνται ως προς την επάρκειά τους ως εξής:

Βαθμός	Επάρκεια	Περιγραφή
1	ΧΑΜΗΛΗ	Παρέχουν κυρίως δυνατότητα έγκαιρης ανίχνευσης
2	ΜΕΣΗ	Παρέχουν δυνατότητες μερικής αντιμετώπισης των επιπτώσεων
3	ΥΨΗΛΗ	Παρέχουν δυνατότητες πρόληψης, αποτρέποντας την εμφάνιση της αιτίας

2. Στόχοι

Μετά από ανάλυση των επιχειρησιακών επιπτώσεων (BIA) μιας ενδεχόμενης καταστροφής των ΠΣ, όπως αυτή παρατίθεται στο ΠΑΡΑΡΤΗΜΑ, καθορίζονται οι παρακάτω γενικοί και ειδικοί στόχοι.

2.1 Παραδοχές

Το παρόν σχέδιο:

- έχει συσταθεί με γνώμονα την ολοκληρωτική απώλεια των ΠΣ του οργανισμού από κάποιο καταστροφικό περιστατικό. Ωστόσο είναι δυνατό να χρησιμοποιηθεί και για περιστατικά που προκαλούν περιορισμένη ή μερική απώλεια των ΠΣ.
- στοχεύει στην αντιμετώπιση καταστροφών οι οποίες δεν είναι ικανές να πλήξουν ταυτόχρονα και τις κύριες και τις εναλλακτικές εγκαταστάσεις.
- απευθύνεται κυρίως σε πρόσωπα τα οποία είναι εξοικειωμένα με τα ΠΣ του οργανισμού. Για το λόγο αυτό έχει αποφευχθεί το υψηλό επίπεδο λεπτομέρειας στις περιγραφόμενες ενέργειες.
- Οι χρόνοι ανάκαμψης (RTO, RPO) λογίζονται από τη στιγμή που θα ενεργοποιηθεί το παρόν σχέδιο.

2.2 Γενικοί στόχοι

Ειδοποίηση/Ενεργοποίηση: Η Ειδοποίηση σε περίπτωση καταστροφής θα πρέπει να είναι **ΑΜΕΣΗ**. Η Ενεργοποίηση του παρόντος σχεδίου καθώς και η απόφαση χρήσης η μη των Εναλλακτικών εγκαταστάσεων θα πρέπει να έχει παρθεί **εντός 4 Ωρών**.

Ανάκαμψη: η Ανάκαμψη των ΠΣ είτε λάβει χώρα στις κύριες εγκαταστάσεις είτε στις εναλλακτικές θα πρέπει να πραγματοποιηθεί βάσει του πίνακα στην §2.4 (Χρόνοι MTD), σε χρόνο **1-5 Ημερών**.

Ανασύσταση/Επαναφορά Κυρίως εγκαταστάσεων: Οι εναλλακτικές εγκαταστάσεις θα πρέπει να είναι σε θέση να φιλοξενήσουν τα ΠΣ για χρόνο ίσο **με 2 Εβδομάδες**, στη διάρκεια του οποίου θα πρέπει να έχουν αποκατασταθεί οι κυρίως εγκαταστάσεις και να είναι σε θέση να φιλοξενήσουν και πάλι τα ΠΣ.

2.3 Κρίσιμες λειτουργίες

Στον παρακάτω πίνακα παρατίθενται οι κρισιμότερες λειτουργίες του οργανισμού ταξινομημένες σύμφωνα με την προτεραιότητα με την οποία πρέπει να ανακαμφθούν. Στον ίδιο πίνακα φαίνονται και οι χρόνοι-στόχοι μέσα στους οποίους πρέπει να πραγματοποιηθεί η ανάκαμψη για κάθε μια από αυτές.

Α/Α	Οργανωτικές Μονάδες	Λειτουργίες ανά Μονάδα	MTD	CI	RPO
1	**Κλινική Φροντίδα**	Υπηρεσίες υγείας	**1Η**	15	**1Η**
2	**Ιατρικές Απεικονίσεις**	Υπηρεσίες υγείας	**1Η**	15	**1Η**
3	**Αποκατάσταση-Αποθεραπεία**	Υπηρεσίες υγείας	**1Η**	15	**1Η**
4	**Βιοπαθολογικά Εργαστήρια**	Διενέργεια εργαστηριακών εξετάσεων	**1Η**	15	**1Η**
5	**Υπηρεσίες Πληροφορικής**	Ασφάλεια ΠΣ-Πληροφοριών	**1Η**	12	**1Η**
6	**Υπηρεσίες Πληροφορικής**	Υποστήριξη ΠΣ	**1Η**	10	**1Ε**
7	**Διοικητικές Υπηρεσίες**	Κλείσιμο ραντεβού	**1Η**	10	**1Η**
8	**Οικονομικές Υπηρεσίες**	Υπηρεσίες Λογιστηρίου (Τιμολόγηση)	**3Η**	11	**1Η**
9	**Υπηρεσίες Βιοϊατρικής Τεχνολογίας**	Υποστήριξη Βιοϊατρικού εξοπλισμού	**3Η**	8	**1Ε**
10	**Οικονομικές Υπηρεσίες**	Σχεδιασμός-Εκτέλεση προϋπολογισμού	**1Ε**	10	**1Ε**
11	**Οικονομικές Υπηρεσίες**	Προμήθεια και διαχείριση υλικού	**1Ε**	8	**1Ε**
12	**Διοικητικές Υπηρεσίες**	Διαχείριση Ανθρωπίνου Δυναμικού	**1Ε**	8	**1Ε**
13	**Υπηρεσίες Ολικής Ποιότητας**	Έλεγχος Συστήματος Ποιότητας	**1Ε**	8	**1Ε**
14	**Τεχνικές Υπηρεσίες**	Υποστήριξη Υποδομών	**1Ε**	7	**1Ε**
15	**Διοικητικές Υπηρεσίες**	Γραμματειακή υποστήριξη	**1Ε**	6	**1Ε**
16	**Νομικές Υπηρεσίες**	Νομικές Υπηρεσίες	**1Ε**	6	**1Ε**
17	**Υπηρεσίες Εσωτερικού Ελέγχου**	Εσωτερικός Έλεγχος	**1Ε**	6	**1Ε**
18	**Οικονομικές Υπηρεσίες**	Έκδοση μισθοδοσίας	**1Ε**	5	**1Ε**

MTD : Maximum Tolerable Downtime

CI : Criticality Indicator

RPO : Recovery Point Objective

Ω : Ώρα

Η : Ημέρα

Ε : Εβδομάδα

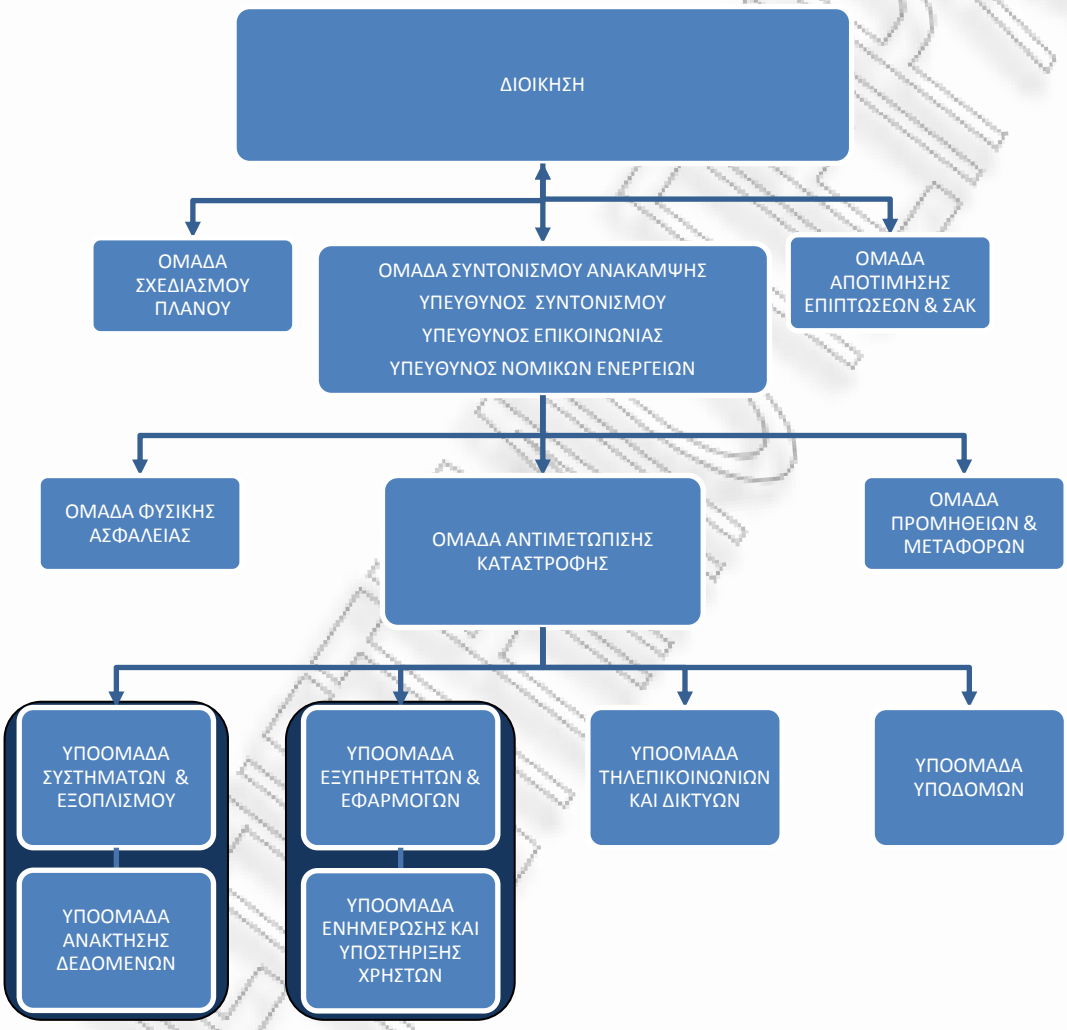
2.4 Κρίσιμοι Πληροφοριακοί πόροι

Σύμφωνα με την ανάλυση επικινδυνότητας, και με βάση την ταξινόμηση των κρίσιμων λειτουργιών, στον παρακάτω πίνακα παρατίθεται η προτεραιότητα και οι χρόνοι-στόχοι βάσει των οποίων θα πρέπει να πραγματοποιηθεί η ανάκαμψη των Πληροφοριακών Συστημάτων του οργανισμού.

Α/Α	ΠΛΗΡΟΦΟΡΙΑΚΟ ΣΥΣΤΗΜΑ	MTD	CI	RPO
1	**Intranet (LAN)**	1H	15	1H
2	**printing services**	1H	15	1H
3	**EHR**	1H	15	1H
4	**Internet (WAN)**	1H	15	1H
5	**RIS/PACS**	1H	15	1H
6	**e-Health**	1H	15	1H
7	**LIS**	1H	15	1H
8	**MED APPS**	1H	15	1H
9	**security services**	1H	12	1H
10	**file services**	1H	10	1E
11	**mail services**	1H	10	1H
12	**web portal**	1H	10	1E
13	**ERP**	3H	11	1H
14	**QMIS**	3H	8	1E
15	**MIS**	1E	10	1E
16	**HRIS**	1E	8	1E
17	**PMIS**	1E	5	1E

3. Ρόλοι & Αρμοδιότητες

3.1 Οργανόγραμμα



3.2 Υπεύθυνοι

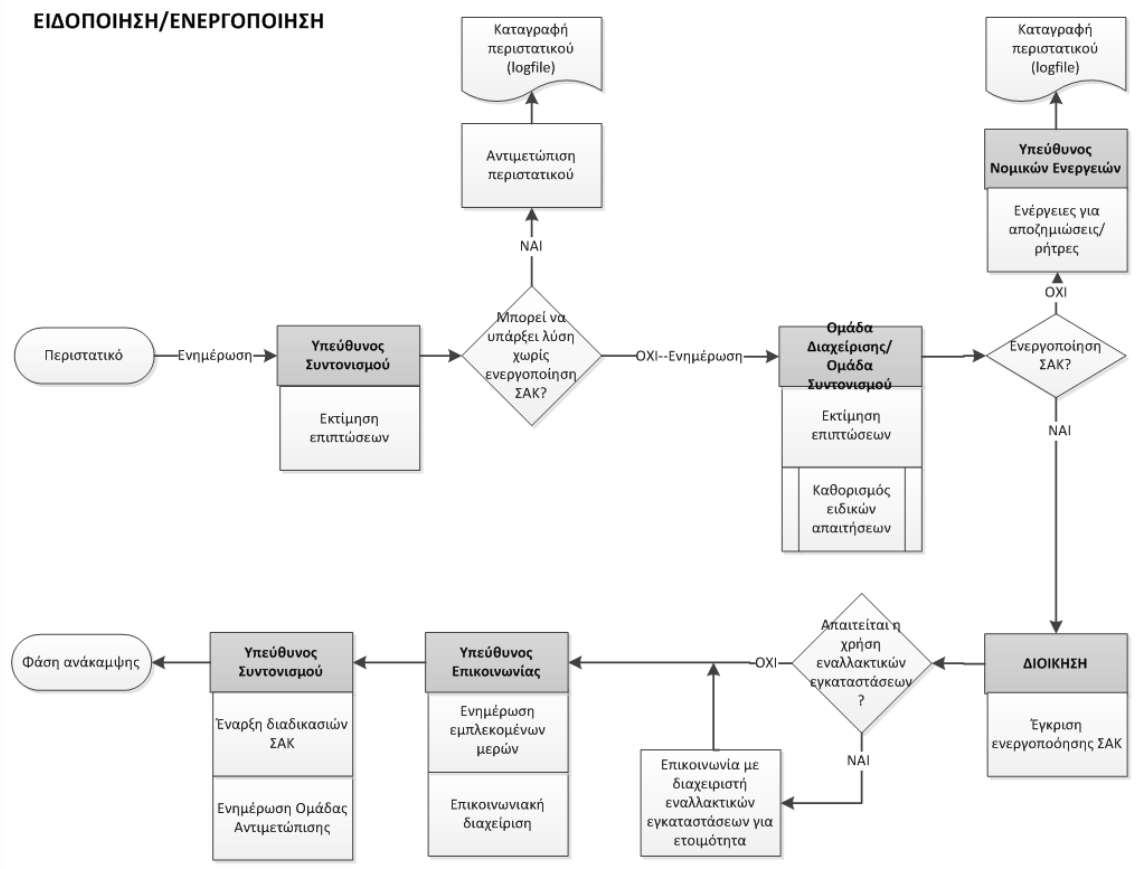
Ρόλος	Περιγραφή
Υπεύθυνος Συντονισμού	Αναφέρεται απευθείας στη Διοίκηση. Φέρει την κύρια ευθύνη για το σχεδιασμό, λειτουργία και συντήρηση του ΣΑΚ και δρα ως ενορχηστρωτής όλων των εμπλεκομένων μερών. Μπορεί να ηγείται τόσο της Ομάδας Διαχείρισης ΣΑΚ όσο και της Ομάδας Αντιμετώπισης Καταστροφής.
Υπεύθυνος Επικοινωνίας	Είναι μέλος της Ομάδας Διαχείρισης ΣΑΚ και υπεύθυνος για την επικοινωνιακή διαχείριση της καταστροφής. Αναλαμβάνει να ενημερώσει όλους τους άμεσα εμπλεκόμενους (πελάτες, προμηθευτές, προσωπικό, διοίκηση) έγκαιρα και έγκυρα προλαμβάνοντας φαινόμενα πανικού και διασφαλίζοντας την υπόληψη του οργανισμού.
Υπεύθυνος Επικαιροποίησης	Είναι υπεύθυνος για την επικαιροποίηση του ΣΑΚ και την αναθεώρησή του όποτε και αν απαιτείται. Αναλαμβάνει μετά από κάθε αλλαγή είτε στις λειτουργίες/υπηρεσίες του οργανισμού είτε στα ΠΣ να εξετάσει κατά πόσο απαιτείται προσαρμογή του ΣΑΚ.
Υπεύθυνος Νομικών ενεργειών	Είναι υπεύθυνος για τη νομική κάλυψη του οργανισμού που αφορούν στην εκδήλωση κάποιας καταστροφής. Φέρει την ευθύνη να εντοπίσει όλες τις νομικές υποχρεώσεις στις οποίες υποχρεούται να συμμορφώνεται ο οργανισμός κυρίως όσον αφορά τα προσβεβλημένα δεδομένα σε σχέση με τρίτους (πελάτες, προσωπικό). Παράλληλα επικουρεί στην δημιουργία ρητρών στις συμβάσεις προμήθειας υπηρεσιών/υλικών με τρόπο που να εξυπηρετεί τις ανάγκες του ΣΑΚ. Κινεί άμεσα όλες τις απαραίτητες διαδικασίες, εφόσον προβλέπονται, για την αποζημίωση του οργανισμού από ασφαλιστήρια συμβόλαια κινδύνου ή ρήτρες (SLAs).
Υπεύθυνος Εκπαίδευσης	Φέρει την ευθύνη για την επαρκή και συνεχή εκπαίδευση όλων των εμπλεκομένων μερών. Εισηγείται τις εκπαιδευτικές ανάγκες του άμεσα εμπλεκόμενου προσωπικού. Προγραμματίζει και σχεδιάζει τις απαραίτητες ασκήσεις που απαιτούνται για τη δοκιμή του ΣΑΚ.

3.3 Ομάδες

Ομάδα	Περιγραφή
Ομάδα Διαχείρισης ΣΑΚ	Είναι η ομάδα που φέρει την ευθύνη για την πλήρη διαχείριση και εφαρμογή του ΣΑΚ και αναφέρεται στη Διοίκηση του Οργανισμού. Αποτελείται από το σύνολο των Υπευθύνων, όπως περιγράφονται παραπάνω, με επικεφαλής τον Υπεύθυνο Συντονισμού. Ανάλογα με την χρονική περίοδο σε σχέση με την εκτέλεση ενός ΣΑΚ δηλαδή πριν, κατά τη διάρκεια, η μετά την ολοκλήρωσή του η Ομάδα αυτή μπορεί να αναλάβει διαφορετικό ρόλο όπως περιγράφεται παρακάτω.
(Ομάδα Σχεδιασμού Πλάνου)	Φέρει την ευθύνη για το σχεδιασμό, τη βελτίωση και τον έλεγχο της λειτουργικότητας του ΣΑΚ. Το έργο της αφορά κυρίως στον προπαρασκευαστικό τομέα και πριν την εμφάνιση κάποιας καταστροφής. Μπορεί να περιλαμβάνει επιπρόσθετα και έμπειρα μέλη από την Ομάδα Αντιμετώπισης Καταστροφής.
(Ομάδα Συντονισμού Ανάκαμψης)	Αναλαμβάνει δράση με την εμφάνιση και αναγνώριση κάποιου περιστατικού καταστροφής και είναι υπεύθυνη για το συντονισμό του ΣΑΚ. Αποφασίζει για την ενεργοποίηση ή μη του ΣΑΚ, την επιλογή της ακολουθούμενης στρατηγικής και τη λήψη εκτελεστικών αποφάσεων. Εισηγείται στη Διοίκηση για σημαντικά θέματα όπως η αναγκαιότητα μετάβασης σε εναλλακτικές εγκαταστάσεις και αναλαμβάνει την εν γένει επικοινωνία και αλληλεπίδραση με τρίτους.
(Ομάδα Αποτίμησης ΣΑΚ)	Με την ολοκλήρωση του ΣΑΚ και την επιστροφή στο επίπεδο λειτουργικότητας πριν την καταστροφή η ομάδα αυτή καλείται να αποτιμήσει τις επιπτώσεις και τις όποιες συνέπειες της καταστροφής. Αναλύει την αποτελεσματικότητα του ΣΑΚ και προτείνει τυχόν διορθωτικές ενέργειες που απαιτούνται για την βελτίωσή του.
Ομάδα Αντιμετώπισης Καταστροφής	Η ομάδα αυτή είναι υπεύθυνη για το γενικό συντονισμό και την εφαρμογή ενεργειών για την αποκατάσταση/ανάκαμψη κυρίως σε τεχνικό/τεχνολογικό επίπεδο είτε στις τοπικές είτε στις εναλλακτικές εγκαταστάσεις. Αναλαμβάνει δράση με την απόφαση ενεργοποίησης του ΣΑΚ και αναφέρεται στον Υπεύθυνο Συντονισμού. Ανάλογα με την πολυπλοκότητα των Πληροφοριακών Συστημάτων η ομάδα αυτή μπορεί να διαχωρίζεται σε υποομάδες, όπως περιγράφονται παρακάτω.
Υποομάδα Υποδομών	Είναι υπεύθυνη για την αποκατάσταση των απαραίτητων υποδομών για τη λειτουργία των ΠΣ. Οι υποδομές αυτές μπορεί να αφορούν εξοπλισμό γραφείου, ισχυρά και ασθενή ρεύματα, δομημένη καλωδίωση.
Υποομάδα Συστημάτων και Περιφερειακών	Είναι υπεύθυνη για την αποκατάσταση της λειτουργίας των συστημάτων των χρηστών και του λοιπού περιφερειακού εξοπλισμού. (σταθμοί εργασίας, εκτυπωτές)
Υποομάδα Εξυπηρετητών και Εφαρμογών	Είναι υπεύθυνη για την αποκατάσταση της λειτουργίας των εξυπηρετητών καθώς και των κρίσιμων εφαρμογών του οργανισμού. (λειτουργικά συστήματα, η-υπηρεσίες)
Υποομάδα Τηλεπικοινωνιών και δικτύων	Είναι υπεύθυνη για την αποκατάσταση των τηλεπικοινωνιακών και δικτυακών υπηρεσιών. (LAN, WAN, WWW)
Υποομάδα Ανάκτησης δεδομένων	Είναι υπεύθυνη για τη διενέργεια δράσεων και για το συντονισμό ενεργειών για την ανάκτηση-αποκατάσταση όλων των δεδομένων. (αντίγραφα ασφαλείας, βάσεις δεδομένων)
Υποομάδα Ενημέρωσης και υποστήριξης χρηστών	Η ομάδα αυτή αποτελεί τον επικοινωνιακό δίαυλο της Ομάδας Αντιμετώπισης τόσο μεταξύ των Υποομάδων όσο και προς τις ιεραρχικά ανώτερες ομάδες. Αναλαμβάνει να ενημερώσει τους χρήστες του οργανισμού για την κατάσταση των ΠΣ και με σαφήνεια να τους υποδείξει τις αλλαγές στον τρόπο χειρισμού που απαιτούνται μέχρι την πλήρη επαναφορά σε κανονική λειτουργία. Παράλληλα αναλαμβάνει να υποδείξει εναλλακτικούς τρόπους με τους οποίους μπορούν να καλύψουν τις ανάγκες τους.
Ομάδα Προμηθειών και Μεταφοράς	Η ομάδα αυτή είναι υπεύθυνη για την εξασφάλιση επαρκών προμηθειών (υλικών, εξοπλισμού, αναλωσίμων) που μπορεί να απαιτηθούν κατά την ανάκαμψη. Ταυτόχρονα είναι υπεύθυνη για την έγκαιρη μεταφορά τους είτε στις κύριες είτε στις εναλλακτικές εγκαταστάσεις. Αναφέρεται στην Ομάδα Συντονισμού.
Ομάδα Φυσικής ασφάλειας	Η ομάδα αυτή είναι υπεύθυνη για τη φυσική ασφάλεια των εγκαταστάσεων κατά την εκτέλεση του ΣΑΚ. Ασφαλίζει τις πληγείσες εγκαταστάσεις αλλά και τις εναλλακτικές από παράνομη πρόσβαση, για όσο διαρκεί η διαδικασία ανάκαμψης, διατηρώντας λίστα εγκεκριμένων προσώπων. Αναφέρεται στην Ομάδα Συντονισμού.

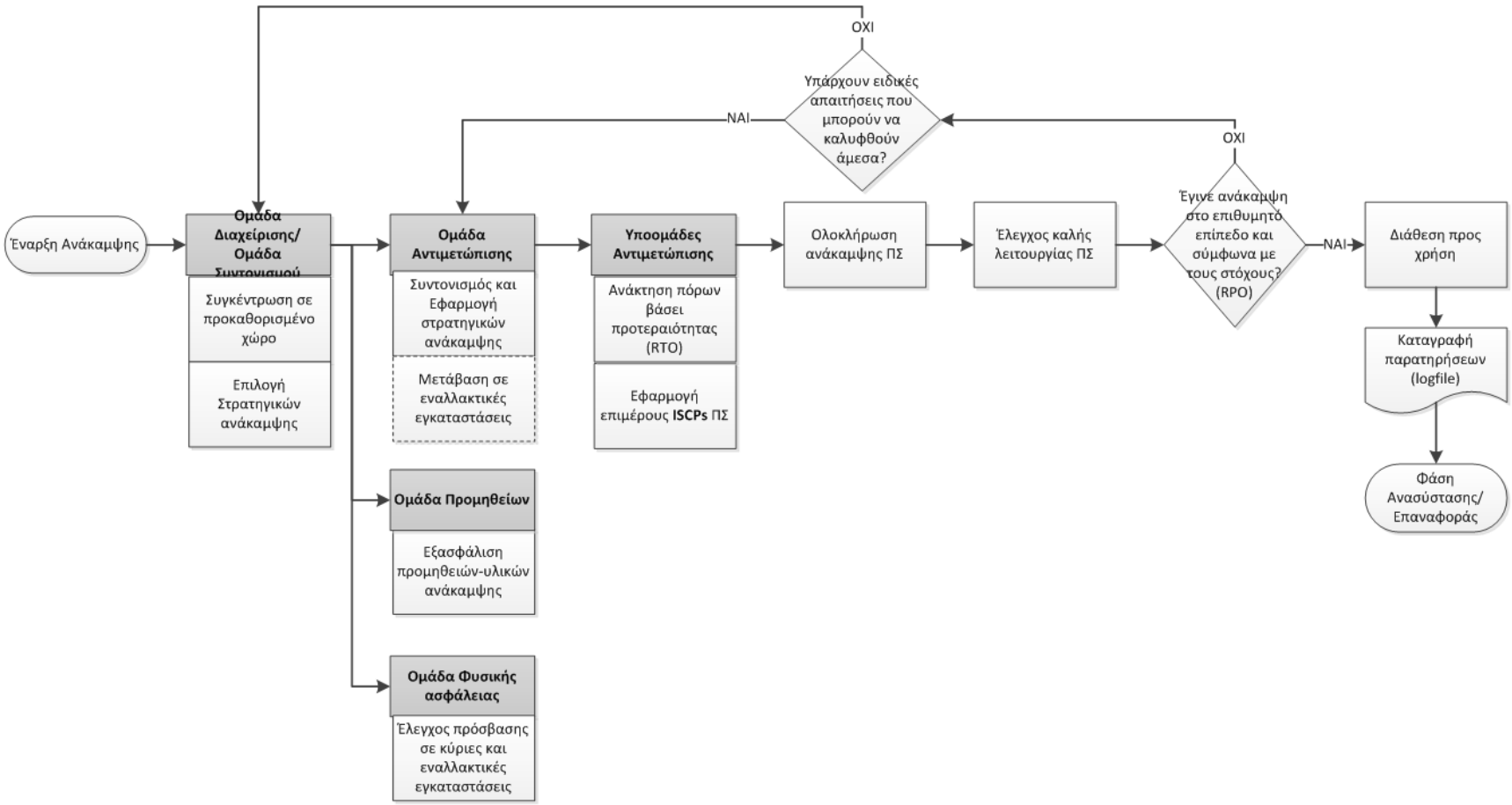
4. Ενέργειες Αντιμετώπισης

4.1 Ειδοποίηση/ενεργοποίηση



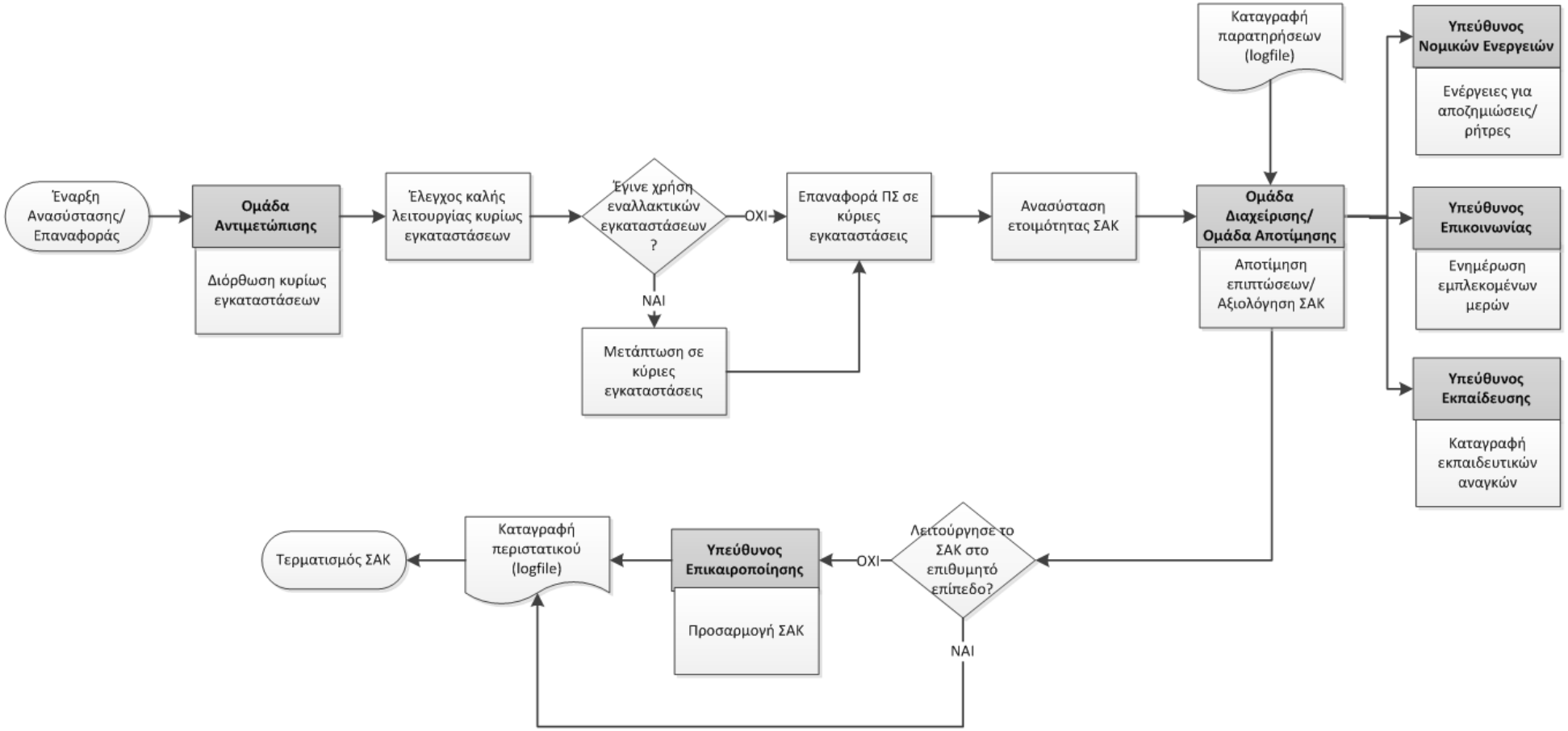
4.2 Ανάκαμψη

ΑΝΑΚΑΜΨΗ



4.3 Ανασύσταση/επαναφορά

ΑΝΑΣΥΣΤΑΣΗ/ΕΠΑΝΑΦΟΡΑ



5. Στρατηγικές και μέτρα ανάκαμψης

5.1 Εφαρμοζόμενες στρατηγικές

Οι εφαρμοζόμενες στρατηγικές ανάκαμψης ανά ΠΣ παρατίθενται στο ΠΑΡΑΡΤΗΜΑ.

5.2 Πολιτική αντιγράφων ασφαλείας

Η πολιτική που ακολουθείται για τα αντίγραφα ασφαλείας σε κάθε ΠΣ καθορίζεται από την απαιτούμενη τιμή του RPO. Διακρίνονται οι εξής περιπτώσεις:

Α. Φύλαξη εντός, στις κύριες εγκαταστάσεις

- Εβδομαδιαίο αντίγραφο με πλήρη (Full) λήψη και αποθήκευση σε Δίσκο (HD)
- Ημερήσιο αντίγραφο με διαφορική (Differential) λήψη και αποθήκευση σε Δίσκο (HD)

Β. Φύλαξη/Μεταφορά εκτός, στις εναλλακτικές εγκαταστάσεις

- Εβδομαδιαίο αντίγραφο με πλήρη (Full) λήψη και αποθήκευση σε Κασέτα (Tape)
- Ημερήσιο αντίγραφο με διαφορική (Differential) λήψη και Online αποθήκευση απευθείας στις εναλλακτικές εγκαταστάσεις.

Στον παρακάτω πίνακα παρουσιάζεται η ακολουθούμενη πολιτική για κάθε ΠΣ.

					ΕΝΤΟΣ (ΦύλαξηΤοπικά)		ΚΤΟΣ (Φύλαξη σε Εναλλακτικές εγκαταστάσεις		
Α/Α	ΠΛΗΡΟΦΟΡΙΑΚΟ ΣΥΣΤΗΜΑ	MTD	CI	RPO	Ημερήσιο-Διαφορικό-σε Δίσκο	Εβδομαδιαίο-Πλήρες-σε Δίσκο	Ημερήσιο -Διαφορικό-online	Εβδομαδιαίο-Πλήρες-σε Κασέτα	ΠΑΡΑΤΗΡΗΣΕΙΣ
1	Intranet (LAN)	1H	15	1H					Δεν περιλαμβάνει αποθηκευμένα δεδομένα
2	printing services	1H	15	1H					Δεν περιλαμβάνει αποθηκευμένα δεδομένα
3	EHR	1H	15	1H	X	X	X	X	
4	Internet (WAN)	1H	15	1H					Δεν περιλαμβάνει αποθηκευμένα δεδομένα
5	RIS/PACS	1H	15	1H	X	X	X	X	
6	e-Health	1H	15	1H					Εκτός διαχείρισης οργανισμού.Απαίτηση με SLA.
7	LIS	1H	15	1H	X	X	X	X	
8	MED APPS	1H	15	1H	X	X	X	X	
9	security services	1H	12	1H	X	X	X	X	
10	file services	1H	10	1E	(X)	X		X	
11	mail services	1H	10	1H					Εκτός διαχείρισης οργανισμού.Απαίτηση με SLA.
12	web portal	1H	10	1E					Εκτός διαχείρισης οργανισμού.Απαίτηση με SLA.
13	ERP	3H	11	1H	X	X	X	X	
14	QMIS	3H	8	1E	(X)	X		X	
15	MIS	1E	10	1E					Δεν περιλαμβάνει αποθηκευμένα δεδομένα
16	HRIS	1E	8	1E	(X)	X		X	
17	PMIS	1E	5	1E	(X)	X		X	

5.3 Εφαρμοζόμενα μέτρα ανάκαμψης και τρόπος υλοποίησης

Τα χρησιμοποιούμενα μέτρα ανάκαμψης για τα δομικά συστατικά κάθε ΠΣ περιγράφονται στον παρακάτω πίνακα. Ο τρόπος που αυτά εφαρμόζονται σε κάθε ΠΣ (διαδικασίες, ενέργειες, απαραίτητες οδηγίες) περιγράφεται στα αντίστοιχα Πλάνα Αντιμετώπισης Καταστροφής για κάθε ΠΣ (ISCPs) τα οποία βρίσκονται συνημμένα στο παρόν ΣΑΚ.

		ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ																	
	ΣΤΡΑΤΗΓΙΚΗ	Treat & Transfer	Treat & Transfer	Treat & Transfer	Treat & Transfer	Treat & Transfer	tolerate	Treat & Transfer	Treat & Transfer	Treat & Transfer	Treat & Transfer	transfer	transfer	Treat & Transfer	Treat & Transfer	Treat & Transfer	Treat	Treat	
	ΜΕΤΡΑ	Intranet (LAN)	printing services	EHR	Internet (WAN)	RIS/PACS	e-Health	LIS	MED APPS	security services	file services	mail services	web portal	ERP	QMIS	MIS	HRIS	PMIS	ΠΑΡΑΤΗΡΗΣΕΙΣ
Άνθρωποι	**Αριθμ.επάρκεια**																		
	Αναπλήρωση (redundancy)	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	Η αναπλήρωση αυτή αφορά κυρίως το ρόλο του διαχειριστή και του κύριου χρήστη. Εφαρμόζεται για όλα τα ΠΣ εκτός από αυτά που φιλοξενούνται και διαχειρίζονται εξ' ολοκλήρου από εξωγενείς παράγοντες
	Ανάθεση (Outsouring)	X	X	X	X	X		X	X	X	X			X	X	X	X	X	Ανάθεση σε εξειδικευμένους εξωτερικούς συνεργάτες για συνεργασία με υπάρχον προσωπικό. Σύναψη συμβολαίων παροχής υπηρεσιών, ιδίως για τα κρίσιμα ΠΣ.
	Τηλεεργασία	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	Δυνατότητα τηλεεργασίας για όλα τα ΠΣ.
	Εκπαίδευση																		
	Βασική εκπαίδευση	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Βασική εκπαίδευση και ενημέρωση προσωπικού για εφαρμοζόμενες στρατηγικές.
	Εξειδικευμένη εκπαίδευση	X	X	X	X	X		X	X	X	X								Εκπαίδευση εξειδικευμένου προσωπικού του οργανισμού για κρίσιμα συστήματα.
Εγκαταστάσεις	**Ιδιοκτησιακά**																		
	Ιδιόκτητες	X	X	X	X	X		X	X	X	X			X	X	X	X	X	Χρήση ιδιόκτητων εναλλακτικών εγκαταστάσεων.
	Ανταποδοτική συμφωλία																		
	Εμπορική μίσθωση																		
	Επίπεδο εξοπλισμού																		
	cold sites																		
	warm sites	X	X	X	X	X		X	X	X	X			X	X	X	X	X	Ύπαρξη κατάλληλων υποδομών και εξοπλισμού προς χρήση.
	hot sites																		
	mobile sites																		
	mirrored sites																		
Τεχνολογίες	**Πλατφόρμες-Συστήματα**																		
	Συστήματα Υψηλής διαθεσιμότητας			X				X		X	X								Χρήση σε κρίσιμα συστήματα και όπου είναι εφικτό.
	Εικονικοποίηση		X	X		X		X	X	X	X			X	X	X	X	X	Χρήση κυρίως για επιτάχυνση της εγκατάστασης σε εναλλακτικές εγκαταστάσεις.
	Υπολογιστικό νέφος-DRaaS																		
	Τηλεπικοινωνίες																		
	Αρχιτεκτονικές εφεδρείας	X			X														Χρήση σε τοπολογία δικτύου κυρίως εγκαταστάσεων.
	Βελτιστοποίηση απόδοσης (wan optimization)				X														Χρήση σε WAN και σε διασύνδεση με εναλλακτικές εγκαταστάσεις.
	Εναλλακτικά μέσα μετάδοσης																		
	satellite																		
	mobile				X														Χρήση σε WAN και σε διασύνδεση με εναλλακτικές εγκαταστάσεις.
	Απομακρυσμένη πρόσβαση																		
	IPSec VPN	X	X	X	X	X		X	X	X	X			X	X	X	X	X	Χρήση για απομακρυσμένη υποστήριξη.
	SSL VPN																		
	Cloud VPN																		
Δεδομένα	**Μέσα**																		
	tape			X		X		X	X	X	X			X	X		X	X	Αφορά σε εβδομαδιαίο πλήρες αντίγραφο ασφαλείας που αποστέλλεται στις εναλλακτικές εγκαταστάσεις.
	hd			X		X		X	X	X	X			X	X		X	X	Αφορά σε ημερήσιο διαφορικό αντίγραφο ασφαλείας
	online			X		X		X	X	X				X					Αφορά σε ημερήσιο διαφορικού αντιγράφου που αποστέλλεται online στις εναλλακτικές εγκαταστάσεις
	Μέθοδοι																		
	full			X		X		X	X	X	X			X	X		X	X	Αφορά σε εβδομαδιαίο πλήρες αντίγραφο ασφαλείας.
	differential			X		X		X	X	X	X			X	X		X	X	Αφορά σε ημερήσιο διαφορικό αντίγραφο ασφαλείας
	incremental																		
	Τεχνικές																		
	replication sync																		
	replication async																		
	deduplication			X		X		X	X	X	X			X	X	X	X	X	
	cdp																		
	snapshot																		
Διαδικασίες	**Εφαρμογή προτύπων**	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Υιοθέτηση προτύπων (ISO27001,δυνητικά και ISO24762)
	Λήψη οργανωτικών μέτρων	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Ενημέρωση, Διαδικασίες, Δοκιμές
Προμηθευτές	**Αντικατάσταση εξοπλισμού**																		
	συμφωνα με προμηθευτες (SLAs)					X				X									Συμφωλία με προμηθευτές λόγω εξειδικευμένου εξοπλισμού.
	εφεδρικός εξοπλισμός		X	X				X	X		X			X	X	X	X	X	Χρήση εφεδρικού εξοπλισμού ο οποίος βρίσκεται στις εναλλακτικές εγκαταστάσεις.
	συμβατός εξοπλισμός	X			X														
	Προγραμματισμός δαπανών	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Το ποσό που προκύπτει από τον προγραμματισμό θα πρέπει να είναι εξασφαλισμένο και πάντα διαθέσιμο σε τραπεζικό λογαριασμό.
	Ανάθεση υπηρεσιών (outsourcing)					X													Συμφωλία με προμηθευτές λόγω εξειδικευμένου εξοπλισμού.

ΠΑΡΑΡΤΗΜΑ

Στοιχεία επικοινωνίας

Ημερομηνία Αναθεώρησης: <00/00/0000>
Στοιχεία Επικοινωνίας
Παρατηρήσεις: * Η Λίστα αυτή χρησιμοποιείται και για την αντιστοίχιση των ρόλων σε φυσικά πρόσωπα

Ρόλος	Όνομα	Τηλ.Κινητού	Τηλ.Σπιτιού	Τηλ.Εργασίας	E-mail
ΟΜΑΔΕΣ ΣΑΚ					
Ομάδα Διαχείρισης ΣΑΚ					
Υπεύθυνος Συντονισμού					
(Αναπληρωτής)					
Υπεύθυνος Επικοινωνίας					
(Αναπληρωτής)					
Υπεύθυνος Επικαιροποίησης					
(Αναπληρωτής)					
Υπεύθυνος Νομικών ενεργειών					
(Αναπληρωτής)					
Υπεύθυνος Εκπαίδευσης					
(Αναπληρωτής)					
Ομάδα Αντιμετώπισης Καταστροφής					
Υποομάδα Υποδομών					
Υποομάδα Συστημάτων και Περιφερειακών					
Υποομάδα Εξυπηρετητών και Εφαρμογών					
Υποομάδα Τηλεπικοινωνιών και δικτύων					
Υποομάδα Ανάκτησης δεδομένων					
Υποομάδα Ενημέρωσης και υποστήριξης χρηστών					
Ομάδα Προμηθειών και Μεταφοράς					
Ομάδα Φυσικής ασφάλειας					
Κυρίως Εγκαταστάσεις					
Εναλλακτικές Εγκαταστάσεις					

Εξωτερικοί συνεργάτες					
Πληροφοριακό Σύστημα 1					
Πληροφοριακό Σύστημα 2					

Πάροχοι Υπηρεσιών - Προμηθευτές - εξωτερικές επαφές					
Ηλεκτρισμός					
Τηλεπικοινωνίες					
Εξοπλισμός					
Ασφαλιστική κάλυψη					
Υπηρεσίες φύλαξης					
Τοπικές Εφημερίδες					
Τοπικοί Ρ/Φ σταθμοί					
Τοπικοί Τ/Ο σταθμοί					

Υπηρεσίες Έκτακτης Ανάγκης					
Αστυνομία					
Πυροσβεστική					
ΕΚΑΒ					
Δίωξη Ηλεκτρονικού Εγκλήματος					

Κωδικοί πρόσβασης διαχειριστών

Ημερομηνία Αναθεώρησης: <00/00/0000>
Κωδικοί πρόσβασης διαχειριστών
Παρατηρήσεις: * Η Λίστα αυτή είναι προσβάσιμη μόνο από τον Υπεύθυνο Ασφαλείας και τον αναπληρωτή του. Σε περίπτωση που δεν υπάρχει Υπεύθυνος Ασφαλείας η λίστα είναι προσβάσιμη από τον Υπεύθυνο Συντονισμού.

Πληροφοριακό Σύστημα-Πλατφόρμα	Όνομα Χρήστη	Κωδικός Χρήστη	Παρατηρήσεις

Συμβόλαια με τρίτους

Ημερομηνία Αναθεώρησης: <00/00/0000>

Συμβόλαια (παροχής υπηρεσιών/ασφάλισης/εγγυημένου επιπέδου υπηρεσιών)
Παρατηρήσεις: * Στο παρόν σχέδιο θα πρέπει να βρίσκονται συνημμένα και αντίγραφα των συμβολαίων αυτών.

Αρ.Συμβολαίου	Αντισυμβαλλόμενος	Τίτλος	Περιγραφή	Ρήτρα/Αποζημίωση	Επικοινωνία	Ημ/μηνία Λήξης	Παρατηρήσεις

Λίστα απαραίτητων πόρων για ανάκαμψη

	Ημερομηνία Αναθεώρησης: <00/00/0000>
Λίστα πόρων ανάκαμψης	
Παρατηρήσεις: * Περιγράφονται τα υλικά και οι πόροι που κρίνονται απαραίτητα για τη διαδικασία της ανάκαμψης * Οι περιγραφόμενοι πόροι βρίσκονται διαθέσιμοι προς χρήση στις εναλλακτικές εγκαταστάσεις	

Είδος	Ποσότητα	Περιγραφή-Παρατηρήσεις
Εφεδρικός εξοπλισμός		
φορητοί υπολογιστές		Χρήση από ομάδα ανάκαμψης.
εξυπηρετητες		Διασυνδεδεμένοι με προεγκατεστημένες και προρυθμισμένες εικονικές μηχανές έτοιμες για χρήση ανάκαμψης.
εκτυπωτές		
σταθμοί εργασίας		Χρήση από χρήστες-κλειδιά των ΠΣ. Με προεγκατεστημένες και προρυθμισμένες απαραίτητες εφαρμογές.
δικτυακός εξοπλισμός		
Επικουρικός εξοπλισμός		
κινητά τηλέφωνα		
θέσεις εργασίας		Περιλαμβάνει γραφεία, καρέκλες και λοιπό εξοπλισμό γραφείου.
καλώδια		
σκληροί δίσκοι		
Λοιπά εργαλεία		
Λειτουργικές δαπάνες		
Υπερωρίες (Εργατοώρες)		
Έξοδα μεταφοράς/μετακίνησης		
Αναλώσιμα		
Λοιπές δαπάνες		

Ανάλυση επιχειρησιακών επιπτώσεων (BIA)

Οργανωτικές Μονάδες	Λειτουργίες ανά Μονάδα	ΚΛΙΝΙΚΑ ΠΣ					ΔΙΟΙΚΗΤΙΚΑ ΠΣ					ΥΠΟΣΤΗΡΙΚΤΙΚΑ ΠΣ							Επιπτώσεις από δυσλειτουργία-απώλεια						Μέγιστος ανεκτός χρόνος δυσλειτουργίας(MTD				Μέγιστος ανεκτός χρόνος απώλειας δεδομένων(RPO)		
		EHR	LIS	RIS/PACS	Medical Applications	e-Health	PMIS	HRIS	QMIS	MIS	ERP	mail services	file services	printing services	web-portal	internet access (WAN)	intranet access (LAN)	Security services	Νομικές-Κανονιστικές	Οικονομικές	Λειτουργικές-Παραγωγικές	Υπόληψη-Υστεροφημία	Υγιεινή & Ασφάλεια	Δείκτης Κρισιμότητας (CI)	4Ω	1Η	3Η	1Ε	1Ω	1Η	1Ε
Κλινική Φροντίδα	Υπηρεσιες υγείας	X		X	X	X								X		X	X		Y	Y	Y	Y	Y	15		X				X	
Ιατρικές Απεικονίσεις	Υπηρεσιες υγείας			X										X			X		Y	Y	Y	Y	Y	15		X				X	
Αποκατάσταση-Αποθεραπεία	Υπηρεσιες υγείας	X			X	X								X			X		Y	Y	Y	Y	Y	15		X				X	
Βιοπαθολογικά Εργαστήρια	Διενέργεια εργαστηριακών εξετάσεων		X											X			X		Y	Y	Y	Y	Y	15		X				X	
Διοικητικές Υπηρεσίες	Διαχείριση Ανθρωπίνου Δυναμικού						X	X				X	X	X			X		M	X	Y	X	X	8				X			X
	Γραμματειακή υποστήριξη											X	X	X	X		X		X	X	M	X	X	6				X			X
	Κλείσιμο ραντεβού	X										X			X		X		M	Y	M	M	X	10		X				X	
Οικονομικές Υπηρεσίες	Σχεδιασμός-Εκτέλεση προϋπολογισμού									X	X		X	X			X		Y	Y	M	X	X	10				X			X
	Έκδοση μισθοδοσίας						X							X			X		X	X	X	X	X	5				X			X
	Υπηρεσίες Λογιστηρίου (Τιμολόγηση)										X			X			X		Y	Y	M	M	X	11			X			X	
	Προμήθεια και διαχείριση υλικού										X	X					X		M	X	X	M	M	8				X			X
Υπηρεσίες Πληροφορικής	Υποστήριξη ΠΣ												X	X		X	X		M	M	Y	X	M	10		X					X
	Ασφάλεια ΠΣ-Πληροφοριών																X	X	Y	X	X	Y	M	12		X				X	
Υπηρεσίες Βιοϊατρικής Τεχνολογίας	Υποστήριξη Βιοιατρικού εξοπλισμού								X			X	X			X	X		M	X	X	M	M	8			X				X
Τεχνικές Υπηρεσίες	Υποστήριξη Υποδομών								X			X	X			X	X		M	X	X	X	M	7				X			X
Υπηρεσίες Ολικής Ποιότητας	Έλεγχος Συστήματος Ποιότητας								X								X		M	X	X	M	M	8				X			X
Νομικές Υπηρεσίες	Νομικές Υπηρεσίες												X				X		M	X	X	X	X	6				X			X
Υπηρεσίες Εσωτερικού Ελέγχου	Εσωτερικός Έλεγχος								X				X				X	X	M	x	x	X	X	6				X			X

Στρατηγικές ανάκαμψης ανά Πληροφοριακό Σύστημα

Α/Α	ΠΛΗΡΟΦΟΡΙΑΚΟ ΣΥΣΤΗΜΑ	MTD	CI	RPO	ΣΤΡΑΤΗΓΙΚΗ ΑΝΑΚΑΜΨΗΣ				ΠΕΡΙΓΡΑΦΗ
					Treat	Transfer	Treat & Transfer	Tolerate or Terminate	
1	Intranet (LAN)	1H	15	1H			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
2	printing services	1H	15	1H			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
3	EHR	1H	15	1H			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
4	Internet (WAN)	1H	15	1H			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
5	RIS/PACS	1H	15	1H			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
6	e-Health	1H	15	1H				X	Αφορά κρατικές υπηρεσίες ηλεκτρονικής συνταγογράφησης και ηλεκτρονικής διάγνωσης/παραμπομπής τα οποία ανήκουν σε εξωτερικούς φορείς. Ως στρατηγική αντιμετώπισης προτείνεται η εφαρμογή χειροκίνητων διαδικασιών μέχρι την ανάκαμψη του ΠΣ.
7	LIS	1H	15	1H			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
8	MED APPS	1H	15	1H			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
9	security services	1H	12	1H			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
10	file services	1H	10	1E			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
11	mail services	1H	10	1H		X			Παρέχεται ως υπηρεσία από εξωτερικό οργανισμό. Μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
12	web portal	1H	10	1E		X			Παρέχεται ως υπηρεσία από εξωτερικό οργανισμό. Μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
13	ERP	3H	11	1H			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
14	QMIS	3H	8	1E			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
15	MIS	1E	10	1E			X		Λήψη απαραίτητων μέτρων και μεταφορά κόστους επιπτώσεων για χρόνο μη διαθεσιμότητας > MTD, μέσω ρητρών σε συμβόλαια υποστήριξης/παροχής υπηρεσιών.
16	HRIS	1E	8	1E	X				Λήψη απαραίτητων μέτρων
17	PMIS	1E	5	1E	X				Λήψη απαραίτητων μέτρων

Έντυπο πλάνου αντιμετώπισης καταστροφής Πληροφοριακών Συστημάτων (ISCPs)

Ημερομηνία Αναθεώρησης: <00/00/0000>

Αντιμετώπιση Καταστροφής Πληροφορικού Συστήματος (ISCP) **< ΟΝΟΜΑ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ >**

ΠΛΗΡΟΦΟΡΙΕΣ
Περιγραφή ΠΣ:
Οργανωτικές Μονάδες που επηρεάζει:
Απαιτήσεις Ανάκαμψης:
Εξάρτηση από άλλα ΠΣ:

ΔΟΜΙΚΑ ΣΤΟΙΧΕΙΑ				
Περιγραφή	**Μέτρα ανάκαμψης**	**Υπεύθυνη ομάδα**	**RTO/RPO**	**Παρατηρήσεις**
Άνθρωποι				
<Διαχειριστής>				
<Χρήστης>				
<Χρήστης>				
Εγκαταστάσεις				
<εγκατάσταση ΠΣ>				
<εγκατάσταση ΠΣ>				
<εγκατάσταση ΠΣ>				
Τεχνολογίες (Εξοπλισμός)				
<εξυπηρετητής>				
<σταθμός εργασίας>				
<αποθηκευτικό μέσο>				
<δικτυακός εξοπλισμός>				
<εκτυπωτής>				
<λειτουργικό σύστημα>				
<εφαρμογή λογισμικού>				
<εφαρμογή λογισμικού>				
<εργαλεία ανάπτυξης>				
<……>				
<……>				
Δεδομένα				

<βάση δεδομένων>				
<βάση δεδομένων>				
<βάση δεδομένων>				
Προμηθευτές				
<υλικού>				
<λογισμικού>				
<υπηρεσίας>				
Διαδικασίες (Συνημμένα στο παρόν σχέδιο)				

- ☐ **Οδηγίες εγκατάστασης**
- ☐ **Οδηγίες διαχείρισης**
- ☐ **Οδηγίες χρήσης**
- ☐ **Οδηγίες ανάκτησης δεδομένων**
- ☐ **CD εγκατάστασης**
- ☐ **Άδειες χρήσης**
- ☐ **Άλλα τεχνικά εγχειρίδια**
- ☐ **Αρχιτεκτονική διάταξη**
- ☐ **…….**
- ☐ **…….**

ΕΝΕΡΓΕΙΕΣ ΑΝΑΚΑΜΨΗΣ				
Α/Α	**Περιγραφή**	**Υπεύθυνη Ομάδα**	**RTO**	**Παρατηρήσεις**
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

ΕΛΕΓΧΟΙ ΣΩΣΤΗΣ ΛΕΙΤΟΥΡΓΙΑΣ				
Α/Α	**Περιγραφή**	**Υπεύθυνη Ομάδα**	**RTO**	**Παρατηρήσεις**
1				
2				
3				
4				
5				

Έντυπο καταγραφής περιστατικού-Αναφοράς παρατηρήσεων

Ημερομηνία Αναθεώρησης: <00/00/0000>
Έντυπο Καταγραφής Περιστατικού Ανάκαμψης

Εμφάνιση Περιστατικού	
Ημερομηνία	
Ώρα	
Τόπος	
Όνομα Παρατηρητή	
Περιγραφή	
Παρατηρήσεις	

Καταγραφή ζημιών						
Πληροφοριακό Σύστημα	**Άνθρωποι**	**Εγκαταστάσεις**	**Εξοπλισμός**	**Δεδομένα**	**Προμηθευτές**	**Διαδικασίες**
<Πληροφοριακό Σύστημα 1>						
<Πληροφοριακό Σύστημα 2>						
<Πληροφοριακό Σύστημα 3>						
Παρατηρήσεις						

Καθορισμός στόχων Ανάκαμψης				
Πλήρης Ανάκαμψη Πληροφοριακών Συστημάτων	☐ΝΑΙ	☐ΟΧΙ	☐ΜΕΡΙΚΗ	**Περιγραφή:**
Χρήση Εναλλακτικών Εγκαταστάσεων	☐ΝΑΙ	☐ΟΧΙ	Αν ΝΑΙ, δώστε το χρόνο επαναφοράς στις κύριες εγκαταστάσεις	
RTO				
RPO				
Παρατηρήσεις				

Διαδικασία Ανάκαμψης			
Αποκλίσεις-Δυσκολίες	**Ομάδα**	**Τρόπος Αντιμετώπισης**	**Παρατηρήσεις**

Σύνοψη Ανάκαμψης

Επιτυχία Ανάκαμψης			
	☐ΝΑΙ	☐ΟΧΙ	☐ΜΕΡΙΚΗ
Παρατηρήσεις:			

Αποτίμηση Επιπτώσεων Περιστατικού					
Νομικές-Κανονιστικές	**Οικονομικές**	**Λειτουργικές-Παραγωγικές**	**Υπόληψη-Υστεροφημία**	**Υγιεινή και Ασφάλεια**	**Άλλες**

Διορθωτικές Ενέργειες				
Ελλείψεις που παρατηρήθηκαν	**Αίτια**	**Διορθωτικά μέτρα**	**Υπεύθυνος Υλοποίησης**	**Χρόνος**