Πανεπιστήμιο Πειραιώς
Τμήμα Ψηφιακών Συστημάτων

ΜΠΣ: Διδακτική της τεχνολογίας και Ψηφιακών Συστημάτων

Κατεύθυνση : Δικτυοκεντρικά Συστήματα

Διπλωματική εργασία: «Risk Management Δικτυοκεντρικού Συστήματος»

ΚΥΡΙΤΣΗ ΒΑΣΙΛΙΚΗ ΜΕ11061

Επιβλέπων: Θεμιστοκλέους Μαρίνος

ΠΕΡΙΕΧΟΜΕΝΑ

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

ΚΕΦΑΛΑΙΟ 1

1.1 Περίληψη

Ένα Έργο Πληροφορικής μεγάλου μεγέθους και πολυπλοκότητας εμπεριέχει ποικίλους κινδύνους που απειλούν την επιτυχία της εφαρμογής του. Σκοπός της Διπλωματικής Εργασίας ήταν η περιγραφή των τεχνικών αναγνώρισης και αντιμετώπισης των πιθανών κινδύνων. Πιο συγκεκριμένα παρουσιάστηκαν όλα τα στάδια της διαδικασίας διαχείρισης κινδύνων 1) Εκτίμηση κινδύνων, 2) Επιλογή μεθόδων αντιμετώπισης κινδύνων και 3) Παρακολούθηση σχεδίου αντιμετώπισης κινδύνων. Κατά την εκτίμηση κινδύνων έγινε η παρουσίαση κάποιων πιθανών κινδύνων, των μεθόδων αξιολόγησης της σοβαρότητας αυτών, ως προς την πιθανότητα εμφάνισής τους και το μέγεθος των επιπτώσεών τους, στο επόμενο στάδιο προτάθηκαν μέθοδοι και πολιτικές αντιμετώπισής τους και στο τελευταίο παρουσιάστηκαν οι μέθοδοι παρακολούθησης του σχεδίου προστασίας του έργου.

Στο τέλος έγινε η εφαρμογή των διαδικασιών διαχείρισης κινδύνων στο έργο «*E-PRESCRIPTION* ». Για το έργο αυτό απαριθμήθηκαν οι πληροφορίες που πρέπει να αναζητηθούν, οι κίνδυνοι που το απειλούν, έγινε αξιολόγηση της πιθανότητας εμφάνισης και των επιπτώσεων αυτών των κινδύνων και προτάθηκαν μέθοδοι αντιμετώπισης αυτών ανάλογα με την αξία του μετριασμού τους για την πορεία υλοποίησης του έργου.

Η μεθοδολογία που περιγράφηκε μπορεί να αποτελέσει χρήσιμο εργαλείο για τη διεξαγωγή μελετών διαχείρισης κινδύνων και συμβάλει στον άρτιο σχεδιασμό και την επιτυχημένη υλοποίηση μεγάλων πληροφοριακών έργων. Η γενικότητα της μεθοδολογίας έγκειται στο γεγονός ότι περιγράφονται αναλυτικά όλα τα βήματα που ακολουθούνται για τη διαχείριση κινδύνων και οι κίνδυνοι που περιγράφονται αφορούν όλα τα είδη πληροφοριακών έργων.

1.2 Αντικείμενο της Εργασίας

Τα αντικείμενα της έρευνας είναι η θεωρητική ανάλυση της έννοιας «Διαχείριση Κινδύνων» μέσω της σχετικής βιβλιογραφίας, η διερεύνηση μίας μελέτης περίπτωσης (case study / use case) και η μελέτη και ανάλυση ενός συστήματος σχετικό με τη μελέτη περίπτωσης και τη διαχείριση κινδύνων.

Θεωρητική ανάλυση: Ανάλυση των βασικών εννοιών της έρευνας, του κύκλου ζωής της διαχείρισης κινδύνων και των μεθοδολογιών ασφάλειας των πληροφοριακών συστημάτων.

Μελέτη περίπτωσης: Ανάλυση του συστήματος E-PRESCRIPTION το οποίο στη συνέχεια θα συνδεθεί με τη διαχείριση κινδύνων.

Μελέτη συστήματος: Ανάλυση της λειτουργίας του συστήματος E-PRESCRIPTION, των προβλημάτων που παρουσιάστηκαν κατά τη διάρκειά της και της διαδικασίας διαχείρισης κινδύνων που έπρεπε να έχει λάβει χώρα ώστε να μειωθούν ή να αποφευχθούν τα προβλήματα αυτά.

1.3 Σκοπός και αντικειμενικοί στόχοι

Σκοπός της εργασίας είναι η ανάλυση της έννοιας «διαχείριση κινδύνου» και η μελέτη των παραγόντων που την πλαισιώνουν. Μέσα από αυτή την έρευνα θα γίνουν πλήρως κατανοητοί οι παράγοντες αυτοί και να είναι εφικτή η άρτια αντιμετώπιση του ρίσκου σε οποιαδήποτε δραστηριότητα ή έργο.

1.4 Δομή εργασίας

Η παρούσα εργασία αποτελείται από 7 κεφάλαια.

Στο **κεφάλαιο 1** γίνεται αναφορά στις έννοιες του κινδύνου, της διαχείρισης αυτού και του έργου και προσδιορίζονται ο σκοπός και τα αντικείμενα της έρευνας.

Στο **κεφάλαιο 2** δίνεται αναλυτικά η βιβλιογραφική επισκόπηση της έρευνας. Αρχικά, δίνονται κάποια γενικά στοιχεία για το έργο (project) και στη συνέχεια αναλύεται η έννοια της διαχείρισης κινδύνου (risk management) και ο κύκλος ζωής αυτής.

Στο **κεφάλαιο 3** αναφέρονται κάποια γενικά στοιχεία για τα πληροφοριακά έργα και τη σημαντικότητα της διαχείρισης κινδύνου σε αυτά. Επίσης αναφέρονται οι κυριότεροι μηχανισμοί ασφαλείας.

Στο **κεφάλαιο 4** αναφέρονται κάποια γενικά στοιχεία για το σύστημα υγείας στη Ελλάδα και η έννοια της κοινωνικής ασφάλισης καθώς και τη σημαντικότητα της ύπαρξης ενός ενιαίου συστήματος παροχής ηλεκτρονικών υπηρεσιών όπου θα εξυπηρετούνται οι πολίτες άμεσα και με ασφάλεια.

Στο **κεφάλαιο 5** αναφέρονται κάποια γενικά στοιχεία για την ηλεκτρονική συνταγογράφηση και στη συνέχεια για το σύστημα E-PRESCRIPTION. Περιγράφεται η λειτουργία του συστήματος E-PRESCRIPTION, ο τρόπος εγγραφής ενός χρήστη στο σύστημα και τα πλεονεκτήματα που παρέχει. Επίσης τα προβλήματα που παρατηρήθηκαν κατά την εφαρμογή του συστήματος E-PRESCRIPTION.

Στο **κεφάλαιο 6** αναλύεται η διαδικασία διαχείρισης κινδύνων του συστήματος E-PRESCRIPTION, λαμβάνοντας υπ' όψιν τα προβλήματα που προέκυψαν κατά τη διάρκεια της λειτουργίας του.

Στο **κεφάλαιο 7** αναφέρονται τα συμπεράσματα της έρευνας.

ΚΕΦΑΛΑΙΟ 2

2.1 Κίνδυνος

Ορισμός

Ο κίνδυνος γενικά μπορεί να ορισθεί ως ο συνδυασμός της πιθανότητας ενός γεγονότος και των συνεπειών του. Σε όλους τους τύπους των δραστηριοτήτων, υπάρχει το ενδεχόμενο για γεγονότα και συνέπειες που συνιστούν ευκαιρίες προς όφελος ή απειλές της επιτυχίας.

Η έννοια του κινδύνου χρησιμοποιείται παγκόσμια σε διαφορετικές εννοιολογικές περιοχές. Για παράδειγμα ενώ στον οικονομικό τομέα χρησιμοποιείται για να δηλώσει την πιθανότητα να συμβεί μια οικονομική απώλεια, στον ιατρικό τομέα χρησιμοποιείται για να δηλώσει την πιθανότητα μιας δυσλειτουργίας στην ζωή ενός ανθρώπου.

Στον τομέα της πληροφορικής η έννοια του κινδύνου είναι συνυφασμένη με σφάλματα ή προβλήματα που μπορεί να προκύψουν κατά την λειτουργία ενός πληροφοριακού συστήματος (πρόβλημα υλικού ή λογισμικού).

Στα έργα πληροφορικής δίνεται ιδιαίτερη έμφαση στους κινδύνους που προκύπτουν από τον κώδικα του λογισμικού, τις συγχωνεύσεις εταιρειών (συνένωση των πληροφοριακών συστημάτων των εταιρειών) και τις συμβάσεις για την συντήρηση των πληροφοριακών συστημάτων.

2.2 Διαχείριση Κινδύνου

Η πιο απλή ερμηνεία για το τι είναι η διαχείριση κινδύνων είναι αυτό που υποδηλώνει και ο τίτλος της, δηλαδή είναι ένας τρόπος για το πώς να διαχειριζόμαστε και να αντιμετωπίζουμε κινδύνους. Πιο αναλυτικά μπορούμε να πούμε ότι συμπεριλαμβάνει όλες τις ενέργειες που εκτελούνται για να ελαχιστοποιηθούν οι αβεβαιότητες που συνδέονται με συγκεκριμένες δραστηριότητες ή γεγονότα. Στα πλαίσια των έργων η διαχείριση κινδύνων μειώνει τις επιπτώσεις των ανεπιθύμητων γεγονότων σε ένα έργο.

Η διαχείριση κινδύνων σε οποιοδήποτε έργο απαιτεί την λήψη αποφάσεων σε συγκεκριμένες δραστηριότητες που εκτελούνται.

2.3 Κύκλος Ζωής Διαχείριση Κινδύνου (Risk Management)

Ένα έργο διαχείρισης κινδύνου περιλαμβάνει τις διαδικασίες του σχεδιασμού, του καθορισμού, της ανάλυσης, του σχεδιασμού αντιμετώπισης και της παρακολούθησης και ελέγχου του έργου.

Οι αντικειμενικοί στόχοι ενός έργου της διαχείρισης κινδύνου είναι να αυξήσει την πιθανότητα και την επίδραση των θετικών γεγονότων και να μειώσει την πιθανότητα και την επίδραση των αρνητικών γεγονότων σε ένα έργο.

Ο κίνδυνος είναι ένα γεγονός ή μια κατάσταση που με την εμφάνιση του σε ένα έργο μπορεί να έχει επίδραση σε τουλάχιστον έναν αντικειμενικό στόχο του έργου. Οι στόχοι ενός έργου μπορεί να περιλαμβάνουν παραμέτρους του όπως είναι το εύρος, ο σχεδιασμός, το κόστος και η ποιότητα του. Ένας κίνδυνος μπορεί να έχει ένα ή περισσότερα αίτια και αν προκύψει μπορεί να έχει μία ή περισσότερες επιδράσεις. Μια αιτία μπορεί να είναι μια απαίτηση, μια υπόθεση, ένας περιορισμός, ή μια περίπτωση που δημιουργεί την πιθανότητα αρνητικών ή θετικών αποτελεσμάτων. Ο κίνδυνος ενός έργου έχει τις ρίζες του στην αβεβαιότητα που είναι υπαρκτή σε όλα τα έργα.

Γνωστοί κίνδυνοι είναι αυτοί που έχουν προσδιοριστεί και αναλυθεί καθιστώντας δυνατό τον σχεδιασμό αντιμετώπισης τους. Ορισμένοι άγνωστοι κίνδυνοι δεν μπορούν να είναι διαχειρίσιμοι προληπτικά με αποτέλεσμα η ομάδα έργου θα πρέπει να δημιουργήσει ένα σχεδιασμό ενδεχομένων.

Οι οργανισμοί και οι επιχειρήσεις αντιλαμβάνονται τον κίνδυνο σαν αποτέλεσμα της αβεβαιότητας στους στόχους τους. Οι οργανισμοί και οι εμπλεκόμενοι σε ένα έργο είναι πρόθυμοι να αποδεχτούν ποικίλες βαθμίδες κινδύνων. Αυτό ονομάζεται ανοχή κινδύνου. Οι κίνδυνοι που αποτελούν απειλή για ένα έργο μπορεί να γίνουν αποδεκτοί εάν βρίσκονται μέσα στα όρια της ανοχής κινδύνου και σε ισορροπία με τις ανταμοιβές που μπορεί να αποκομιστούν λαμβάνοντας αποφάσεις που εμπεριέχουν τους κινδύνους αυτούς.

Τα άτομα και οι ομάδες υιοθετούν συμπεριφορές προς τον κίνδυνο οι οποίες επηρεάζουν τον τρόπο που αντιδρούν. Αυτές οι συμπεριφορές καθοδηγούνται από την αντίληψη της κάθε ομάδας, τις ανοχές και άλλους παράγοντες που θα πρέπει να γίνονται σαφείς όποτε είναι δυνατό.

Σε κάθε έργο θα πρέπει να αναπτύσσεται μια συνεκτική προσέγγιση σε σχέση με τον κίνδυνο ενώ θα πρέπει να υπάρχει συνεχής επικοινωνία για τον κάθε πιθανό κίνδυνο και τον χειρισμό του.

Η απόκριση κάθε οργανισμού ως προς τους κινδύνους αντανακλά τον τρόπο που αντιλαμβάνονται την αποφυγή ή την επιλογή του κινδύνου.

Για να είναι επιτυχής στην ολοκλήρωση κάθε έργου ένας οργανισμός, θα πρέπει να δεσμεύεται πως θα ασχολείται με τη διαχείριση κινδύνου προληπτικά και με συνέπεια σε όλη τη διάρκεια ζωής του έργου. Θα πρέπει να γίνεται μια συνειδητή επιλογή προσδιορισμού των κινδύνων και να επιδιώκεται μια αποτελεσματική διαχείριση κινδύνου ενός έργου σε όλα τα επίπεδα ενός οργανισμού ή μιας επιχείρησης. Ο κίνδυνος υπάρχει σε ένα έργο πριν ακόμα αρχίσει να υλοποιείται.

Προχωρώντας με την έναρξη ενός έργου χωρίς να έχει γίνει προηγουμένως προληπτικά μια προσεκτική διαχείριση κινδύνου, αυξάνει την επίδραση ενός κινδύνου που ενδεχομένως να παρουσιαστεί και είναι περισσότερο πιθανό να οδηγήσει στην αποτυχία του έργου.

Ένα έργο διαχείρισης κινδύνου αποτελείται από τις εξής διαδικασίες:

- **Σχεδιασμός Διαχείρισης Κινδύνου**

Είναι η διαδικασία ορισμού των ενεργειών διεξαγωγής της διαχείρισης κινδύνου σε ένα έργο.

- **Αναγνώριση Κινδύνων**

Είναι η διαδικασία καθορισμού των πιθανών κινδύνων που μπορεί να επηρεάσουν το έργο και η καταγραφή των χαρακτηριστικών τους.

- **Ποιοτική Ανάλυση Κινδύνων**

Είναι η διαδικασία ιεράρχησης των κινδύνων για περαιτέρω ανάλυση. Σε αυτή την ανάλυση γίνεται και η αξιολόγησή τους μέσω του συνδυασμού της πιθανότητας να συμβούν και της επίδρασής τους.

- **Ποσοτική Ανάλυση Κινδύνων**

Είναι η διαδικασία αριθμητικής ανάλυσης της επίδρασης των κινδύνων που έχουν καθοριστεί σε όλο το εύρος του έργου.

- **Σχεδιασμός Απόκρισης Κινδύνων**

Είναι η διαδικασία ανάπτυξης επιλογών και ενεργειών για να ενισχύσουν τις ευκαιρίες και να μειώσουν τις απειλές που θα υπάρξουν κατά τη διάρκεια του έργου.

- **Παρακολούθηση και Έλεγχος Κινδύνων**

Είναι η διαδικασία εφαρμογής του σχεδίου αντιμετώπισης κινδύνων, παρακολούθησης των προσδιορισμένων κινδύνων, καθορισμός νέων κινδύνων και αξιολόγηση της αποτελεσματικότητας της διαδικασίας διαχείρισης κινδύνου σε όλο το έργο.

2.3.1 Σχεδιασμός Διαχείρισης Κινδύνου

Ο σχεδιασμός της διαχείρισης κινδύνου είναι η διαδικασία καθορισμού των ενεργειών της διαχείριση κινδύνου που θα διεξαχθούν για το έργο. Ο προσεκτικός και σαφής σχεδιασμός ενισχύει την πιθανότητα της επιτυχίας για τις επόμενες 5 διαδικασίες διαχείρισης κινδύνου όπως παρουσιάζονται στη συνέχεια.

Ο σχεδιασμός της διαχείρισης κινδύνου είναι σημαντικό να εξασφαλίσει ότι ο βαθμός και ο τύπος της διαχείρισης κινδύνου είναι ανάλογα με τους κινδύνους και τη σπουδαιότητα του έργου στον οργανισμό. Ο σχεδιασμός είναι επίσης σημαντικό να παρέχει επαρκείς πόρους και χρόνο για τις δραστηριότητες της διαχείρισης του κινδύνου. Επίσης κατά το σχεδιασμό θα πρέπει να δημιουργηθεί μια συμφωνημένη βάση για την αξιολόγηση των κινδύνων. Η διαδικασία του σχεδιασμού της

διαχείρισης κινδύνου πρέπει να ξεκινά πριν την έναρξη του έργου και να ολοκληρώνεται κατά τη διάρκεια του σχεδιασμού του έργου. Οι βασικές πληροφορίες που είναι απαραίτητες και πρέπει να προσδιοριστούν για το σωστό σχεδιασμό αναλύονται στη συνέχεια.

- **Καθορισμός πλαισίου του έργου**

Δίνει μια γενική άποψη για το έργο και για την επίδραση της διαχείρισης κινδύνου σε αυτό.

- **Σχεδιασμός Διαχείρισης Κόστους**

Αποτελεί σημαντική πληροφορία η γνώση του προϋπολογισμού διαχείρισης κινδύνου.

- **Σχεδιασμός Διαχείρισης Προγραμματισμού**

Είναι απαραίτητη η γνώση του προγράμματος εργασιών για τον χρονικό προσδιορισμός της διαχείρισης κινδύνου.

- **Σχεδιασμός Διαχείρισης Επικοινωνίας**

Είναι σημαντικό να υπάρχει επικοινωνία μεταξύ των ομάδων του έργου για τη σωστή διαχείριση κινδύνου.

- **Περιβαλλοντικοί Παράγοντες Επιχείρησης**

Επηρεάζουν την συμπεριφορά μιας επιχείρησης στην αντιμετώπιση των κινδύνων.

- **Περιουσιακά στοιχεία επιχείρησης**

Τα περιουσιακά στοιχεία της επιχείρησης που μπορεί να επηρεάσουν τη διαδικασία σχεδιασμού διαχείρισης κινδύνων περιλαμβάνουν:

- Κατηγορίες κινδύνων
- Ορισμούς κανόνων
- Πρότυπα έκθεσης κινδύνων
- Ρόλοι και υπευθυνότητες
- Επιχειρησιακά επίπεδα αποφάσεων
- Μητρώα εμπλεκομένων

2.3.2 Αναγνώριση Κινδύνων

Η αναγνώριση κινδύνων είναι η διαδικασία προσδιορισμού των κινδύνων που μπορούν να επηρεάσουν ένα έργο και η καταγραφή των χαρακτηριστικών τους. Οι εμπλεκόμενοι στις ενέργειες προσδιορισμού των κινδύνων είναι οι ακόλουθοι:

Ο διευθυντής του έργου, τα μέλη της ομάδας έργου, η ομάδα διαχείρισης κινδύνου(αν υπάρχει), οι πελάτες, οι τελικοί χρήστες, οι εμπλεκόμενοι και οι ειδικοί διαχείρισης κινδύνου.

Η αναγνώριση κινδύνων είναι μια επαναληπτική διαδικασία καθώς νέοι κίνδυνοι μπορεί να εξελιχθούν ή να εμφανιστούν κατά τη διάρκεια του κύκλου ζωής του έργου. Η συχνότητα επανάληψης της διαδικασίας και οι συμμετέχοντες κάθε φορά μπορεί να είναι διαφορετικοί.

Η μορφή της διαχείρισης των κινδύνων πρέπει να μοιάζει σε όλες τις περιπτώσεις για να είναι δυνατή η σύγκριση των επιδράσεων των κινδύνων στο έργο.

Για τον προσδιορισμό των κινδύνων θα πρέπει ιδανικά να γνωρίζουμε τα εξής:

- **Σχεδιασμός διαχείρισης κινδύνου**

Είναι η διαδικασία ορισμού των ενεργειών διεξαγωγής της διαχείρισης κινδύνου σε ένα έργο.

- **Εκτίμηση κόστους δραστηριοτήτων**

Το κόστος κάθε δραστηριότητας καθορίζει το κατά πόσο θα ληφθεί ή όχι σοβαρά υπόψη η δραστηριότητα στην διαχείριση κινδύνου.

- **Εκτίμηση της διάρκειας της κάθε δραστηριότητας**

Σημαντικό ρόλο στη διαχείριση κινδύνου παίζουν τα επιτρεπτά χρονικά περιθώρια της κάθε δραστηριότητας ή ολόκληρου του έργου .

- **Εύρος και πλαίσιο έργου**

Θα πρέπει να ληφθούν υπόψη οι διάφορες υποθέσεις όσον αφορά το πλαίσιο του έργου, και η πιθανότητα να συμβεί κάποια από αυτές.

- **Εμπλεκόμενοι στο έργο**

Οι πληροφορίες όσον αφορά τους εμπλεκόμενους στο έργο είναι πολύ χρήσιμες καθώς αυτοί μπορεί να καθορίσουν τους κινδύνους του έργου.

- **Σχεδιασμός Διαχείρισης Κόστους**

Αποτελεί σημαντική πληροφορία η γνώση του προϋπολογισμού διαχείρισης κινδύνου.

- **Σχεδιασμός Διαχείρισης Προγραμματισμού**

Η αναγνώριση των κινδύνων απαιτεί και την καλή γνώση του προγράμματος εργασιών.

- **Σχεδιασμός Ποιότητας**

Η αναγνώριση των κινδύνων απαιτεί τη γνώση των απαιτούμενων ποιοτικών χαρακτηριστικών των εργασιών.

- **Έγγραφα έργου**

Είναι σημαντικό να γνωρίζουμε τα έγγραφα του έργου που περιγράφουν διεργασίες ή περιλαμβάνουν πληροφορίες που μπορεί να φανούν χρήσιμες στη διαχείριση κινδύνου.

- **Περιβαλλοντικοί παράγοντες**

Όπως και στο σχεδιασμό του κινδύνου, έτσι και στον καθορισμό τους, είναι καλό να υπάρχει γνώση των περιβαλλοντικών παραγόντων.

- **Περιουσιακά στοιχεία επιχείρησης**

Τα περιουσιακά στοιχεία της επιχείρησης που μπορεί να επηρεάσουν τη διαδικασία σχεδιασμού διαχείρισης κινδύνων περιλαμβάνουν:

- Αρχεία έργου
- Διαδικασίες ελέγχου έργου
- Πρότυπα έκθεσης κινδύνων

Αναγνώριση κινδύνων: Εργαλεία και Τεχνικές

- **Έγγραφα Ολοκληρωμένων Έργων**

Μια ολοκληρωμένη ανασκόπηση των εγγράφων ενός έργου, που περιλαμβάνει τα σχέδια, τις υποθέσεις, συμβόλαια και προηγούμενα αρχεία έργων, καθώς επίσης και οποιαδήποτε άλλη πληροφορία.

- **Τεχνικές Συλλογής Πληροφοριών**

Μερικά παραδείγματα συλλογής πληροφοριών που χρησιμοποιούνται για τον προσδιορισμό κινδύνων:

- **Brainstorming**

Ο σκοπός του brainstorming είναι να δημιουργηθεί μια περιεκτική λίστα κινδύνων του έργου. Η ομάδα έργου χρησιμοποιεί το brainstorming συνήθως σε μια ομάδα ειδικών που δεν αποτελούν μέρος της ομάδας ανάλυσης κινδύνου. Η διαδικασία του brainstorming συντονίζεται από ένα άτομο, και χρησιμοποιεί είτε αδόμητη συζήτηση, είτε μια περισσότερο δομημένη διαδικασία. Είναι δυνατό να χρησιμοποιηθούν κατηγορίες κινδύνων, όπως μια αναλυτική δομή (πίνακας) κινδύνων ως βάση για τη διαδικασία. Οι κίνδυνοι που παράγονται από τη συζήτηση αυτή κατηγοριοποιούνται με βάση τους τύπους κινδύνου και γίνονται πιο σαφείς.

- **Τεχνική Delphi**

Η τεχνική Delphi είναι ένας τρόπος να αποκτήσεις την κοινή συναίνεση των ειδικών. Οι ειδικοί κινδύνου του έργου συμμετέχουν σε αυτή τη διαδικασία ανώνυμα. Ο συντονιστής χρησιμοποιεί ένα ερωτηματολόγιο για να συλλέξει ιδέες για σημαντικούς κινδύνους του έργου. Οι απαντήσεις συλλέγονται και στη συνέχεια δίνονται πάλι στους ειδικούς για περαιτέρω σχολιασμό. Η απαραίτητη συναίνεση όσον αφορά τους κινδύνους, δίνεται μετά από μερικές επαναλήψεις της διαδικασίας. Η τεχνική Delphi βοηθάει στην αποφυγή πόλωσης όσον αφορά τα δεδομένα και αποτρέπει αδικαιολόγητη επιρροή ενός ατόμου στο τελικό αποτέλεσμα.

- **Συνεντεύξεις**

Οι συνεντεύξεις έμπειρων στελεχών του έργου, των εμπλεκομένων και διάφορων ειδικών του έργου μπορεί να οδηγήσει στον προσδιορισμό κινδύνων.

- **Ανάλυση αιτίου – αποτελέσματος**

Η ανάλυση αυτή αποτελεί μια συγκεκριμένη τεχνική για τον προσδιορισμό ενός προβλήματος, τα υποκείμενα αίτια που οδηγούν σε αυτό, ενώ επίσης οδηγεί και στην ανάπτυξη προληπτικών ενεργειών.

- **Ανάλυση Λίστας Ελέγχου**

Οι λίστες προσδιορισμού κινδύνων αναπτύσσονται βασισμένες σε ιστορικά δεδομένα και συσσωρευμένες γνώσεις από προηγούμενα έργα, καθώς και από άλλες πηγές πληροφοριών. Τα κατώτερα στρώματα της δομής πόρων του έργου μπορεί επίσης να χρησιμοποιηθούν ως λίστα ελέγχου κινδύνων. Ενώ μια τέτοια λίστα μπορεί να είναι γρήγορη και απλή, είναι αδύνατο να είναι πολύ αναλυτική. Η ομάδα κινδύνου θα πρέπει να είναι σίγουρη πως υπάρχουν κίνδυνοι που δεν εμφανίζονται στη λίστα. Η λίστα μπορεί μετά το τέλος του έργου να χρησιμοποιηθεί ξανά και να ενσωματωθεί σε μελλοντικά έργα.

- **Ανάλυση Υποθέσεων**

Κάθε έργο και κάθε προσδιορισμένος κίνδυνος έργου είναι βασισμένος σε υποθέσεις. Η ανάλυση υποθέσεων ερευνά την εγκυρότητα των υποθέσεων σε περίπτωση που εμφανιστούν στο έργο. Επίσης προσδιορίζει τους κινδύνους του έργου λόγω ανακριβειών, ασταθών παραγόντων, ασυνεπειών ή και ανολοκλήρωτων υποθέσεων.

- **Τεχνικές Διαγραμμάτων**

Οι τεχνικές διαγραμμάτων περιλαμβάνουν:

- Διαγράμματα αιτίων και αποτελεσμάτων. Αυτά είναι επίσης γνωστά ως διαγράμματα Ishikawa και είναι χρήσιμα για τον προσδιορισμό αιτίων κινδύνων.
- Διαγράμματα ροής διαδικασιών. Αυτά δείχνουν τον τρόπο με τον οποίο τα διάφορα στοιχεία του συστήματος συσχετίζονται.
- Διαγράμματα επιρροής. Είναι γραφικές αναπαραστάσεις καταστάσεων που δείχνουν επιρροές και άλλες σχέσεις μεταξύ μεταβλητών και αποτελεσμάτων.

- **Ανάλυση SWOT**

Η τεχνική αυτή εξετάζει το έργο από όλες τις πλευρές SWOT (strengths – δυνάμεις, weaknesses – αδυναμίες, opportunities – ευκαιρίες, και threats – απειλές), και τον τρόπο με τον οποίο οι εσωτερικές αυτές παράμετροι είναι δυνατό να αυξήσουν τα αρνητικά αποτελέσματα των κινδύνων. Η τεχνική αρχίζει με τον προσδιορισμό των δυνάμεων και των αδυναμιών της επιχείρησης, εστιάζοντας

είτε στην οργάνωση του έργου, είτε στην ευρύτερη επιχείρηση. Ο προσδιορισμός των παραγόντων αυτών γίνεται συνήθως με τη χρήση της τεχνικής brainstorming. Στη συνέχεια η ανάλυση SWOT προσδιορίζει οποιεσδήποτε ευκαιρίες που είναι δυνατό να προκύψουν εκμεταλλευόμενοι τις δυνάμεις της επιχείρησης, και τις απειλές που μπορεί να εμφανιστούν λόγω των αδυναμιών της. Η ανάλυση SWOT επίσης εξετάζει το βαθμό στον οποίο οι δυνάμεις της επιχείρησης αντισταθμίζουν τις απειλές και οι ευκαιρίες που παρουσιάζονται μπορεί να χρησιμοποιηθούν για να ξεπεραστούν οι αδυναμίες.

- **Κρίση Εμπειρογνωμόνων**

Οι κίνδυνοι μπορεί να προσδιοριστούν απευθείας από ειδικούς με σχετική εμπειρία σε παρόμοια έργα ή σε αντίστοιχους επιχειρηματικούς τομείς. Τέτοιοι ειδικοί θα πρέπει να βρίσκονται από τον project manager του έργου και να καλούνται ώστε να εξετάσουν όλες τις πτυχές του έργου ώστε να προτείνουν πιθανούς κινδύνους βασισμένοι σε προηγούμενη εμπειρία. Η γνώμη των ειδικών θα πρέπει να λαμβάνεται υπόψη σε αυτή τη διαδικασία.

Αναγνώριση κινδύνων: Συμπεράσματα

- **Μητρώο Κινδύνων**

Τα βασικά συμπεράσματα της διαδικασίας Αναγνώρισης Κινδύνων αποτελούν τις αρχικές εισόδους στο μητρώο κινδύνων. Το μητρώο αυτό περιέχει τελικά τα αποτελέσματα άλλων διαδικασιών διαχείρισης κινδύνου, που έχουν ως αποτέλεσμα αύξηση του επιπέδου και του περιεχομένου της πληροφορίας που αφορά τους κινδύνους κατά τη διάρκεια του χρόνου. Η προετοιμασία του μητρώου κινδύνων αρχίζει με τη διαδικασία Αναγνώρισης Κινδύνων (με τις πληροφορίες που παρουσιάζονται στη συνέχεια) και στη συνέχεια γίνεται διαθέσιμο και στις υπόλοιπες διαδικασίες project και risk management.

- **Λίστα προσδιορισμένων κινδύνων**

Οι προσδιορισμένοι κίνδυνοι περιγράφονται με τις απαραίτητες λεπτομέρειες ώστε να γίνονται κατανοητοί. Η δομή των κινδύνων της λίστας θα πρέπει να είναι απλή και να αναφέρει το γεγονός που μπορεί να εμφανιστεί, προκαλώντας κάποια επίπτωση, ή κάποιο αίτιο που μαζί με ένα γεγονός θα επιφέρει κάποια αποτελέσματα. Επιπλέον, οι αιτίες των κινδύνων μπορεί να γίνουν περισσότερο προφανείς μέσα από αυτή τη διαδικασία. Οι αιτίες αυτές αποτελούν θεμελιώδεις προϋποθέσεις για την αύξηση των προσδιορισμένων κινδύνων και θα πρέπει να καταγράφονται για να χρησιμοποιηθούν σε μελλοντικό προσδιορισμό των κινδύνων του υπάρχοντος ή κάποιου μελλοντικού έργου.

- **Λίστα πιθανών αποκρίσεων**

Οι πιθανές αποκρίσεις σε έναν κίνδυνο μπορεί ορισμένες φορές να προσδιοριστούν κατά τη διάρκεια της διαδικασίας Σχεδιασμού Αποκρίσεων Κινδύνων

2.3.3 Ποιοτική Ανάλυση Κινδύνων

Είναι η διαδικασία ιεράρχησης των κινδύνων για περαιτέρω ανάλυση. Σε αυτή την ανάλυση γίνεται και η αξιολόγησή τους μέσω του συνδυασμού της πιθανότητας να συμβούν και της επίδρασής τους. Οι οργανισμοί μπορούν να βελτιώσουν την επίδοση σε ένα έργο εστιάζοντας σε κινδύνους υψηλή προτεραιότητας. Η διαδικασία Ποιοτικής Ανάλυσης Κινδύνου αξιολογεί την προτεραιότητα των προσδιορισμένων κινδύνων χρησιμοποιώντας τη σχετική πιθανότητα εμφάνισης, τις αντίστοιχες επιδράσεις στο έργο με την εμφάνιση κάποιου κινδύνου καθώς επίσης και άλλους παράγοντες όπως ο χρόνος απόκρισης κα η ανοχή της εταιρίας στον κίνδυνο που σχετίζεται με μεγέθη όπως είναι το κόστος, ο προγραμματισμός, το εύρος του έργου και η ποιότητα. Η αποτελεσματική αξιολόγηση των κινδύνων θα πρέπει να λαμβάνει σοβαρά υπόψη τις διάφορες συμπεριφορές απέναντι στον κίνδυνο των βασικών συμμετεχόντων στη διαδικασία ποιοτικής ανάλυσης κινδύνου. Όπου εμφανίζονται τέτοιες συμπεριφορές και δημιουργούν προβλήματα στην αξιολόγηση των κινδύνων θα πρέπει να λαμβάνονται και οι αντίστοιχες διορθωτικές αποφάσεις.

Ορίζοντας τα διάφορα επίπεδα πιθανότητας και επίδρασης των κινδύνων είναι δυνατόν να μειώσουμε την αρνητική επιρροή των υποκειμενικών απόψεων. Επίσης η αξιολόγηση της ποιότητας της διαθέσιμης πληροφορίας που αφορά τους κινδύνους του έργου βοηθάει στο να αντιληφθούμε τη σπουδαιότητα του κάθε κινδύνου στο έργο.

Η Ποιοτική Ανάλυση Κινδύνου είναι συνήθως μια αποδοτική διαδικασία που συμβάλει στην ιεράρχηση του Σχεδιασμού Απόκρισης Κινδύνων καθώς και στην Ποσοτική Ανάλυση Κινδύνου. Η Ποιοτική Ανάλυση Κινδύνου πρέπει να επανεξετάζεται κατά τη διάρκεια του κύκλου ζωής του έργου και να ενημερώνεται με οποιαδήποτε αλλαγή κινδύνου του έργου.

- **Μητρώο Κινδύνων**

  Το μητρώο κινδύνων έχει αναλυθεί προηγουμένως.

- **Σχεδιασμός Διαχείρισης Κινδύνων**

Βασικά στοιχεία του σχεδιασμού διαχείρισης κινδύνων που χρησιμοποιούνται στην Ποιοτική Ανάλυση Κινδύνων περιλαμβάνουν τους ρόλους και τις ευθύνες των στελεχών που διεξάγουν την ανάλυση κινδύνου, τον προϋπολογισμό, τον προγραμματισμό των ενεργειών της ανάλυσης κινδύνου, τις κατηγορίες κινδύνων, τον πίνακα πιθανοτήτων και επιπτώσεων καθώς και τις ανοχές των

συμμετεχόντων ως προς τον κίνδυνο. Αυτές οι πληροφορίες συχνά προσαρμόζονται στο έργο κατά τη διάρκεια του Σχεδιασμού Ανάλυσης Κινδύνων. Αν δεν είναι διαθέσιμοι τότε, αναπτύσσονται κατά τη διαδικασία Ποιοτικής Ανάλυσης.

- **Πεδίο Εφαρμογής Έργου**

Έργα κοινά ή επαναλαμβανόμενα τείνουν να έχουν καλά καθορισμένους κινδύνους. Έργα που είναι πολύ περίπλοκα ή υψηλής τεχνολογίας τείνουν να έχουν μεγαλύτερη αβεβαιότητα. Αυτές οι παράμετροι εξετάζονται κατά την αρχική δήλωση του πεδίου εφαρμογής του έργου.

- **Εταιρικά Περιουσιακά Στοιχεία**

Τα εταιρικά περιουσιακά στοιχεία που μπορεί να επηρεάσουν τη διαδικασία Ποιοτικής Ανάλυσης περιλαμβάνουν (αλλά δεν περιορίζονται σε):

- Πληροφορίες προηγούμενων ίδιων ολοκληρωμένων έργων
- Εξέταση παρόμοιων έργων από ειδικούς διαχείρισης κινδύνου
- Βάσεις δεδομένων που μπορεί να είναι διαθέσιμες από τη βιομηχανία ή και ιδιοκτήτες

Ποιοτική Ανάλυση Κινδύνων: Εργαλεία και Τεχνικές

- **Πιθανότητα Κινδύνου και Εκτίμηση Επιπτώσεων**

Η εκτίμηση πιθανότητας κινδύνων ερευνά την πιθανότητα κάθε κίνδυνος να παρουσιαστεί. Η εκτίμηση επιπτώσεων των κινδύνων μελετά το πιθανό αποτέλεσμα που θα έχει σε ένα αντικειμενικό στόχο του έργου, όπως είναι το πρόγραμμα, το κόστος, η ποιότητα ή η επίδοση, περιλαμβάνοντας είτε αρνητικά αποτελέσματα λόγω απειλών, είτε θετικά αποτελέσματα λόγω ευκαιριών.

Η πιθανότητα και η επίπτωση εκτιμώνται για κάθε προσδιορισμένο κίνδυνο. Οι κίνδυνοι μπορεί να εκτιμηθούν μέσω συνεντεύξεων ή συναντήσεων με επιλεγμένους συμμετέχοντες όσους είναι οικείοι με τους ως προς συζήτηση κινδύνους. Επίσης περιλαμβάνονται μέλη της ομάδας έργου καθώς και πρόσωπα εκτός έργου που έχουν τις απαραίτητες γνώσεις.

Ο βαθμός της πιθανότητας κάθε κινδύνου και το αποτέλεσμα σε κάθε αντικειμενικό σκοπό του έργου αξιολογείται κατά τη διάρκεια των συνεντεύξεων ή των συναντήσεων. Επίσης περιλαμβάνονται και επεξηγηματικές λεπτομέρειες που δικαιολογούν την εκτίμηση και το αποτέλεσμα του κάθε κινδύνου. Αυτοί κατατάσσονται σε σχέση με τους ορισμούς που έχουν δοθεί στην αρχική φάση του σχεδιασμού διαχείρισης κινδύνου. Κίνδυνοι χαμηλής πιθανότητας και αποτελέσματος επίσης περιλαμβάνονται σε μια λίστα για μελλοντική παρακολούθηση.

- **Πίνακας Πιθανοτήτων και Επιπτώσεων**

Οι κίνδυνοι μπαίνουν σε προτεραιότητα για μελλοντική ποσοτική ανάλυση και απόκριση βασιζόμενοι στη βαθμολόγησή τους. Συνήθως οι κανόνες βαθμολόγησης μπαίνουν στην αρχή του έργου και αποτελούν περιουσιακό στοιχείο της εταιρίας. Οι κανόνες μπορεί να προσαρμοστούν στο συγκεκριμένο έργο στη διαδικασία Σχεδιασμού Διαχείρισης Κινδύνων. Εκτίμηση της σημαντικότητας του κάθε κινδύνου άρα και προτεραιότητά του γίνεται με τη χρήση ενός πίνακα, του πίνακα πιθανοτήτων και επιπτώσεων. Αυτός ο πίνακας καθορίζει συνδυασμούς πιθανότητας και αποτελέσματος που οδηγεί στην κατάταξη των κινδύνων ως χαμηλής, μεσαίας ή υψηλής προτεραιότητας.

Η κατάταξη των κινδύνων βοηθά στις αποφασισμένες αποκρίσεις. Για παράδειγμα οι κίνδυνοι που έχουν αρνητικό αποτέλεσμα στους στόχους του έργου (απειλές) και είναι στη ζώνη υψηλού κινδύνου στον πίνακα χρειάζονται διαχείριση με υψηλή προτεραιότητα και επιθετικές στρατηγικές απόκρισης. Οι απειλές χαμηλού κινδύνου δεν χρειάζονται κάποια ιδιαίτερη ενέργεια, μόνο τοποθετούνται σε μια λίστα παρακολούθησης.

Ομοίως οι ευκαιρίες που μπορεί να δώσουν μεγαλύτερο όφελος θα πρέπει να στοχοποιούνται πρώτα. Οι ευκαιρίες που δίνουν μικρότερο όφελος θα πρέπει να βρίσκονται υπό παρακολούθηση.

- **Εκτίμηση Ποιότητας Δεδομένων Κινδύνου**

Η ποιοτική ανάλυση κινδύνου απαιτεί ακριβή στοιχεία για να είναι αξιόπιστη. Η ανάλυση της ποιότητας των δεδομένων κινδύνου είναι μια τεχνική αξιολόγησης του βαθμού χρησιμότητάς τους στην ανάλυση κινδύνου. Περιλαμβάνει την ακρίβεια, την ποιότητα, την αξιοπιστία των δεδομένων κινδύνου. Αν η ποιότητα δεν είναι αποδεκτή, ίσως να είναι απαραίτητη η συλλογή στοιχείων καλύτερης ποιότητας.

- **Κατηγοριοποίηση Κινδύνων**

Οι κίνδυνοι ενός έργου μπορεί να κατηγοριοποιηθούν ως προς την πηγή τους, την περιοχή του έργου που θα επηρεαστεί και κάθε άλλη κατηγορία που μπορεί να δημιουργηθεί. Η ομαδοποίηση των κινδύνων ως προς κοινή αιτία οδηγεί σε πιο αποτελεσματική αντιμετώπισή τους.

- **Εκτίμηση Επειγόντων Κινδύνων**

Επείγοντες θεωρούνται οι κίνδυνοι που χρειάζονται βραχυπρόθεσμη αντιμετώπιση. Η προτεραιότητα του κάθε κινδύνου μπορεί να περιλαμβάνει και το χρόνο αντίδρασης, προειδοποιητικά σημεία καθώς και τη βαθμολόγησή τους. Σε ορισμένες ποιοτικές αναλύσεις η εκτίμηση της άμεσης αντιμετώπισης ενός κινδύνου μπορεί να συνδυαστεί με την κατάταξη του κάθε

κινδύνου που απορρέει από τον πίνακα πιθανοτήτων και αποτελέσματος, έτσι ώστε να πάρουμε την τελική σημασία του κάθε κινδύνου.

- **Κρίση Εμπειρογνωμόνων**

Η γνώμη των εμπειρογνωμόνων είναι απαραίτητη για να εκτιμηθεί η πιθανότητα και το αποτέλεσμα κάθε κινδύνου και να προσδιοριστεί η θέση του στον πίνακα πιθανοτήτων και αποτελέσματος. Οι εμπειρογνώμονες έχουν πρόσφατη εμπειρία από παρόμοια έργα. Επίσης όσοι ασχολούνται με το συγκεκριμένο έργο έχουν σημαντική γνώση για αυτό. Η εμπειρία τους λαμβάνεται υπόψη μέσω συνεντεύξεων και συναντήσεων κατά τη διαδικασία αυτή.

Ποιοτική Ανάλυση Κινδύνων: Συμπεράσματα

- **Ενημέρωση Μητρώου Κινδύνων**

Το μητρώο κινδύνων δημιουργείται κατά τη διαδικασία Προσδιορισμού Κινδύνων. Το μητρώο κινδύνων ενημερώνεται με πληροφορίες από την Ποιοτική Ανάλυση Κινδύνων και το ενημερωμένο μητρώο περιλαμβάνεται στα έγγραφα του έργου. Οι ενημερώσεις του μητρώου κατά την Ποιοτική Ανάλυση Κινδύνου περιλαμβάνουν:

- **Σχετική κατάταξη ή λίστα προτεραιότητας κινδύνων**

Ο πίνακας πιθανοτήτων και αποτελεσμάτων μπορεί να χρησιμοποιηθεί για να ταξινομήσει τους κινδύνους με βάση την ατομική τους σημασία. Χρησιμοποιώντας συνδυασμούς της πιθανότητας εμφάνισης ενός κινδύνου και του αποτελέσματος στους στόχους του έργου, εάν εμφανιζόταν, οι κίνδυνοι παίρνουν προτεραιότητα ο ένας ως προς τον άλλο και ταξινομούνται ως υψηλού, μέτριου και χαμηλού κινδύνου. Οι κίνδυνοι μπορεί να πάρουν προτεραιότητα ξεχωριστά για το πρόγραμμα, το κόστος και το αποτέλεσμά τους, καθώς οι εταιρίες μπορεί να ενδιαφέρονται περισσότερο για την επίτευξη συγκεκριμένων στόχων. Ο project manager μπορεί να με βάση τη λίστα προτεραιοτήτων να δώσει μεγαλύτερη σημασία στους κινδύνους που έχουν μεγαλύτερη σημασία ως προς τους στόχους της εταιρίας, έτσι ώστε οι αποκρίσεις να οδηγήσουν σε καλύτερα αποτελέσματα.

- **Κατηγοριοποίηση κινδύνων**

Η κατηγοριοποίηση των κινδύνων μπορεί να αποκαλύψει κοινά αίτια κινδύνων σε διάφορες περιοχές του έργου που χρίζουν ιδιαίτερης προσοχής. Η ανακάλυψη συγκεκριμένων αιτίων κινδύνου μπορεί να οδηγήσει σε πιο αποτελεσματική αντιμετώπισή του.

- **Αίτια κινδύνου ή περιοχές του έργου που χρειάζονται συγκεκριμένη προσοχή**

Η ανακάλυψη συγκεκριμένων αιτίων κινδύνου μπορεί να οδηγήσει σε πιο αποτελεσματική αντιμετώπισή του.

- **Λίστα κινδύνων που χρειάζονται βραχυπρόθεσμες δράσεις**

Οι κίνδυνοι που πρέπει να αντιμετωπιστούν άμεσα και αυτοί που μπορεί να αντιμετωπιστούν αργότερα μπορεί να μπουν σε διαφορετικές λίστες.

- **Λίστα κινδύνων που χρειάζονται επιπλέον ανάλυση και δράση**

Ορισμένοι κίνδυνοι χρειάζονται περισσότερη ανάλυση συνήθως Ποιοτική.

- **Λίστα παρακολούθησης των κινδύνων χαμηλής προτεραιότητας**

Οι κίνδυνοι που δεν έχουν εκτιμηθεί ως πολύ σημαντικοί κατά την Ποιοτική Ανάλυση, μπορεί να μπουν σε μια λίστα παρακολούθησης για μελλοντική παρακολούθηση.

- **Τάσεις στα αποτελέσματα της ποιοτικής ανάλυσης κινδύνων**

Η επανάληψη της ανάλυσης μπορεί να αποκαλύψει τάσεις και μπορεί να οδηγήσει σε δράσεις ή περαιτέρω ανάλυση κάνοντάς τους περισσότερο ή λιγότερο σημαντικούς.

2.3.4 Ποσοτική Ανάλυση Κινδύνων

Η Ποσοτική Ανάλυση Κινδύνου είναι η διαδικασία αριθμητικής ανάλυσης των αποτελεσμάτων που έχουν οι προσδιορισμένοι κίνδυνοι συνολικά στο έργο. Η Ποσοτική Ανάλυση Κινδύνου γίνεται για κινδύνους που έχουν ιεραρχηθεί προηγουμένως κατά τη διεργασία Ποιοτικής Ανάλυσης Κινδύνου και οι οποίοι έχουν ουσιαστική επίδραση στις απαιτήσεις του έργου. Η Ποσοτική Ανάλυση Κινδύνου αναλύει τα αποτελέσματα των κινδύνων. Επίσης μπορεί να χρησιμοποιηθεί είτε για αριθμητική εκτίμηση του κάθε κινδύνου ξεχωριστά είτε λαμβάνοντας υπόψη όλους τους κινδύνους συνολικά που επηρεάζουν το έργο.

Αποτελεί την ποσοτική προσέγγιση των αποφάσεων σε περιβάλλον αβεβαιότητας.

Η Ποσοτική Ανάλυση ακολουθεί την Ποιοτική Ανάλυση, αν και σε ορισμένες περιπτώσεις δεν είναι αναγκαία. Η διαθεσιμότητα σε χρόνο και χρήμα καθώς και η ανάγκη ή όχι ποιοτικών και ποσοτικών συμπερασμάτων για τους κινδύνους και τις επιδράσεις τους στο έργο θα προσδιορίσει και τις μεθόδους που θα χρησιμοποιηθούν. Η Ποσοτική Ανάλυση θα πρέπει να επαναλαμβάνεται μετά από κάθε σχέδιο απόκρισης κινδύνου ως μέρος της παρακολούθησης και του ελέγχου των κινδύνων για να καθοριστεί αν ο συνολικός κίνδυνος για το έργο έχει μειωθεί ικανοποιητικά.

- **Μητρώο Κινδύνων**

Το μητρώο κινδύνων έχει αναλυθεί προηγουμένως.

- **Σχεδιασμός Διαχείρισης Κινδύνων**

Τα παραπάνω δεδομένα εισόδου έχουν αναλυθεί σε προηγούμενες παραγράφους.

- **Σχεδιασμός Διαχείρισης Κόστους**

Ο σχεδιασμός διαχείρισης κόστους του έργου δημιουργεί τα κριτήρια για το σχεδιασμό, τη δόμηση, την εκτίμηση και τον έλεγχο των εξόδων του έργου. Οι έλεγχοι αυτοί βοηθούν στον προσδιορισμό και της δομής και του ελέγχου του κόστους του έργου και στον προσδιορισμό της ποσοτικής ανάλυσης του προϋπολογισμού.

- **Σχεδιασμός Διαχείρισης Προγράμματος**

Ο σχεδιασμός διαχείρισης προγράμματος του έργου βοηθά αντίστοιχα με το σχεδιασμό του κόστους στον καλύτερο έλεγχο και στην πιο αποτελεσματική προσέγγιση του προγράμματος.

- **Επιχειρησιακές Διαδικασίες**

Οι επιχειρησιακές διαδικασίες βοηθούν και μπορούν να επηρεάσουν την Ποσοτική Ανάλυση Κινδύνου ως εξής:

- Με πληροφόρηση προηγουμένων ίδιων ολοκληρωμένων έργων
- Μελέτη παρόμοιων έργων από ειδικούς
- Βάσεις δεδομένων διαθέσιμες από τη βιομηχανία ή επιχειρησιακές

Ποσοτική Ανάλυση Κινδύνων: Εργαλεία και Τεχνικές

- **Συλλογή Δεδομένων και Τεχνικές Αναπαράστασης**
  - **Συνεντεύξεις**

Οι τεχνικές συνεντεύξεων βασίζονται στην εμπειρία και στα ιστορικά δεδομένα για να ποσοτικοποιήσουν την πιθανότητα και το αποτέλεσμα των κινδύνων στους αντικειμενικούς στόχους του έργου. Η απαραίτητη πληροφορία εξαρτάται από τον τύπο της κατανομής πιθανοτήτων που θα χρησιμοποιηθεί. Για παράδειγμα, οι πληροφορίες θα συλλέγονταν για το αισιόδοξο, το απαισιόδοξο και το πιο πιθανό σενάριο για τις πιο συχνά χρησιμοποιούμενες κατανομές.

- **Πιθανοτικές Κατανομές**

Οι συνεχείς πιθανοτικές κατανομές, που χρησιμοποιούνται εκτενώς στη μοντελοποίηση και στην προσομοίωση, αναπαριστούν την αβεβαιότητα τιμών όπως διάρκειες προγράμματος διαφόρων ενεργειών του έργου και κόστη κομματιών του έργου. Οι διακριτές κατανομές μπορεί να χρησιμοποιηθούν για να αναπαρασταθούν αβέβαια γεγονότα όπως το αποτέλεσμα ενός τέστ ή ένα πιθανό σενάριο σε ένα δέντρο αποφάσεων.

- **Ποσοτική Ανάλυση Κινδύνων και Τεχνικές Μοντελοποίησης**

Οι πιο συχνά χρησιμοποιούμενες τεχνικές περιλαμβάνουν προσεγγίσεις ανάλυσης σχετικές είτε με γεγονότα είτε με το έργο.

- **Ανάλυση Ευαισθησίας**

Η ανάλυση ευαισθησίας βοηθά στον προσδιορισμό των κινδύνων που έχουν τη μεγαλύτερη πιθανή επίπτωση στο έργο. Εξετάζει την έκταση στην οποία η αβεβαιότητα του κάθε μέρους του έργου επηρεάζει τον στόχο που εξετάζεται, όταν όλα τα υπόλοιπα αβέβαια μέρη έχουν τις βασικές τους τιμές. Τυπικό δείγμα ανάλυσης ευαισθησίας είναι το διάγραμμα «ανεμοστρόβιλος» (tornado diagram) το οποίο είναι χρήσιμο για τη σύγκριση παραμέτρων σχετικής σημαντικότητας και επίδρασης οι οποίες έχουν μεγαλύτερο βαθμό αβεβαιότητας σε σχέση με άλλες περισσότερο σταθερές.

- **Αναμενόμενη ανάλυση νομισματικής αξίας**

Η αναμενόμενη ανάλυση νομισματικής αξίας (Expected Monetary Value) είναι μια στατιστική μέθοδος που υπολογίζει το μέσο αποτέλεσμα όταν συμβούν ή όχι μελλοντικά σενάρια (αποτελεί δηλαδή ανάλυση με αβεβαιότητα). Η ανάλυση EMV των ευκαιριών εκφράζεται γενικά με θετικές τιμές, ενώ η ανάλυση των απειλών με αρνητικές. Η ανάλυση EMV απαιτεί υποθέσεις ουδέτερου ρίσκου για να εφαρμοστεί. Η EMV ενός έργου υπολογίζεται πολλαπλασιάζοντας την τιμή του πιθανού αποτελέσματος με την πιθανότητα εμφάνισης και προσθέτοντας τα γινόμενα που προκύπτουν. Μια κοινή χρήση ανάλυσης τέτοιου τύπου αποτελούν τα Δέντρα Αποφάσεων.

- **Μοντελοποίηση και προσομοίωση**

Η προσομοίωση ενός έργου χρησιμοποιεί ένα μοντέλο που μεταφράζει τις προσδιορισμένες με λεπτομέρεια αβεβαιότητες του έργου στο πιθανό αποτέλεσμα στους στόχους του έργου. Προσομοιωτές ολοκλήρωσης χρησιμοποιούν συνήθως τη μέθοδο Monte Carlo. Σε μια προσομοίωση, ένα μοντέλο υπολογίζεται πολλές φορές (ολοκλήρωση) με τις εισόδους (κόστος, διάρκεια εργασιών) να διαλέγονται τυχαία σε κάθε επανάληψη, από τις κατανομές πιθανότητας της κάθε μεταβλητής. Η πιθανοτική κατανομή (συνολικό κόστος ή ημερομηνία ολοκλήρωσης του έργου) υπολογίζεται από τις επαναλήψεις. Για μια ανάλυση κινδύνου κόστους, η προσομοίωση χρησιμοποιεί εκτιμήσεις κόστους. Για μια ανάλυση κινδύνου προγραμματισμού χρησιμοποιείται το διάγραμμα προγράμματος και εκτιμήσεις διάρκειας.

- **Κρίση Εμπειρογνωμόνων**

Η κρίση των εμπειρογνωμόνων (ιδανικά θα πρέπει οι ειδικοί να έχουν σχετική και πρόσφατη εμπειρία) είναι απαραίτητη για τον προσδιορισμό των πιθανών επιπτώσεων στο κόστος και στον προγραμματισμό, και για τον προσδιορισμό των εισόδων (όπως για παράδειγμα οι πιθανοτικές κατανομές) στα διάφορα εργαλεία που θα χρησιμοποιηθούν.

Ποσοτική Ανάλυση Κινδύνων: Συμπεράσματα

- **Ενημερώσεις Μητρώου Κινδύνων**

Το μητρώο κινδύνων ενημερώνεται με τα αποτελέσματα της ποσοτικής ανάλυσης κινδύνων που περιλαμβάνει λεπτομέρειες ως προς την ποσοτική προσέγγιση, τα δεδομένα εξόδου και ενδεχόμενες συστάσεις.

- **Πιθανοτική Ανάλυση του έργου**

Γίνονται εκτιμήσεις για τα πιθανά αποτελέσματα του κόστους και του προγράμματος καταχωρώντας τις ημερομηνίες ολοκλήρωσης μαζί με συνδεδεμένα επίπεδα εμπιστοσύνης. Το αποτέλεσμα αυτό που συχνά εκφράζεται ως μια σωρευτική κατανομή, μπορεί να χρησιμοποιηθεί μαζί με τις ανοχές κινδύνου των εμπλεκομένων για να εμποδίσουν την χρήση αποθεματικών επείγουσας επέμβασης που αφορούν το κόστος και το χρόνο. Τα αποθεματικά αυτά χρειάζονται για να επαναφέρουν στόχους του έργου που έχουν υπερβεί τα όρια, σε επίπεδα αποδεκτά από την επιχείρηση.

- **Πιθανότητα Επίτευξης Στόχων Κόστους και Χρόνου**

Με τους κινδύνους που αντιμετωπίζει το έργο, η πιθανότητα επίτευξης των στόχων του έργου με το συγκεκριμένο σχεδιασμό, μπορεί να εκτιμηθεί με χρήση των αποτελεσμάτων ποσοτικής ανάλυσης κινδύνων.

- **Λίστα Προτεραιοτήτων Ποσοτικοποιημένων Κινδύνων**

Η λίστα κινδύνων περιλαμβάνει αυτούς που αποτελούν μεγαλύτερη απειλή ή παρουσιάζουν μεγαλύτερες ευκαιρίες για το έργο. Περιλαμβάνονται οι κίνδυνοι που έχουν το μεγαλύτερο αποτέλεσμα σε ένα ενδεχόμενο κόστος και αυτοί που είναι περισσότερο πιθανό να επηρεάσουν το κρίσιμο μονοπάτι. Οι κίνδυνοι αυτοί μπορεί να προσδιοριστούν σε ορισμένες περιπτώσεις μέσω ενός διαγράμματος tornado που παράγεται από μια ανάλυση προσομοίωσης.

- **Τάσεις Ποσοτικής Ανάλυσης Αποτελεσμάτων**

Με την επανάληψη της ανάλυσης φανερώνονται πολλές φορές τάσεις που οδηγούν σε συμπεράσματα που επηρεάζουν τις αποκρίσεις στους κινδύνους. Νέες ιδέες μπορεί να προκύψουν μέσα από τη διαδικασία Ποσοτικής Ανάλυσης Κινδύνων που αλλάζοντας τις πληροφορίες ιστορικού μιας επιχείρησης που αφορούν τον προγραμματισμό, κόστη, την ποιότητα και τις επιδόσεις. Αυτά τα ιστορικά στοιχεία μπορεί να πάρουν μια μορφή αναφοράς ποσοτικής ανάλυσης κινδύνων. Η αναφορά μπορεί να είναι χωρισμένη ή συνδεδεμένη με το μητρώο κινδύνων.

2.3.5 Σχεδιασμός Απόκρισης Κινδύνων

Είναι η διαδικασία ανάπτυξης επιλογών και ενεργειών για να ενισχύσουν τις ευκαιρίες και να μειώσουν τις απειλές που θα υπάρξουν κατά τη διάρκεια του έργου.

Ακολουθεί την ποιοτική και ποσοτική ανάλυση. Περιλαμβάνει τον προσδιορισμό και την ανάθεση σε συγκεκριμένα άτομα να αναλάβουν τον σχεδιασμό της απόκρισης σε κάθε κίνδυνο. Ο Σχεδιασμός Απόκρισης είναι μια διαδικασία κατά τη διάρκεια της οποίας αντιμετωπίζονται οι κίνδυνοι με βάση την προτεραιότητα τους, εισάγει πόρους και απαραίτητες δράσεις στον προϋπολογισμό και στον προγραμματισμό του έργου όπου είναι απαραίτητο.

Η αντιμετώπιση κάθε κινδύνου θα πρέπει να είναι ρεαλιστική όσον αφορά το περιβάλλον του έργου, αποδοτική όσον αφορά το κόστος και το χρόνο και να συμφωνούν με αυτή όλοι οι εμπλεκόμενοι του έργου.

- **Μητρώο Κινδύνων**

Το μητρώο κινδύνων έχει αναλυθεί προηγουμένως

- **Σχεδιασμός Διαχείρισης Κινδύνων**

Τα παραπάνω δεδομένα εισόδου έχουν αναλυθεί σε προηγούμενες παραγράφους.

Σχεδιασμός Απόκρισης Κινδύνων: Εργαλεία και Τεχνικές

Υπάρχουν διαθέσιμες διάφορες στρατηγικές απόκρισης στους κινδύνους. Θα πρέπει κάθε φορά να διαλέγεται η στρατηγική ή οι στρατηγικές που είναι πιο αποτελεσματικές για τον κάθε κίνδυνο. Εργαλεία ανάλυσης κινδύνου, όπως τα δέντρα αποφάσεων, μπορεί να χρησιμοποιηθούν για να επιλεγούν οι πιο αποτελεσματικές αποκρίσεις. Συγκεκριμένες ενέργειες αναπτύσσονται για να υλοποιηθεί η κάθε στρατηγική, συμπεριλαμβάνοντας βασικές και δευτερεύουσες στρατηγικές, όπου κρίνεται απαραίτητο. Ένα εφεδρικό σχέδιο μπορεί να αναπτυχθεί για υλοποίηση αν η επιλεγμένη στρατηγική αποδειχθεί λιγότερο αποτελεσματική από το αναμενόμενο, ή αν εμφανιστεί ένας αποδεκτός κίνδυνος. Δευτερεύοντες κίνδυνοι (δηλαδή κίνδυνοι που προκύπτουν από τις στρατηγικές) θα πρέπει επίσης να επανεξετάζονται. Ένα αποθεματικό επείγουσας επέμβασης πολύ συχνά διατίθεται για τον χρόνο ή το κόστος. Αν αναπτυχθεί, μπορεί να περιλαμβάνει ταυτοποίηση των συνθηκών που ενεργοποιούν τη χρήση του.

- **Στρατηγικές Αρνητικών Κινδύνων ή Απειλών**

Τρεις από τις στρατηγικές που ακολουθούν ασχολούνται με απειλές ή κινδύνους που έχουν αρνητικά αποτελέσματα στους στόχους του έργου σε περίπτωση που εμφανιστούν. Η τέταρτη στρατηγική, η αποδοχή, μπορεί να χρησιμοποιηθεί είτε για αρνητικούς κινδύνους ή απειλές, είτε για

θετικούς κινδύνους ή ευκαιρίες. Οι στρατηγικές αυτές είναι η αποφυγή, η μεταφορά, ο μετριασμός και η αποδοχή.

- **Αποφυγή**

Η αποφυγή του κινδύνου περιλαμβάνει την αλλαγή του σχεδιασμού του έργου για την πλήρη εξάλειψη του κινδύνου. Ο project manager μπορεί επίσης να απομονώσει τους στόχους του έργου από την επίδραση του κινδύνου, ή να αλλάξει τον στόχο που επηρεάζεται. Παραδείγματα περιλαμβάνουν την επέκταση του προγράμματος, την αλλαγή της στρατηγικής ή τη μείωση του πεδίου δράσης του έργου. Η πιο ριζοσπαστική στρατηγική αποφυγής είναι η παύση του έργου τελείως. Ορισμένοι κίνδυνοι που εμφανίζονται νωρίς στο έργο μπορούν να αποφευχθούν διευκρινίζοντας απαιτήσεις, αποκτώντας πληροφορίες, βελτιώνοντας την επικοινωνία ή αποκτώντας ειδικές και επιπλέον γνώσεις.

- **Μεταφορά**

Η μεταφορά κινδύνων απαιτεί τη μεταφορά ορισμένων ή όλων των αρνητικών αποτελεσμάτων ή απειλών, μαζί με την ευθύνη της απόκρισης σε έναν εξωτερικό συνεργάτη. Η μεταφορά του κινδύνου απλώς δίνει την ευθύνη διαχείρισης σε έναν εξωτερικό συνεργάτη, δεν εξαλείφει τον κίνδυνο. Η μεταφορά ευθύνης ενός κινδύνου είναι περισσότερο αποτελεσματική σε περιπτώσεις έκθεσης σε οικονομικούς κινδύνους. Η μεταφορά κινδύνου σχεδόν πάντα περιλαμβάνει την πληρωμή στον εξωτερικό συνεργάτη που αναλαμβάνει την αντιμετώπιση του κινδύνου. Τα εργαλεία μεταφοράς ποικίλουν και περιλαμβάνουν (χωρίς να είναι αυστηρά περιορισμένα σε) χρήση ασφάλιστρων, εγγυητικών επιστολών, ενταλμάτων, εγγυήσεων κλπ. Τα συμβόλαια επίσης μπορεί να χρησιμοποιηθούν για τη μεταφορά του κινδύνου σε μια άλλη ομάδα. Για παράδειγμα, όταν ένας αγοραστής έχει ικανότητες που ο πωλητής δεν διαθέτει, μπορεί να είναι καλύτερα να μεταφερθεί δουλειά και το αντίστοιχο ρίσκο στον αγοραστή μέσω συμβολαίου.

- **Μετριασμός**

Η μείωση του κινδύνου σημαίνει τη μείωση της πιθανότητας και του αποτελέσματος ενός σοβαρού κινδύνου, σε αποδεκτά όρια. Οι ενέργειες που γίνονται για τη μείωση της πιθανότητας και του αποτελέσματος ενός κινδύνου που ίσως εμφανιστεί στο έργο είναι περισσότερο αποτελεσματικές από την προσπάθεια διόρθωσης της ζημιάς μετά την εμφάνιση του κινδύνου. Παραδείγματα μείωσης του κινδύνου είναι η υιοθέτηση λιγότερο πολύπλοκων διαδικασιών, η διεξαγωγή περισσότερων ελέγχων ή η επιλογή καλύτερου προμηθευτή. Όπου δεν είναι εφικτό να μειωθεί η πιθανότητα εμφάνισης, η μείωση του αποτελέσματος μπορεί να επικεντρωθεί σε διασυνδέσεις του αποτελέσματος που καθορίζουν τη σοβαρότητά του. Για παράδειγμα, ο σχεδιασμός ενός εφεδρικού συστήματος μπορεί να μειώσει το αποτέλεσμα μιας ζημιάς του αρχικού.

- **Αποδοχή**

Η στρατηγική αυτή υιοθετείται επειδή σπάνια είναι δυνατό να εξαλειφθούν όλοι οι κίνδυνοι και οι απειλές από ένα έργο. Η στρατηγική υποδεικνύει ότι η ομάδα έργου έχει αποφασίσει να μην αλλάξει το σχεδιασμό του έργου για να αντιμετωπίσει έναν κίνδυνο, ή αδυνατεί να προσδιορίσει διαφορετική στρατηγική απόκρισης. Η στρατηγική αυτή μπορεί να είναι είτε ενεργητική είτε παθητική. Η παθητική αποδοχή δεν απαιτεί καμία ενέργεια, εκτός από να καταγράψει τη στρατηγική, αφήνοντας την ομάδα έργου να ασχοληθεί με τους κινδύνους καθώς συμβαίνουν. Η πιο κοινή ενεργητική στρατηγική αποδοχής είναι να δημιουργηθεί ένα αποθεματικό επείγουσας επέμβασης, που περιλαμβάνει χρόνο, χρήματα και πόρους, έτσι ώστε να είναι δυνατός ο χειρισμός των κινδύνων.

- **Στρατηγικές Θετικών Κινδύνων ή Ευκαιριών**

Τρεις από τις τέσσερις αποκρίσεις ασχολούνται με κινδύνους με πιθανά θετικά αποτελέσματα στους στόχους του έργου. Η τέταρτη στρατηγική, η αποδοχή, μπορεί να χρησιμοποιηθεί για αρνητικούς κινδύνους ή απειλές, όπως και για θετικούς κινδύνους και ευκαιρίες. Οι στρατηγικές αυτές που περιγράφονται παρακάτω είναι η εκμετάλλευση, η διανομή, η ενίσχυση και η αποδοχή.

- **Εκμετάλλευση**

Η στρατηγική αυτή επιλέγεται για κινδύνους με θετικά αποτελέσματα, όπου η επιχείρηση θέλει να είναι σίγουρη ότι η ευκαιρία θα πραγματοποιηθεί. Η στρατηγική αυτή επιδιώκει να εξαλείψει την αβεβαιότητα που εμφανίζεται με τον θετικό κίνδυνο, εξασφαλίζοντας ότι η ευκαιρία θα εμφανιστεί σίγουρα. Για παράδειγμα μια επιχείρηση μπορεί να αναθέσει το έργο στους πιο αποτελεσματικούς υπαλλήλους για να μειώσει το χρόνο και το κόστος ολοκλήρωσης του έργου.

- **Διαμερισμός**

Η στρατηγική αυτή εννοεί πως ένας θετικός κίνδυνος και η ευκαιρία που συνεπάγεται, μοιράζεται σε έναν εξωτερικό συνεργάτη που μπορεί να συλλάβει καλύτερα την ευκαιρία για το όφελος του έργου. Παραδείγματα αποτελούν οι συνεργασίες εταιριών έτσι ώστε όλοι οι συνεργαζόμενοι να επωφεληθούν από τις ενέργειες που θα γίνουν.

- **Ενίσχυση**

Η στρατηγική αυτή χρησιμοποιείται για να αυξηθεί η πιθανότητα και/ή τα αποτελέσματα μιας ευκαιρίας. Προσδιορίζοντας και μεγιστοποιώντας τις βασικές κινητήριες δυνάμεις των θετικών αυτών κινδύνων, είναι πιθανό να αυξηθεί η πιθανότητα εμφάνισής τους. Παράδειγμα αποτελεί η χρήση περισσότερων πόρων για να τελειώσει μια ενέργεια νωρίτερα.

- **Αποδοχή**

Αποδοχή μιας ευκαιρίας είναι το να την εκμεταλλευτεί η εταιρία χωρίς όμως να επιδιώκει κάτι τέτοιο ενεργά.

- **Ενδεχόμενες Στρατηγικές Αντιμετώπισης**

Ορισμένες αποκρίσεις σχεδιάζονται για χρήση μόνο αν ένα συγκεκριμένο γεγονός εμφανιστεί. Για κάποιους κινδύνους είναι καταλληλότερο για την ομάδα έργου να φτιάξει ένα σχέδιο απόκρισης που θα εκτελεστεί μόνο κάτω από προκαθορισμένες συνθήκες. Θεωρείται πως θα υπάρχει προειδοποίηση για να υλοποιηθεί το σχέδιο. Τα γεγονότα που ενεργοποιούν μια τέτοια στρατηγική θα πρέπει να προσδιορίζονται και να ακολουθούνται.

- **Κρίση Εμπειρογνωμόνων**

Η κρίση εμπειρογνωμόνων είναι η γνώση μιας ομάδας ανθρώπων που χρησιμοποιείται για τις ενέργειες που πρέπει να γίνουν για ένα συγκεκριμένο και προσδιορισμένο κίνδυνο.

Σχεδιασμός Απόκρισης Κινδύνων: Συμπεράσματα

- **Ενημέρωση Μητρώου Κινδύνων**

Κατά τη διαδικασία Σχεδιασμού Αποκρίσεων Κινδύνων επιλέγονται κατάλληλες αποκρίσεις, όπως έχει συμφωνηθεί, και περιλαμβάνονται στο μητρώο κινδύνων. Το μητρώο κινδύνων θα πρέπει να έχει γραφτεί με λεπτομέρεια που αντιστοιχεί στην προτεραιότητα του κάθε κινδύνου και στη σχεδιασμένη απόκριση. Συνήθως οι υψηλοί και μέτριοι κίνδυνοι γράφονται με λεπτομέρεια. Οι κίνδυνοι που κρίνονται ως χαμηλής προτεραιότητας περιλαμβάνονται σε μια λίστα παρακολούθησης για περιοδικό έλεγχο. Τα στοιχεία του μητρώου κινδύνων σε αυτό το σημείο μπορεί να περιλαμβάνουν:

- Προσδιορισμένους κινδύνους, τις περιγραφές τους, τις περιοχές του έργου που επηρεάζονται, τα αίτια, και πως μπορεί να επηρεάσουν τους στόχους του έργου
- Τα πρόσωπα που είναι υπεύθυνα για τον κάθε κίνδυνο αναλαμβάνουν τις ευθύνες τους
- Τις εξόδους από τη διαδικασία Ποιοτικής Ανάλυσης Κινδύνου, συμπεριλαμβανομένου τις λίστες προτεραιότητας των κινδύνων
- Συμφωνημένες στρατηγικές αποκρίσεων
- Συγκεκριμένες ενέργειες για την υλοποίηση της επιλεγμένης στρατηγικής απόκρισης
- Συμπτώματα και στοιχεία που δείχνουν ότι ένας κίνδυνος μπορεί να εμφανιστεί
- Ενέργειες σχετικές με τον προϋπολογισμό και τον προγραμματισμό που είναι απαραίτητες για την υλοποίηση των επιλεγμένων αποκρίσεων
- Σχέδια επείγουσας ανάγκης που απαιτείται να εκτελεστούν

- Εφεδρικά σχέδια που θα χρησιμοποιηθούν ως αντίδραση σε έναν κίνδυνο που έχει εμφανιστεί και η βασική απόκριση είναι τελικά ανεπαρκής
- Ορισμένους κινδύνους που είναι αναμενόμενο να παραμείνουν και μετά από την εφαρμογή των σχεδιασμένων αποκρίσεων, καθώς και τους κινδύνους που έχουν γίνει σκόπιμα αποδεκτοί
- Δευτερεύοντες κινδύνους που εμφανίζονται ως άμεσο αποτέλεσμα μιας απόκρισης κινδύνου
- Αποθεματικά που υπολογίζονται βασιζόμενα στην ποσοτική ανάλυση κινδύνων του έργου και στο κατώφλι κινδύνου της εταιρίας.

- **Αποφάσεις Συμβολαίων Λόγω Κινδύνων**

Αποφάσεις για μεταφορά του κινδύνου, όπως συμφωνίες για ασφάλιση, υπηρεσίες και άλλα στοιχεία, επιλέγονται επίσης σε αυτή τη διαδικασία. Αυτό μπορεί να συμβεί ως αποτέλεσμα μείωσης ή μεταφοράς μέρους ή όλης της απειλής, ή ενίσχυσης ή μοιράσματος μέρους ή όλης της ευκαιρίας. Το είδος του συμβολαίου που επιλέγεται παρέχει επίσης έναν μηχανισμό διαμοιρασμού των κινδύνων.

- **Ενημέρωση Σχεδιασμού Έργου**

Στοιχεία του σχεδιασμού διαχείρισης του έργου που μπορεί να ενημερωθούν περιλαμβάνουν:

- **Σχεδιασμό Προγραμματισμού Έργου**

Ο σχεδιασμός προγραμματισμού έργου ενημερώνεται για να αντικατοπτρίσει τις αλλαγές που γίνονται στη διαδικασία και στις ενέργειες λόγω των αποκρίσεων κινδύνου. Μπορεί να περιλαμβάνει αλλαγές στην ανοχή ή στη συμπεριφορά των πόρων ως προς την ποσότητα εργασιών, καθώς και στο πρόγραμμα χρονικά.

- **Σχεδιασμό Κόστους Έργου**

Ο σχεδιασμός κόστους έργου ενημερώνεται για να αντικατοπτρίσει τις αλλαγές που γίνονται στη διαδικασία και στις ενέργειες λόγω των αποκρίσεων κινδύνου. Μπορεί να περιλαμβάνει αλλαγές στην ανοχή ή στη συμπεριφορά σχετικά με τη λογιστική του κόστους, την παρακολούθηση και τις αναφορές, καθώς και ενημερώσεις στον προϋπολογισμό και στην κατανάλωση των αποθεματικών.

- **Σχεδιασμό Ποιότητας Έργου**

Ο σχεδιασμός ποιότητας έργου ενημερώνεται για να αντικατοπτρίσει τις αλλαγές που γίνονται στη διαδικασία και στις ενέργειες λόγω των αποκρίσεων κινδύνου. Μπορεί να περιλαμβάνει αλλαγές στην ανοχή ή στη συμπεριφορά σχετικά με τις απαιτήσεις, την διαβεβαίωση ποιότητας, ή τον έλεγχο ποιότητας, καθώς και ενημερώσεις των εγγράφων με τις απαιτήσεις του έργου.

- **Σχεδιασμό Προμηθειών Έργου**

Ο σχεδιασμός προμηθειών έργου ενημερώνεται για να αντικατοπτρίσει τις αλλαγές που γίνονται στη στρατηγική, όπως εναλλαγές στις αποφάσεις μεταξύ κατασκευής ή αγοράς ορισμένων στοιχείων ή στους τύπους συμβολαίων, που επηρεάζονται από τις αποκρίσεις κινδύνου.

- **Σχεδιασμό Ανθρωπίνων Πόρων Έργου**

Ο σχεδιασμός ανθρωπίνων πόρων έργου, που είναι μέρος του σχεδιασμού ανθρωπίνων πόρων, ενημερώνεται για να αντικατοπτρίσει τις αλλαγές που γίνονται στην οργανωτική δομή του έργου και στις εφαρμογές των πόρων, που οφείλονται στις αποκρίσεις κινδύνου. Μπορεί να περιλαμβάνει αλλαγές στην ανοχή ή στη συμπεριφορά σχετικές με την κατανομή του προσωπικού, καθώς και με την ποσότητα των εργασιών που αναθέτεται στους πόρους.

- **Αναλυτική Δομή Εργασιών**

Η αναλυτική δομή εργασιών μπορεί να αλλάξει λόγω του νέου φόρτου εργασιών ή των αλλαγών του που οφείλονται στις αποκρίσεις των κινδύνων.

- **Βασικό Χρονοδιάγραμμα**

Το βασικό χρονοδιάγραμμα μπορεί να αλλάξει λόγω του νέου φόρτου εργασιών ή των αλλαγών του που οφείλονται στις αποκρίσεις των κινδύνων.

- **Βασικό Κόστος Επίδοσης**

Το βασικό κόστος επένδυσης μπορεί να αλλάξει λόγω του νέου φόρτου εργασιών ή των αλλαγών του που οφείλονται στις αποκρίσεις των κινδύνων.

- **Ενημερώσεις Εγγράφων Έργου**

Η ενημέρωση των εγγράφων του έργου περιλαμβάνει:

- **Ενημερώσεις Παραδοχών**

Νέες πληροφορίες γίνονται διαθέσιμες με την εφαρμογή των αποκρίσεων κινδύνων, οπότε οι διάφορες παραδοχές που έχουν γίνει αλλάζουν. Η ενημέρωση των παραδοχών λόγω των αλλαγμένων πληροφοριών είναι απαραίτητη και γίνεται είτε στη δήλωση του πεδίου εφαρμογής του έργου είτε σε ξεχωριστά έγγραφα.

- **Ενημερώσεις τεχνικών εγγράφων**

Νέες πληροφορίες γίνονται διαθέσιμες με την εφαρμογή των αποκρίσεων κινδύνων, επομένως τεχνικές προσεγγίσεις ή παραδοτέα που έχουν αποφασιστεί θα πρέπει να επανεξεταστούν.

2.3.6 Παρακολούθηση και Έλεγχος Κινδύνων

Είναι η διαδικασία εφαρμογής του σχεδίου αντιμετώπισης κινδύνων, παρακολούθησης των προσδιορισμένων κινδύνων, καθορισμός νέων κινδύνων και αξιολόγηση της αποτελεσματικότητας της διαδικασίας διαχείρισης κινδύνου σε όλο το έργο.

Η αντιμετώπιση των κινδύνων που έχουν συμπεριληφθεί στον προγραμματισμό του έργου εκτελούνται καθ'όλη τη διάρκεια ζωής του έργου ενώ παράλληλα θα πρέπει να είναι συνεχής η παρακολούθηση και ο έλεγχος για τυχόν νέους κινδύνους.

Η διαδικασία παρακολούθησης και ελέγχου των κινδύνων απαιτεί τη χρήση πληροφορίας που παρέχεται κατά τη διάρκεια του έργου. Επίσης χρησιμοποιείται για τον προσδιορισμό των παρακάτω:

- Αν οι αρχικές υποθέσεις του έργου είναι ακόμη έγκυρες.
- Αν η ανάλυση που έχει γίνει δείχνει ότι ένας κίνδυνος έχει ξεπεραστεί ή έχει αλλάξει.
- Αν οι διαδικασίες της διαχείρισης κινδύνου ακολουθούνται.
- Αν η αρχική πρόβλεψη κόστους και σχεδιασμού όσον αφορά τον κίνδυνο θα πρέπει να αλλάξει σε σχέση με την τρέχουσα εκτίμηση κινδύνου.

Η παρακολούθηση και ο έλεγχος των κινδύνων μπορεί να περιλαμβάνει εναλλακτικές στρατηγικές, διορθωτικές ενέργειες και αλλαγή στον προγραμματισμό του έργου. Το άτομο που αναλαμβάνει να διαχειριστεί το κάθε πιθανό ενδεχόμενο που αφορά έναν κίνδυνο θα πρέπει να αναφέρει περιοδικά στον διαχειριστή του έργου τυχόν αναπάντεχα φαινόμενα, να κρίνει αν είναι ή όχι αποτελεσματικό το υπάρχον πλάνο διαχείρισης του κινδύνου και να προτείνει αλλαγές εάν κάτι τέτοιο θεωρηθεί αναγκαίο.

Τέλος τα δεδομένα που αφορούν ένα κίνδυνο, ανεξάρτητα από το αν θα παρουσιαστεί ή όχι κατά τη διάρκεια του έργου, διατηρούνται στη βάση δεδομένων του οργανισμού που το εκτελεί και δύναται να χρησιμοποιηθούν για μελλοντικά έργα.

- **Μητρώο Κινδύνων**

Το μητρώο κινδύνων έχει σημαντικές εισόδους για το έργο και περιλαμβάνει τους προσδιορισμένους κινδύνους και τους υπεύθυνους, συμφωνημένες αποκρίσεις, συγκεκριμένες ενέργειες υλοποίησης, συμπτώματα και προειδοποιητικά σημάδια κινδύνων, δευτερεύοντες κινδύνους, λίστα παρακολούθησης κινδύνων χαμηλής προτεραιότητας, καθώς και αποθεματικά χρόνου και κόστους.

- **Σχεδιασμός Διαχείρισης Έργου**

Ο σχεδιασμός διαχείρισης έργου εμπεριέχει το σχεδιασμό διαχείρισης κινδύνων, που περιλαμβάνει ανοχές κινδύνου, πρωτόκολλα και αναθέσεις ανθρώπων (συμπεριλαμβανομένου υπεύθυνων κινδύνου) και χρόνου, καθώς και άλλους πόρους στο σχεδιασμό διαχείρισης κινδύνων.

- **Πληροφορίες Προόδου Εργασιών**

Οι πληροφορίες προόδου εργασιών που σχετίζονται με διάφορα αποτελέσματα προόδου, περιλαμβάνουν:

- Κατάσταση Παραδοτέων
- Πρόοδο προγράμματος
- Υφιστάμενα Κόστη

- **Αναφορές Προόδου**

Οι αναφορές προόδου παίρνουν πληροφορίες από μετρήσεις προόδου και τις αναλύουν, παρέχοντας πληροφορίες προόδου των εργασιών του έργου, συμπεριλαμβάνοντας ανάλυση διακύμανσης, δεδομένα εκτελεσθείσας αξίας, και δεδομένα προβλέψεων.

Παρακολούθηση και Έλεγχος Κινδύνων: Εργαλεία και Τεχνικές

- **Επανεκτίμηση Κινδύνων**

Η Παρακολούθηση και ο Έλεγχος των Κινδύνων έχει ως αποτέλεσμα τον προσδιορισμό νέων κινδύνων, επανεκτίμηση τωρινών κινδύνων, και το κλείσιμο των παλαιότερων κινδύνων. Η επανεκτίμηση των κινδύνων του έργου θα πρέπει να προγραμματίζεται τακτικά. Η επανάληψη της διαδικασίας επανεκτίμησης εξαρτάται από την πρόοδο του έργου σε σχέση με τους στόχους του.

- **Έλεγχος Κινδύνων**

Ο έλεγχος κινδύνων εξετάζει και καταγράφει την αποτελεσματικότητα των αποκρίσεων σε σχέση με τους προσδιορισμένους κινδύνους και τα αίτιά τους, καθώς και ως προς την αποτελεσματικότητα της διαδικασίας διαχείρισης κινδύνων. Ο διαχειριστής του έργου είναι υπεύθυνος για τη διασφάλιση εκτέλεσης των ελέγχων με τη σωστή συχνότητα, όπως καθορίζεται στο σχεδιασμό διαχείρισης έργου. Οι έλεγχοι κινδύνων μπορεί να συμπεριλαμβάνονται στις καθιερωμένες συναντήσεις για την πρόοδο του έργου, ή σε ξεχωριστές συναντήσεις. Ο τρόπος που γίνεται ο έλεγχος και οι σκοποί του θα πρέπει να έχουν καθοριστεί πριν την εφαρμογή του.

- **Ανάλυση Διακύμανσης και Τάσης**

Πολλές διαδικασίες ελέγχου χρησιμοποιούν ανάλυση διακύμανσης για να συγκρίνουν τα σχεδιασμένα με τα πραγματικά αποτελέσματα. Για τους σκοπούς της παρακολούθησης και ελέγχου των γεγονότων κινδύνου, θα πρέπει να επανεξετάζονται οι τάσεις που εμφανίζονται κατά την εκτέλεση του έργου χρησιμοποιώντας πληροφορίες επίδοσης. Ανάλυση εκτελεσθείσας αξίας και άλλες μέθοδοι ανάλυσης διακύμανσης και τάσεων του έργου μπορεί να χρησιμοποιηθούν για την παρακολούθηση της συνολικής επίδοσης του έργου. Τα αποτελέσματα από μια τέτοια ανάλυση μπορεί να προβλέψουν πιθανή παρέκκλιση του έργου από τους στόχους κόστους και προγραμματισμού. Μια τέτοια παρέκκλιση μπορεί να δείχνει τυχόν εμφάνιση απειλών ή ευκαιριών.

- **Μέτρηση Τεχνικών Επιδόσεων**

Η μέτρηση τεχνικών επιδόσεων συγκρίνει τους τεχνικούς στόχους που πραγματοποιήθηκαν κατά τη διάρκεια του έργου με την τεχνική πρόοδο που υπάρχει στον αρχικό σχεδιασμό του έργου. Απαιτεί τον προσδιορισμό των ποσοτικά μετρήσιμων τεχνικών στόχων, που θα συγκριθούν με τους αρχικά προσδιορισμένους. Οι μετρήσεις τεχνικής επίδοσης μπορεί να περιλαμβάνουν χρόνους αλληλεπίδρασης, αριθμό ελαττωματικών στοιχείων, χωρητικότητα αποθήκευσης και άλλα. Τυχόν αποκλίσεις σε σχέση με το αρχικό πλάνο βοηθούν στην πρόβλεψη επίτευξης του αρχικού πλάνου του έργου, και μπορεί να εκθέσει και τυχόν τεχνικούς κινδύνους που θα εμφανιστούν.

- **Ανάλυση Αποθεματικών**

Κατά τη διάρκεια εκτέλεσης του έργου, ορισμένοι κίνδυνοι μπορεί να εμφανιστούν, με θετικές ή αρνητικές επιπτώσεις στα αποθεματικά προϋπολογισμού και προγραμματισμού. Η ανάλυση αποθεματικών συγκρίνει την ποσότητα αποθεματικών που απομένει με την ποσότητα του κινδύνου που απομένει σε κάθε χρονική στιγμή του έργου, με σκοπό να προσδιοριστεί εάν τα αποθεματικά που υπάρχουν είναι επαρκή.

- **Συναντήσεις Κατάστασης Έργου**

Η διαχείριση κινδύνων του έργου θα πρέπει να αποτελεί μέρος της συζήτησης στις συναντήσεις που γίνονται περιοδικά για τον έλεγχο του έργου. Ο χρόνος που απαιτείται για το λόγο αυτό ποικίλλει ανάλογα με τους κινδύνους που έχουν προσδιοριστεί, την προτεραιότητά τους, και τη δυσκολία απόκρισης. Η διαχείριση κινδύνων είναι πιο εύκολη όσο συχνότερα γίνεται. Συχνές συζητήσεις από τους εμπλεκομένους για τους κινδύνους αυξάνει την πιθανότητα προσδιορισμού τους, καθώς και ευκαιριών από μπορεί να εμφανιστούν.

Παρακολούθηση και Έλεγχος Κινδύνων: Συμπεράσματα

- **Ενημέρωση Μητρώου Κινδύνων**

Ένα ενημερωμένο μητρώο κινδύνων περιλαμβάνει:

- Αποτελέσματα επανεξέτασης κινδύνων, ελέγχου κινδύνων, και περιοδικής αναθεώρησης κινδύνων. Τα αποτελέσματα αυτά μπορεί να περιλαμβάνουν προσδιορισμό νέων γεγονότων κινδύνου και ενημερώσεις πιθανότητας, αποτελέσματος, προτεραιότητας, σχεδίων απόκρισης, υπευθυνότητας και άλλως στοιχείων του μητρώου κινδύνων.
- Πραγματικά αποτελέσματα των κινδύνων του έργου και των αποκρίσεών τους. Οι πληροφορίες αυτές μπορεί να βοηθήσουν τους διαχειριστές του έργου στο σχεδιασμό ρίσκου στην επιχείρησή τους, καθώς και σε μελλοντικά έργα.

- **Ενημέρωση Διαδικασιών Επιχείρησης**

Οι έξι διαδικασίες Διαχείρισης Κινδύνου Έργου παράγουν πληροφορίες που μπορεί να χρησιμοποιηθούν για μελλοντικά έργα, και θα πρέπει να καταγραφούν ως περιουσιακά στοιχεία της επιχείρησης. Τα περιουσιακά στοιχεία που μπορεί να ενημερωθούν περιλαμβάνουν:

- Πρότυπα για το σχεδιασμό διαχείρισης κινδύνου, που περιλαμβάνουν τον πίνακα πιθανοτήτων και αποτελεσμάτων, και το μητρώο κινδύνων
- Αναλυτική Δομή Κινδύνων
- Διδάγματα από τις δραστηριότητες διαχείρισης κινδύνου του έργου.

Τα έγγραφα αυτά θα πρέπει να ενημερώνονται σωστά κατά το κλείσιμο του έργου. Περιλαμβάνονται τελικές εκδόσεις καταλόγου κινδύνων, πρότυπα σχεδιασμού διαχείρισης κινδύνου, λίστας ελέγχου και αναλυτικής δομής κινδύνων.

- **Αιτήματα Αλλαγής**

Η υλοποίηση σχεδίων επείγουσας επέμβασης μπορεί να καταλήξει σε κάποιο αίτημα αλλαγής. Τα αιτήματα αυτά ετοιμάζονται και υποβάλλονται κατά τη διάρκεια κατάλληλης διαδικασίας. Επίσης μπορεί να περιέχουν διορθωτικές και προληπτικές ενέργειες.

- **Προτεινόμενες διορθωτικές αλλαγές**. Οι προτεινόμενες διορθωτικές αλλαγές περιλαμβάνουν σχέδια επείγουσας επέμβασης και λύσεις. Οι λύσεις είναι αποκρίσεις που δεν είχαν σχεδιαστεί αρχικά αλλά είναι απαραίτητες για αναδυόμενους κινδύνους που ήταν απροσδιόριστοι ή παθητικά αποδεκτοί.
- **Προτεινόμενες προληπτικές ενέργειες**. Οι προτεινόμενες προληπτικές ενέργειες αποτελούν γραπτές οδηγίες εκτέλεσης μιας ενέργειας που μπορεί να μειώσει την πιθανότητα εμφάνισης αρνητικών συνεπειών σχετικών με κινδύνους του έργου.

- **Ενημέρωση Σχεδιασμού Διαχείρισης Έργου**

Εάν οι εγκεκριμένες αιτήσεις αλλαγής έχουν επίδραση στη διαδικασία διαχείρισης κινδύνων, τα αντίστοιχα έγγραφα στοιχείων του σχεδιασμού διαχείρισης του έργου αναθεωρούνται και επανεκδίδονται για να αντικατοπτρίσουν τις εγκεκριμένες αλλαγές. Τα στοιχεία του σχεδιασμού διαχείρισης έργου που ενημερώνονται είναι τα ίδια με αυτά της διαδικασίας Σχεδιασμού Αποκρίσεων Κινδύνων.

- **Ενημέρωση Εγγράφων Έργου**

Τα έγγραφα έργου που μπορεί να ενημερωθούν από τη διαδικασία Παρακολούθησης και Ελέγχου των Κινδύνων είναι ίδια με αυτά της διαδικασίας Σχεδιασμού Αποκρίσεων Κινδύνων.

ΚΕΦΑΛΑΙΟ 3

3.1 Βασικές Αρχές Διαχείρισης κινδύνων στα Έργα Πληροφορικής

Σκοπός της Διαχείρισης Κινδύνων

Η διαχείριση κινδύνων στα έργα πληροφορικής έχει διαφορετικά ζητήματα που πρέπει να επιλύσει (σε σχέση με τα έργα μη πληροφορικής). Βοηθάει στη διάσωση έργων από την αποτυχία εξαιτίας διαφορετικών παραγόντων, όπως μη ολοκλήρωση των έργων μέσα στο καθορισμένο χρονοδιάγραμμα και προϋπολογισμό, και μη ικανοποίησης των απαιτήσεων του πελάτη.

Η διαχείριση κινδύνων εξετάζει τα έργα από διαφορετικές οπτικές γωνίες για να διασφαλίσει ότι οι απειλές που μπορούν να θέσουν σε κίνδυνο τα έργα έχουν προσδιορισθεί, αναλυθεί και έχουν ληφθεί οι κατάλληλες στρατηγικές για να μετριάσουν και να ελέγξουν τους κινδύνους. Οι στρατηγικές μετριασμού των κινδύνων δεν σημαίνουν απαραίτητα ότι θα καταργήσουμε από το έργο τις δραστηριότητες που εμπεριέχουν κίνδυνο.

Στις εταιρείες πληροφορικής πολλές δραστηριότητες μπαίνουν σε φάση υλοποίησης, ακόμα και εάν οι εταιρείες γνωρίζουν ότι αυτές οι δραστηριότητες εμπεριέχουν υψηλό κίνδυνο. Πολλές φορές οι δραστηριότητες που εμπεριέχουν υψηλούς κινδύνους είναι σημαντικές για μια επιχείρηση, για να αποκτήσει η επιχείρηση στρατηγικό πλεονέκτημα έναντι των ανταγωνιστών της.

Ο κύριος σκοπός της διαχείρισης κινδύνων σε ένα έργο είναι να γνωρίζει όλους τους κινδύνους, να εκτιμήσει την σοβαρότητά τους και τις πιθανές συνέπειες που μπορεί να προκαλέσουν και να καθορίσει τα στάδια αντιμετώπισης και εξάλειψης των κινδύνων ανάλογα με την φύση τους. Η κεντρική ιδέα είναι η εξάλειψη οποιουδήποτε αναπάντεχου προβλήματος που μπορεί να προκύψει κατά την διάρκεια του έργου, με το να είναι έτοιμοι και σε εγρήγορση για όλα τα ενδεχόμενα τόσο ο διευθυντής του έργου όσο και η ομάδα του έργου. Ο σωστός σχεδιασμός και η καλή προετοιμασία οδηγούν στην ελαχιστοποίηση των αβεβαιοτήτων, οι οποίες μπορεί να οδηγήσουν σε ολοκλήρωση του έργου με προβλήματα, ή ακόμα χειρότερα και σε πρόωρο τερματισμό του έργου.

Η διαχείριση κινδύνων στην τεχνολογία λογισμικού, και κατ' επέκταση στα έργα πληροφορικής, χρησιμοποιεί μια πολύ προσεκτική προσέγγιση λαμβάνοντας όλα τα δυνατά προληπτικά μέτρα, έτσι ώστε να γίνει η ολοκλήρωση ενός έργου μέσα στον καθορισμένο χρόνο και προϋπολογισμό. Στην πραγματικότητα στα έργα που λαμβάνονται υπόψη οι κίνδυνοι το τελικό αποτέλεσμα είναι πολύ καλύτερο τόσο από πλευράς τελικού κόστους και χρόνου υλοποίησης όσο και από την πλευρά της ποιότητας των παραδοτέων. Χωρίς την διαχείριση κινδύνων θα υπήρχε μεγάλη πιθανότητα οι εταιρείες που υλοποιούν έργα να χάσουν τόσο έσοδα όσο και την φήμη τους στους πελάτες (όπως

και συμβαίνει άλλωστε), ή ακόμα χειρότερα να οδηγηθούν σε ολοκληρωτική πτώχευση οι συμμετέχοντες επιχειρήσεις / οργανισμοί σε ένα έργο.

3.2 Η Διαχείριση Κινδύνων και οι Διαστάσεις της

Η διαχείριση κινδύνων στην τεχνολογία λογισμικού υπάρχει και χρησιμοποιείται εδώ και αρκετές δεκαετίες. Ωστόσο, όπως αναφέρθηκε και νωρίτερα, τα τελευταία χρόνια έχει αποκτήσει καθολική αναγνώριση και αποδοχή από την κοινότητα της τεχνολογίας λογισμικού. Στα έργα πληροφορικής που υλοποιήθηκαν μέχρι και τις αρχές του 21ου αιώνα χρησιμοποιούνταν διαφορετικές και κατά περίπτωση προσεγγίσεις για την διαχείριση κινδύνων, χωρίς παρόλα αυτά να εφαρμόζονται κάποιες συγκεκριμένες μεθοδολογίες. Η ολοένα και αυξανόμενη πολυπλοκότητα των έργων πληροφορικής οδήγησε τις εταιρείες να κατανοήσουν την σπουδαιότητα της διαχείρισης κινδύνων, γιατί πολύ απλά βοηθάει στην εξάλειψη των αβεβαιοτήτων και μειώνει την πιθανότητα να αποτύχει κάποιο έργο.

3.3 Διαχείριση Κινδύνων Πληροφορικής σε Εταιρείες

Το αποτέλεσμα ενός έργου πληροφορικής, είτε είναι προϊόν λογισμικού είτε υπηρεσία πρέπει να έχει σχεδιαστεί σωστά για να μπορέσει να λειτουργήσει αποδοτικά στο περιβάλλον στο οποίο λειτουργεί η επιχείρηση. Είναι σημαντικό να κατανοήσουμε το αντίκτυπο που θα έχει για την επιχείρηση ένα προϊόν λογισμικού το οποίο είτε δυσλειτουργεί, είτε δεν εκπληρώνει τους στόχους για τους οποίους είχε σχεδιαστεί. Σε κάθε περίπτωση όλοι οι κίνδυνοι (ή οι περισσότεροι) που προέρχονται από την τεχνολογία των πληροφοριών θα μπορούσαν να έχουν εξαλειφθεί, εάν κατά το έργο πληροφορικής που απέδωσε το/α συγκεκριμένο/α παραδοτέο/α είχαν ληφθεί υπόψη οι κίνδυνοι που σχετίζονται τόσο με την ανάπτυξη του προϊόντος όσο και με την λειτουργία του.

Πρέπει να κατανοήσουμε ότι τα προϊόντα λογισμικού συντηρούνται και επεκτείνονται σε όλη τη διάρκεια του κύκλου ζωής τους μέχρι να βγουν εκτός παραγωγής. Επιπλέον, πρέπει να έχουμε στο μυαλό μας ότι το πληροφοριακό περιβάλλον της επιχείρησης μεταβάλλεται και δεν μένει σταθερό (π.χ. αλλαγή δικτυακής υποδομής, μεταβολή τελικών χρηστών, νέες πολιτικές ασφάλειας κλπ).

Συνεπώς, η ιδιαίτερη φύση των έργων πληροφορικής και η μεταβλητότητα του πληροφοριακού περιβάλλοντος πρέπει να ληφθούν υπόψη κατά το σχεδιασμό και την ανάπτυξη του προϊόντος λογισμικού.

Στα έργα πληροφορικής παίζει πολύ μεγάλο ρόλο η εμπειρία του διευθυντή του έργου στους τομείς του σχεδιασμού, της ανάπτυξης και του ελέγχου του τελικού προϊόντος, έτσι ώστε να

μπορέσει να τους απεικονίσει με ακρίβεια στο σχέδιο διοίκησης του έργου και να δώσει τις σωστές κατευθυντήριες γραμμές στην ομάδα του έργου.

Το καλό τεχνικό υπόβαθρο του διευθυντή ενός έργου πληροφορικής θα βοηθήσει στο να υπάρχει:

- Καλύτερη κατανόηση των τεχνικών δυσκολιών
- Έγκαιρος προσδιορισμός των κινδύνων
- Καλύτερη επικοινωνία με την ομάδα έργου
- Αποφυγή παρανοήσεων μεταξύ των συμμετεχόντων στο έργο
- Αποτελεσματικότερη παρακολούθηση της πορείας ανάπτυξης του προϊόντος

Είναι απαραίτητο να κατανοήσουμε τους κινδύνους που απορρέουν από την χρήση της τεχνολογίας της πληροφορικής σε μια επιχείρηση έτσι ώστε να μπορέσουμε να κατανοήσουμε το περιβάλλον στο οποίο θα κληθεί να λειτουργήσει το προϊόν λογισμικού που θα υλοποιηθεί ως αποτέλεσμα του έργου.

Μία από τις ιδιαιτερότητες των έργων πληροφορικής είναι το ότι δεν μπορούμε να είμαστε σίγουροι ότι το αποτέλεσμα του έργου είναι «καλό» εάν δεν δουλέψει σε πραγματικές συνθήκες (στο περιβάλλον παραγωγής της εταιρείας). Σε ένα κατασκευαστικό έργο γνωρίζουμε πως εάν έχουμε τηρήσει τους κανόνες των τεχνικών επιμελητηρίων και τις προδιαγραφές του έργου το αποτέλεσμα θα είναι άρτιο.

Όμως σε ένα έργο πληροφορικής εάν το λογισμικό ή υπηρεσία δεν λειτουργήσει σε περιβάλλον παραγωγής και δεν δοκιμαστεί έντονα δεν μπορούμε να είμαστε σίγουροι ότι το αποτέλεσμα είναι άρτιο. Για αυτό ακριβώς το λόγο πρέπει να κατανοήσουμε τους κινδύνους πληροφορικής σε μια επιχείρηση έτσι ώστε κατά την εκτέλεση ενός έργου πληροφορικής να τους λάβουμε υπόψη για να δημιουργήσουμε έναν όσο το δυνατόν αρτιότερο αποτέλεσμα.

Εάν δεν το κάνουμε αυτό υπάρχει ο κίνδυνος να μην πάρει αποδοχή το λογισμικό από την εταιρεία και όλο το έργο να βγει εκτός πλάνου στην καλύτερη περίπτωση. Στην χειρότερη περίπτωση μπορεί το έργο να ακυρωθεί με όλες τις αρνητικές συνέπειες για όλους τους συμμέτοχους στο έργο. Στα έργα πληροφορικής το έργο ολοκληρώνεται όταν το λογισμικό ή η υπηρεσία λειτουργήσει πλήρως και αποδοτικά στο περιβάλλον της επιχείρησης. Εάν αυτό δεν συμβεί τότε το έργο δεν θα παραδοθεί.

Συνεπώς, είναι λάθος να μην ληφθούν υπόψη οι κίνδυνοι της πληροφορικής στις εταιρείες, γιατί και το ίδιο το λογισμικό που αναπτύσσεται θα κληθεί να τους αντιμετωπίσει αφού θα λειτουργήσει στο περιβάλλον της επιχείρησης.

3.4 Πολιτική προστασίας – μηχανισμοί ασφαλείας

3.4.1 Γενική αρχή κανόνων ασφαλείας

Γενική αρχή κανόνων ασφαλείας αποτελεί η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) που έχει ως στόχο της την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από τον νόμο.

Από πρακτική άποψη, η ασφάλεια μπορεί να έγκειται στην επαρκή προστασία ανθρώπων και αγαθών, για την οποία μπορεί να λαμβάνονται διάφορα μέτρα προστασίας από πιθανούς κινδύνους. Για παράδειγμα, η φυσική ασφάλεια ενός κτηρίου έγκειται στην αποτροπή εισόδου κακόβουλων ατόμων και στην αποτροπή ζημιών από φυσικές καταστροφές. Αντίστοιχα, η ασφάλεια μίας ηλεκτρονικής βάσης δεδομένων έγκειται στην προστασία των δεδομένων από καταστροφή, διαγραφή, αλλοίωση ή αποκάλυψη σε μη εξουσιοδοτημένους χρήστες. Θα πρέπει να ορίζονται, να τεκμηριώνονται, να εφαρμόζονται και να αναθεωρούνται συγκεκριμένες διαδικασίες ασφάλειας.

Οι διαδικασίες ασφάλειας καθορίζονται από την ΑΔΑΕ και ορίζουν συγκεκριμένες ενέργειες των εργαζομένων και των συνεργατών τους, των χρηστών και των συνδρομητών, του προσώπου που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών, την αλληλουχία των ενεργειών, τους υπεύθυνους για την εκτέλεσή τους και τον τρόπο και τα μέσα τεκμηρίωσής τους

3.4.2 Γενική αρχή ασφαλούς μεταφοράς δεδομένων μέσω διαδικτύου

Για την ασφάλεια και την διασφάλιση του απορρήτου των εφαρμογών διαδικτύου έχουν αναπτυχθεί διάφορα πρωτόκολλα και εφαρμογές που βασίζονται στις γενικές αρχές κρυπτογράφησης. Ανάλογα και με τον τύπο της εφαρμογής έχουν προτυποποιηθεί και συγκεκριμένα πρωτόκολλα .

Οι πάροχοι διαδικτυακών υπηρεσιών οφείλουν να κάνουν χρήση των ευρέως αποδεκτών τεχνικών και πρωτοκόλλων ασφαλείας των εφαρμογών διαδικτύου. Ενδεικτικά αναφέρονται για εφαρμογές παγκοσμίου ιστού (www) το πρωτόκολλο SSL (Secure Sockets Layer) , για εφαρμογές ηλεκτρονικού ταχυδρομείου το S/MIME, το PEM (Privacy Enhanced Mail) και το PGP (Pretty Good Privacy)και για ηλεκτρονικές πληρωμές μέσω πιστωτικών καρτών το πρωτόκολλο SET (Secure Electronic Transaction).

Δεδομένου ότι τα νέα πρωτόκολλα και τεχνολογίες θα ανακύπτουν με την πρόοδο της επιστήμης των υπολογιστών, η ΑΔΑΕ θα εκδίδει τεχνικές οδηγίες και συστάσεις προς τους παρόχους διαδικτύου σχετικά με τα νέα πρωτόκολλα και τις τεχνολογίες.

Οι πάροχοι διαδικτύου είναι υποχρεωμένοι να ακολουθούν τα εκάστοτε ευρέως χρησιμοποιούμενα πρωτοκόλλα και τεχνολογίες, είτε αυτόβουλα είτε έπειτα από έλεγχο και αντίστοιχη οδηγία από την ΑΔΑΕ.

3.4.3 Γενική αρχή των υποχρεώσεων των παροχέων διαδικτυακών υπηρεσιών

Πρωταρχικό στοιχείο για την διασφάλιση του απορρήτου των επικοινωνιών στο διαδίκτυο αποτελεί η ύπαρξη πολιτικής ασφάλειας στους παρόχους, η οποία αφορά τους χρήστες, τους χρήστες του παρόχου και στα συστήματα που εμπλέκονται στην επικοινωνία από και προς το Διαδίκτυο.

Η γενική αρχή που θα πρέπει να ακολουθήσει ο πάροχος πρέπει να ανταποκρίνεται στις ειδικές απαιτήσεις της ασφάλειας του, να καθορίζει την πολιτική πρόσβασης σε συστήματα και πληροφορίες, την πολιτική αποδεκτής χρήσης , τι ενέργειες που ακολουθούνται για την διατήρηση τις ασφάλειας και τα μέτρα που εφαρμόζονται σε περιπτώσεις παραβίασης ή έκτακτης ανάγκης. Μέσω της γενικής αρχής των παροχέων διαδικτύου προστατεύονται και διασφαλίζονται τα δεδομένα επικοινωνίας των χρηστών και των χρηστών του παρόχου, το απόρρητο των επικοινωνιών, η προστασία των υπολογιστικών συστημάτων και των δικτυακών υποδομών και η προστασία των διαδικτυακών υπηρεσιών και εφαρμογών.

Η πολίτικη ασφάλειας που ακολουθεί ο πάροχος θα πρέπει να συμφωνεί με την γενική αρχή της ΑΔΑΕ, γι αυτό και θα υπόκειται σε έλεγχο από αυτήν τόσο ως προς την αποτελεσματικότητα της αλλά και ως προς τον βαθμό εφαρμογής της. Η φύση των επενδύσεων που γίνονται από τους παρόχους για την διατήρηση της ασφάλειας και της ακεραιότητας του δικτύου πρέπει να ακολουθεί την αρχή της αναλογικότητας, η οποία λαμβάνει υπόψη της το μέγεθος του παρόχου και των αριθμό των χρηστών παρόχου.

Σύμφωνα λοιπόν με την ΑΔΑΕ ο πάροχος υποχρεούται να τηρεί τα παρακάτω:

- Να διαθέτει και να τηρεί πολιτική πρόσβασης για τα συστήματα τα οποία αναφέρονται σε εξωτερικές συνδέσεις, επικοινωνίες δεδομένων, τηλεπικοινωνιακές συσκευές και λογισμικά προγράμματα. Καθώς και να λαμβάνει όλα τα απαραίτητα και πρόσφορα μέτρα για τη φυσική προστασία των εγκαταστάσεών του, για τον έλεγχο της φυσικής πρόσβασης, ώστε αυτή να επιτρέπεται μόνο σε εξουσιοδοτημένα πρόσωπα.
- Να ενημερώνουν τους χρήστες σχετικά με τα μέτρα προστασίας που μπορούν να λαμβάνουν για την διασφάλιση του απορρήτου των επικοινωνιών και των δεδομένων τους π.χ. την χρήση συγκεκριμένου λογισμικού ή τεχνολογιών κρυπτογράφησης.

- Να ενημερώνουν τους χρήστες για δεδομένα επικοινωνίας τα οποία πιθανόν να αποθηκεύονται σε αντίγραφα ασφαλείας αλλά και να του κοινοποιούν το μέγιστο χρονικό διάστημα για το οποίο τα δεδομένα θα είναι αποθηκευμένα.
- Να λαμβάνουν υπόψη και να εφαρμόζουν στο τμήμα της πολιτικής τους τις διατάξεις της νομοθεσίας για την επεξεργασία των δεδομένων επικοινωνίας.
- Να χρησιμοποιούν συστήματα ανίχνευσης επισυνδέσεων για την ενίσχυση προστασίας του δικτύου, 24 ώρες το 24ωρο. Η διακοπή των συστημάτων αυτών επιτρέπεται μόνο σε περιπτώσεις συντήρησης ή κάποιας βλάβης του συστήματος.
- Να διαθέτει απαραίτητο λογισμικό για την προστασία από Ιούς όλων των υπηρεσιών και εφαρμογών που προσφέρει στους χρήστες.
- Να αναπτύξει και να συντηρεί ένα σχέδιο εκτάκτου ανάγκης του συστήματος μετά από κακόβουλες επιθέσεις περιλαμβάνοντας την εκτέλεση αντίγραφων ασφαλείας, την παροχή διαδικασιών για συνέχιση της λειτουργίας σε περίπτωση ανάγκης και την ανάκτηση από μια επίθεση. Επιπλέον, να παραδίδει την πιο πρόσφατη πολιτική Αντιγράφων Ασφάλειας κάθε φορά που επιτελείται κάποια σημαντική αλλαγή σε αυτήν.
- Να διαθέτει σαφή Διαδικασία Χειρισμού Περιστατικών Ασφαλείας (ΔΧΠΑ) τα οποία απειλούν την ασφάλεια των επικοινωνιακών υποδομών αλλά και την διασφάλιση του απορρήτου των επικοινωνιών που διεξάγονται μέσω του παρόχου. Επιπλέον οφείλει να την ανανεώνει και να ελέγχει σε τακτικά διαστήματα την ετοιμότητα ενεργοποίησης όλων των μηχανισμών και προσώπων της ΔΠΧΑ καθώς επίσης και να την παραδίδει στην ΑΔΑΕ κάθε φορά για έλεγχο.
- Να διαθέτει ομάδα ελέγχου ασφάλειας του δικτύου του και κατά τους ελέγχους, να επιτρέπει την πρόσβαση στο δίκτυο ως το επίπεδο που κρίνεται αναγκαίο για την εκτέλεση τους καθώς και ομάδα αντιμετώπισης Ιών που θα μπορεί να παραπέμψει και ένα χρήστη που χρήζει βοήθειας, στην αρμόδια εταιρεία όταν της ζητηθεί.
- Να συγκροτεί ομάδα αποτίμησης κίνδυνου, που θα περιλαμβάνει τόσο τεχνικό προσωπικό (προγραμματιστές, τεχνικούς ασφάλειας κτλ) όσο και ανώτερα στελέχη, ώστε η αποτίμηση να είναι όσο το δυνατόν πιο ολοκληρωμένη.

3.4.4 Γενική αρχή δικαιωμάτων των χρηστών διαδικτυακών υπηρεσιών

Η γενική αρχή των δικαιωμάτων των χρηστών προσδιορίζει τις ειδικές απαιτήσεις σχετικά με τους συνδρομητές ή χρήστες των παρεχομένων διαδικτυακών υπηρεσιών με βάση τα δικαιώματα αυτών.

Πιο συγκεκριμένα προσδιορίζει τις απαιτήσεις των χρηστών από τον πάροχο διαδικτυακών υπηρεσιών, που είναι οι εξής:

Το πρόσωπο που ασχολείται με την παροχή διαδικτυακών υπηρεσιών ή και ηλεκτρονικών επικοινωνιών οφείλει να διατηρεί αρχείο που αναφέρει αναλυτικά τους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης που χρησιμοποιούνται για την πρόσβαση των συνδρομητών ή χρηστών του στις υπηρεσίες ή/και τα δίκτυα που παρέχει.

Το πρόσωπο που ασχολείται με την παροχή διαδικτυακών υπηρεσιών ή και ηλεκτρονικών επικοινωνιών οφείλει να διαμορφώσει και να ακολουθεί συγκεκριμένη διαδικασία διαχείρισης των λογαριασμών πρόσβασης των συνδρομητών ή χρηστών στις υπηρεσίες ή/και τα δίκτυα που παρέχει , στην οποία θα περιγράφεται με σαφήνεια ο τρόπος προσθήκης και κατάργησης λογαριασμών πρόσβασης, καθώς και η απόδοση του ονόματος χρήστη και του κωδικού πρόσβασης στους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών, στην περίπτωση που αυτά καθορίζονται αρχικά από αυτό.

Στην περίπτωση αυτή, το πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να δημιουργεί τους αρχικούς κωδικούς πρόσβασης με τρόπο που να αποτρέπει τον εύκολο προσδιορισμό τους.

Επιπρόσθετα, οφείλει να ενημερώνει με κάθε πρόσφορο μέσο τους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών σχετικά με την αναγκαιότητα αλλαγής του αρχικού κωδικού πρόσβασης, καθώς και σχετικά με ενδεδειγμένους κανόνες δημιουργίας ισχυρών κωδικών πρόσβασης.

Το πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να διαθέτει διαδικασία σύμφωνα με την οποία διενεργείται περιοδικός έλεγχος σχετικά με την αλλαγή του αρχικού κωδικού πρόσβασης από τους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών και εξασφαλίζει την εκ νέου ενημέρωσή τους σχετικά με την αναγκαιότητα αλλαγής των κωδικών πρόσβασης σε περίπτωση που δεν έχουν προβεί στην σχετική αλλαγή, σύμφωνα με την Πολιτική Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών.

Σε περίπτωση που το πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών προσφέρει τη δυνατότητα στους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών να αποκτήσουν πρόσβαση σε δεδομένα επικοινωνίας τους (ενδεικτικά, εξερχόμενες κλήσεις, ηλεκτρονικό ταχυδρομείο) μέσω συγκεκριμένης ιστοθέσης

(web account), οφείλει να χρησιμοποιεί τους ευρέως αποδεκτούς μηχανισμούς ασφαλούς αυθεντικοποίησης και κρυπτογράφησης και να περιγράφει αυτούς σε σχετικό αρχείο το οποίο οφείλει να διατηρεί.

Το πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να ενημερώνει τους συνδρομητές ή χρήστες των παρεχομένων δικτύων ή υπηρεσιών σχετικά με τους κανόνες ενδεδειγμένης συμπεριφοράς αναφορικά με την προστασία των κωδικών πρόσβασης που κατέχουν, με έντυπη ή ηλεκτρονική ενημέρωση, τουλάχιστον κατά την σύναψη της μεταξύ τους σύμβασης, καθώς και σε εύκολα προσβάσιμο σημείο του ισοτόπου του. Οι κανόνες αυτοί θα πρέπει να ακολουθούν τις ευρέως αποδεκτές και διεθνείς πρακτικές.

3.4.5 Πλαίσιο χρήσης μηχανισμών ασφαλείας στο διαδίκτυο

Μια ολοκληρωμένη υλοποίηση Διαδικτυακής επικοινωνίας θα πρέπει να περιλαμβάνει επαρκείς μεθόδους κρυπτογράφησης (encryption), χρησιμοποίηση επαλήθευσης ή προσδιορισμού ταυτότητας (authentication) από τους χρήστες, και ένα σχέδιο διαχείρισης που θα ενσωματώνει αποδοτικές μεθόδους κλειδιών και κωδικών πρόσβασης.

Υπάρχουν περιπτώσεις που οι κωδικοί πρόσβασης δεν αρκούν και χρειάζεται ένα είδος δυναμικής πιστοποίησης των δεδομένων. Αυτό επιτυγχάνεται με μια σειρά από διαφορετικές τεχνολογίες όπως οι γεννήτριες δυναμικών κωδικών, τεχνικές βασισμένες στην κρυπτογραφία, καθώς και ψηφιακές υπογραφές και πιστοποιητικά.

Επίσης, ο πάροχος διαδικτύου θα πρέπει να προστατεύει τους διακομιστές του δικτυού του και να παρέχει την δυνατότητα ανάκτησης των αρχείων του σε περίπτωση απώλειας αυτών. Οι διαχειριστές δικτύου θα πρέπει να παρέχουν μεθόδους εφεδρικών αντιγράφων όπως η πλήρη, η αυξητική και η διαφορική αντιγραφή αρχείων.

Άλλη μια μέθοδος είναι η Δικτυακή αντιγραφή αρχείων στην οποία κρυπτογραφημένα δεδομένα με αυτόματο και ασφαλή τρόπο αντιγράφονται και αποθηκεύονται σε μια περιοχή εκτός του εσωτερικού δικτυού του παρόχου του διαδικτύου.

Επιπλέον, απαραίτητη είναι η χρήση λογισμικού κατά των κακόβουλων επιθέσεων, αυτό γίνεται κυρίως με την χρήσης αναχωμάτων ασφάλειας (firewalls), για την προστασία από ιούς.

Επιπλέον, οι εξυπηρετητές (servers) των εφαρμογών ηλεκτρονικού ταχυδρομείου μπορεί να είναι αρχικοποιημένοι ώστε κάθε μήνυμα να υπογράφεται χρησιμοποιώντας την ψηφιακή υπογραφή του αποστολέα, να απαγορεύουν την αποστολή μηνυμάτων σε μη κατάλληλους προορισμούς και να ανιχνεύουν τα κατάλληλα προγράμματα για αποστολή / λήψη μηνυμάτων. Οι χρήστες θα πρέπει να συμμορφώνονται με τους κανόνες ασφαλείας που ορίζει ο πάροχος διαδικτύου είτε ενυπόγραφα είτε

ηλεκτρονικά, καθώς επίσης δεν θα πρέπει να δημοσιοποιούν υλικό σε ακατάλληλους ή παράνομους ηλεκτρονικούς τόπους.

Παρακάτω περιγράφονται εκτενέστερα οι μέθοδοι της κρυπτογράφησης, της αυθεντικοποίησης και οι μηχανισμοί προστασίας από ιούς.

Κρυπτογράφηση

Η κρυπτογραφία είναι μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Η κρυπτογράφηση στο διαδίκτυο έχει σκοπό την διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της μη αποποίησης ευθύνης στις συναλλαγές προστατεύοντας έτσι την ιδιωτικότητα του χρήστη. Για αυτό και οι πάροχοι οφείλουν να εφαρμόζουν αλγορίθμους και τεχνικές κρυπτογράφησης τόσο στα συστήματα και τις εφαρμογές τους όσο και στην μετάδοση των δεδομένων, ακολουθώντας διεθνή πρότυπα, καθώς υποχρεούνται να ενημερώνουν για τις τεχνικές τους την ΑΔΑΕ. Η ΑΔΑΕ από την μεριάς της οφείλει να εκδίδει τεχνικές οδηγίες και συστάσεις που θα καθορίζουν το μήκος του κλειδιού ανά πεδίο κρυπτογράφησης. Το επίπεδο της κρυπτογράφησης πρέπει να είναι τέτοιο ώστε η παραβίαση να μην είναι δυνατή σε λογικό χρόνο και με λογικούς υπολογιστικούς πόρους.

Αναγνώριση και ταυτοποίηση

Όλοι οι χρήστες του συστήματος (τεχνικό προσωπικό, διαχειριστές, προγραμματιστές, κοινοί χρήστες κλπ.), θα πρέπει να έχουν ένα μοναδικό αναγνωριστικό (user ID), για καθαρά προσωπική τους χρήση στο σύστημα. Με αυτόν τον τρόπο είναι δυνατός ο εντοπισμός του υπεύθυνου ατόμου για όλες τις δραστηριότητες που γίνονται στο πληροφοριακό σύστημα του οργανισμού. Επιπλέον, τα user IDs δεν πρέπει να φανερώνουν τα δικαιώματα του χρήστη στο σύστημα. Μια ομάδα μπορεί να μοιράζεται το ίδιο user ID για την εκτέλεση συγκεκριμένων εργασιών στο σύστημα, μόνο σε εξαιρετικές περιπτώσεις, και εφόσον κάτι τέτοιο είναι απαραίτητο για τον οργανισμό. Σε μια τέτοια περίπτωση θα πρέπει να υπάρχει ειδική έγκριση από τη διοίκηση του οργανισμού, όπως επίσης και να χρησιμοποιηθεί κάποιος μηχανισμός που θα καθορίζει τις ευθύνες των μελών της ομάδας.

Υπάρχουν διάφορες διαδικασίες αυθεντικοποίησης που μπορούν να χρησιμοποιηθούν για την επιβεβαίωση της ταυτότητας ενός χρήστη. Τα συνθηματικά είναι ο πλέον συνηθισμένος τρόπος, ο οποίος βασίζεται στη χρήση ενός μυστικού, γνωστού μόνο στο χρήστη. Άλλοι μηχανισμοί αυθεντικοποίησης περιλαμβάνουν συνδυασμούς κρυπτογραφίας και πρωτοκόλλων εξακρίβωσης της ταυτότητας του χρήστη.

Διάφορα αντικείμενα, όπως έξυπνες κάρτες, τα οποία έχει στην κατοχή του ο χρήστης, μπορούν επίσης να χρησιμοποιηθούν για αυθεντικοποίηση στο σύστημα. Ένας άλλος τρόπος εξακρίβωσης της ταυτότητας, περιλαμβάνει την εξέταση διάφορων βιομετρικών χαρακτηριστικών του χρήστη, όπως είναι τα δακτυλικά αποτυπώματα. Ο συνδυασμός πολλαπλών τεχνολογιών εξακρίβωσης της ταυτότητας, έχει ως αποτέλεσμα ισχυρότερη αυθεντικοποίηση.

Προστασία από ιούς

Ο πάροχος θα πρέπει να διαθέτει κατάλληλο λογισμικό για την προστασία από ιούς για όλες τις υπηρεσίες και εφαρμογές που προσφέρει στους χρήστες . Για παράδειγμα υπηρεσία e-mail απαιτεί χρήση e-mail scanner. Θα πρέπει επίσης να εγκαθιστά μονίμως μνήμη (memory resident) των υπολογιστικών συστημάτων λογισμικό προστασίας από ιούς το οποίο θα εξετάζει αυτομάτως όλα τα εισερχόμενα μηνύματα. Επίσης, και οι χρήστες από την άλλη θα πρέπει να προστατεύονται ομοίως και θα πρέπει να ελέγχονται αλλά και να ενημερώνονται από τον πάροχο σχετικά με το πως μπορούν να προστατευθούν επιπλέον. Θα πρέπει να υλοποιηθούν οι κατάλληλοι μηχανισμοί για την αποτροπή και τον εντοπισμό κακόβουλου λογισμικού. Η προστασία απέναντι στο κακόβουλο λογισμικό θα πρέπει να βασίζεται στην ενημέρωση του προσωπικού για την ασφάλεια του οργανισμού, τα κατάλληλα δικαιώματα προσπέλασης και τους μηχανισμούς διαχείρισης αλλαγών στο σύστημα.

Οι παρακάτω μηχανισμοί ελέγχου έχουν ιδιαίτερη σημασία για την προστασία αρχείων που εξυπηρετούν μεγάλο αριθμό σταθμών εργασίας.

- Μια επίσημη πολιτική που να επιβάλει την ύπαρξη των κατάλληλων αδειών χρήσης λογισμικού και να απαγορεύει τη χρήση μη εξουσιοδοτημένου λογισμικού
- Μια επίσημη πολιτική που να προστατεύει το πληροφοριακό σύστημα από λογισμικό και αρχεία που μπορούν να εισέλθουν στο σύστημα από κάποιο εξωτερικό δίκτυο ή μέσο αποθήκευσης.
- Εγκατάσταση και τακτική ενημέρωση προγραμμάτων antivirus για τον έλεγχο προσωπικών υπολογιστών και αποθηκευτικών μέσων.
- Τακτικός έλεγχος του χρησιμοποιούμενου λογισμικού και των αρχείων του συστήματος. Οποιαδήποτε αλλαγή θα πρέπει να ερευνάται.
- Ο έλεγχος αρχείων και αποθηκευτικών μέσων για ιούς πριν από τη χρήση τους.
- Ο έλεγχος των εισερχόμενων ηλεκτρονικών μηνυμάτων για ιούς. Ο συγκεκριμένος έλεγχος μπορεί να γίνει σε διάφορα σημεία του συστήματος, όπως τους εξυπηρετητές ηλεκτρονικού ταχυδρομείου, τους προσωπικούς υπολογιστές κλπ.
- Την εκπαίδευση των χρηστών και ύπαρξη διαδικασιών για την αντιμετώπιση ιών.

- Την ύπαρξη σχεδίου επιχειρησιακής συνέχειας στην περίπτωση εκτεταμένων ζημιών στο σύστημα από ιούς.
- Την ύπαρξη διαδικασιών για τον έλεγχο της ακρίβειας της πληροφόρησης για ιούς.

3.5 Πολιτική ασφαλείας ιατρικών δεδομένων στο διαδίκτυο

Θεσμικό Πλαίσιο Προστασίας Ιατρικών Δεδομένων

Τα δεδομένα που αφορούν την υγεία του ατόμου αποτελούν μέρος της προσωπικότητας του και είναι απαραίτητη η συγκατάθεση του ασθενή για κάθε ανάκτηση, καταγραφή, επεξεργασία ή μεταφορά τους. Η πρόσβαση και η επεξεργασία των δεδομένων πρέπει να συμφωνεί με τις σχετικές διατάξεις για την προστασία των προσωπικών δεδομένων και το ιατρικό απόρρητο . Όσον αφορά το νομικό πλαίσιο τα ευαίσθητα δεδομένα προστατεύονται και από την Αρχή Προστασίας Προσωπικών Δεδομένων.

Οι ασθενείς έχουν δικαιώματα για την προστασία των προσωπικών δεδομένων τους και την εμπιστευτικότητα της μεταφοράς δεδομένων που σχετίζονται με τη διαχείριση της περίθαλψής τους. Κάθε είδους εξ' αποστάσεως παροχή περίθαλψης σε ασθενείς πρέπει να γίνεται σε κατάλληλο περιβάλλον που εγγυάται την απουσία ατόμων που δεν σχετίζονται με αυτή.

Οι προβλέψεις της νομοθεσίας για την προστασία των ευαίσθητων προσωπικών δεδομένων των ασθενών περιγράφονται συνοπτικά παρακάτω :

1. Η επεξεργασία των ιατρικών δεδομένων επιτρέπεται μόνο όταν συντρέχει μία από τις επόμενες περιπτώσεις:
   - Ο ασθενής έχει δώσει ρητά τη συγκατάθεσή του.
   - Η επεξεργασία είναι απαραίτητη για τη διασφάλιση ζωτικού συμφέροντος του ασθενούς ενώ ο ίδιος τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.
   - Η επεξεργασία είναι αναγκαία για την ιατρική πρόληψη ή διάγνωση, την παροχή ιατροφαρμακευτικής αγωγής ή τη διαχείριση των ιατροφαρμακευτικών υπηρεσιών, η δε επεξεργασία εκτελείται από κατ' επάγγελμα θεράποντα της υγείας που δεσμεύεται από το ιατρικό απόρρητο ή από άλλο πρόσωπο το οποίο υπέχει ανάλογη υποχρέωση.

2. Οι βασικές αρχές της νόμιμης και θεμιτής επεξεργασίας που πρέπει απαραίτητα να τηρούνται, σε συνδυασμό με τα παραπάνω είναι:

- Ο σκοπός και η διάρκεια της επεξεργασίας πρέπει να ορίζεται με σαφήνεια εκ των προτέρων και δεν επιτρέπεται να τροποποιείται αργότερα. Τα δεδομένα πρέπει να είναι απαραίτητα και να μην υπερβαίνουν το σκοπό της επεξεργασίας. Η λεγόμενη αρχή του σκοπού σημαίνει ότι πρέπει να συλλέγονται όσο το δυνατόν λιγότερα προσωπικά δεδομένα για το σκοπό της επεξεργασίας και όπου είναι δυνατό να χρησιμοποιούνται ανώνυμα δεδομένα ή ψευδώνυμα. Τα δεδομένα πρέπει επίσης να είναι ακριβή και εφόσον χρειάζεται να ενημερώνεται η ακρίβειά τους.
- Ο υπεύθυνος επεξεργασίας πρέπει να λαμβάνει όλα τα απαραίτητα τεχνικά και οργανωτικά μέτρα προστασίας των δεδομένων από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση, ιδίως εάν η επεξεργασία συμπεριλαμβάνει και διαβίβαση των δεδομένων μέσω δικτύου. Ο βαθμός ασφάλειας κρίνεται από τις εξής συνιστώσες: τη φύση των δεδομένων, την επικινδυνότητα της επεξεργασίας, την τεχνολογική εξέλιξη και το κόστος εφαρμογής των μέτρων ασφάλειας. Έτσι η διακίνηση ευαίσθητων δεδομένων μέσω δικτύου απαιτεί αυστηρά μέτρα ενώ το κόστος αποκτά δευτερεύουσα σημασία όσο αυξάνει η επικινδυνότητα της επεξεργασίας.
- Επίσης, ο υπεύθυνος της επεξεργασίας πρέπει να γνωστοποιήσει την επεξεργασία στην αρμόδια Αρχή Προστασίας. Σημειώνουμε ότι σε ειδικές κατηγορίες επεξεργασίας που ενέχουν ιδιαίτερους κινδύνους η αρμόδια Αρχή μπορεί να προβεί σε προληπτικό έλεγχο της επεξεργασίας.
- Ο υπεύθυνος επεξεργασίας πρέπει να σέβεται και να εξασφαλίσει την άσκηση των δικαιωμάτων του υποκειμένου της επεξεργασίας (ασθενούς).

3. Τηρούνται τα νόμιμα δικαιώματα του ασθενούς:

- Ο υπεύθυνος επεξεργασίας πρέπει να ενημερώσει τον ασθενή για το σκοπό της επεξεργασίας, τα δεδομένα που είναι απαραίτητα για το σκοπό αυτό και τους αποδέκτες της επεξεργασίας, το κατά πόσο η επεξεργασία είναι υποχρεωτική, και για την ύπαρξη δικαιώματος πρόσβασης στα δεδομένα του.
- Ο ασθενής έχει το δικαίωμα ανά πάσα στιγμή να ζητήσει να πληροφορηθεί ποια προσωπικά του δεδομένα και για ποιο σκοπό έχουν γίνει αντικείμενο επεξεργασίας.
- Ο ασθενής έχει το δικαίωμα της διόρθωσης και διαγραφής των δεδομένων εάν αυτά δεν είναι ακριβή ή η επεξεργασία δεν είναι νόμιμη.
- Ο ασθενής έχει το δικαίωμα ν’ αντιταχθεί στην επεξεργασία.

3.5.1 Ιατρικό Απόρρητο

Σύμφωνα με το ιατρικό απόρρητο κάθε παραβίαση του απορρήτου από τον ιατρό ή τους βοηθούς του, δηλαδή εάν φανερώσει πληροφορίες σε σχέση με τον ασθενή, αποτελεί αδίκημα. Δεν αποτελεί αδίκημα η πράξη εάν ο ιατρός φανερώσει πληροφορίες στο πλαίσιο της εκπλήρωσης καθήκοντος ή της διαφύλαξης έννομου ή για άλλο λόγο δικαιολογημένου, ουσιώδους συμφέροντος του ίδιου ή κάποιου άλλου, το οποίο δεν μπορούσε να διαφυλαχθεί διαφορετικά. Το ιατρικό απόρρητο ως υποχρέωση του ιατρού που παρέχει τις υπηρεσίες του ιδιωτικά ή μέσω οργανισμών δημοσίου ή ιδιωτικού δικαίου κατοχυρώνεται επίσης στον Κανονισμό Ιατρικής Δεοντολογίας.

Συνεπώς, σε εφαρμογές ιατρικής πληροφορικής οι διατάξεις για το ιατρικό απόρρητο και την προστασία των προσωπικών δεδομένων εφαρμόζονται σωρευτικά.

3.5.2 Ασφάλεια των ιατρικών δεδομένων

Η χρήση Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) στον τομέα της υγείας πρέπει να εξασφαλίζει την:

- Πιστοποίηση (authentication): έλεγχος της αυθεντικότητας της ταυτότητας των μερών μιας ανταλλαγής δεδομένων.
- Εξουσιοδότηση (authorisation): η πρόσβαση του χρήστη πρέπει να είναι εξουσιοδοτημένη.
- Εμπιστευτικότητα (confidentiality): η τήρηση του απορρήτου των δεδομένων.
- Ακεραιότητα (integrity): τα δεδομένα θα πρέπει να παραμείνουν ακέραια, δηλαδή να μην υποστούν αλλοίωση.
- Μη δυνατότητα άρνησης συμμετοχής (non-repudiation): ο χρήστης δεν πρέπει να μπορεί να αρνηθεί τη συμμετοχή του στην ανταλλαγή των δεδομένων.
- Δυνατότητα ελέγχου (revision / audit): κάθε τροποποίηση ή επεξεργασία των δεδομένων πρέπει να μπορεί να ελεγχθεί, δηλαδή από ποιόν έγινε και πότε.
- Ευθύνη (accountability): πρέπει να προκύπτει ποιος είναι υπεύθυνος για την εισαγωγή, πρόσβαση ή τροποποίηση κάθε δεδομένου.
- Διαφάνεια (transparency): πρέπει να γίνεται τεκμηρίωση των διαδικασιών της επεξεργασίας ώστε να μπορούν να ελεγχθούν.
- Διαθεσιμότητα (availability): τα δεδομένα πρέπει να είναι διαθέσιμα όταν χρειάζεται.

3.6 Πλαίσιο Ορισμού σχεδίου Ασφαλείας

3.6.1 Απαιτήσεις Ασφαλείας

Οι θεμελιώδης αρχές χρήσης και λειτουργίας των πληροφοριακών συστημάτων θα πρέπει να ικανοποιούν τις ακόλουθες απαιτήσεις ασφάλειας:

Οι πληροφορίες που συσχετίζονται με προσωπικά δεδομένα θα πρέπει να διαχειρίζονται από το συνολικό σύστημα με σκοπό τη βελτίωση των παρεχομένων υπηρεσιών προς τους πολίτες.

Η διαχείριση των πληροφοριών θα πρέπει να γίνεται αποκλειστικά από κατάλληλο εξουσιοδοτημένο προσωπικό .

Τα δικαιώματα πρόσβασης στο σύστημα θα πρέπει να έχουν προσδιοριστεί με διαδικασίες ανεξάρτητες της φάσης υλοποίησης του πληροφοριακού συστήματος. Ο καθορισμός των διαδικασιών αυτών γίνεται σε επίπεδο νομοθετικό (νόμοι, διατάγματα), οργανωτικό (κανόνες λειτουργίας οργανισμού, καθηκοντολόγιο) και δομικό (κατάλληλη στελέχωση, υπεύθυνη επιτροπή ασφάλειας).

Η παροχή εμπιστευτικών πληροφοριών προς τρίτους θα επιτρέπεται κατόπιν έγγραφης άδειας του άμεσα ενδιαφερόμενου.

Οι μηχανισμοί ασφάλειας, δε θα πρέπει να μειώνουν τη συνολική αποτελεσματικότητα του συστήματος. Στη περίπτωση που δεν είναι δυνατή η εφαρμογή του προηγούμενου αξιώματος, θα πρέπει να υπάρχει ικανοποιητική ισορροπία μεταξύ απόδοσης και ασφάλειας του συστήματος.

Η σωστή ανάπτυξη και η αποδοτική λειτουργία πληροφοριακών συστημάτων είναι μια διαδικασία, που εμπεριέχει αναπόσπαστα τη ταυτόχρονη δόμηση ενός πλαισίου ασφάλειας, το οποίο να εξασφαλίζει τις απαιτήσεις ορθότητας, διαθεσιμότητας και μυστικότητας των περιεχομένων πληροφοριών.

3.6.2 Απειλές Ασφάλειας - Μέθοδοι Ασφάλειας

Στην ασφάλεια, μια αποκάλυψη αποτελεί απειλή καθώς είναι ένας τρόπος για πιθανή απώλεια ή βλάβη του Πληροφοριακού Συστήματος. Παραδείγματα αποκαλύψεων είναι η μη εξουσιοδοτημένη αποκάλυψη των δεδομένων, τροποποίηση των δεδομένων ή άρνηση του νόμιμου δικαιώματος πρόσβασης στο σύστημα. Η ευπάθεια είναι η αχίλλειος πτέρνα στο σύστημα ασφάλειας που μπορεί να εκμεταλλευτεί από τρίτους για την πρόκληση απωλειών ή ζημίας.

Ένα πρόσωπο που εκμεταλλεύεται την ευπάθεια του συστήματος διαπράττει μια επίθεση στο σύστημα. Ο συνεχής έλεγχος είναι ένα προστατευτικό μέτρο, που μπορεί να είναι είτε μια ενέργεια ή μια συσκευή ή ακόμα και μια διαδικασία ή τεχνική μέθοδος, και που μειώνει την ευπάθεια του συστήματος.

Τα μεγαλύτερα αντικείμενα του Πληροφοριακού Συστήματος είναι το υλικό, το λογισμικό και τα δεδομένα. Υπάρχουν τέσσερα είδη απειλής στην ασφάλεια του Π.Σ. που είναι:

• **Διακοπή (interruption).**

Τα αντικείμενα του συστήματος χάνονται, δεν είναι διαθέσιμα ή είναι μη χρησιμοποιήσιμα. Παραδείγματα είναι η ηθελημένη καταστροφή μιας συσκευής, το σβήσιμο ενός προγράμματος ή ενός αρχείου δεδομένων, ή η δυσλειτουργία του διαχειριστή αρχείων του λειτουργικού συστήματος, έτσι ώστε να μην μπορεί να βρεθεί ένα συγκεκριμένο αρχείο στο δίσκο.

• **Παρεμπόδιση (interception).**

Σημαίνει πως μια μη εξουσιοδοτημένη ομάδα έχει κερδίσει το δικαίωμα πρόσβασης σε ένα αντικείμενο. Αυτή η εξωτερική ομάδα μπορεί να είναι είτε πρόσωπα, είτε προγράμματα ή ακόμα και παρέμβαση ενός άλλου πληροφοριακού συστήματος. Παραδείγματα αυτού του είδους της αποτυχίας είναι η παράνομη αντιγραφή των προγραμμάτων ή των αρχείων δεδομένων ή οι υποκλοπές των τηλεφωνημάτων για την απόκτηση δεδομένων από το δίκτυο. Παρόλο που μια απώλεια μπορεί να αποκαλυφθεί σχετικά γρήγορα, ο υποκλοπέας μπορεί να μην αφήσει καθόλου ίχνη για την ανίχνευση της ύπαρξης του.

• **Τροποποίηση (modification).**

Εάν μια μη εξουσιοδοτημένη ομάδα όχι μόνο προσπελάσει τα δεδομένα, αλλά ανακατευτεί και με κάποια αντικείμενα, τότε μιλάμε για τροποποίηση. Για παράδειγμα κάποιος μπορεί να αλλάξει τις τιμές σε μια βάση δεδομένων ή να μετατρέψει ένα πρόγραμμα έτσι ώστε να εκτελεί επιπλέον υπολογισμούς ή να τροποποιεί τα δεδομένα που μεταφέρονται ηλεκτρονικά. Είναι ακόμα δυνατό να τροποποιηθεί και το υλικό μέρος του συστήματος.

• **Πλαστοποίηση (fabricate).**

Τέλος μια μη εξουσιοδοτημένη ομάδα μπορεί να κατασκευάσει πλαστά αντικείμενα σε ένα Π.Σ. Ο εισβολέας μπορεί να προσθέσει εγγραφές σε μια υπάρχουσα βάση δεδομένων. Μερικές φορές αυτές οι προσθέσεις ανιχνεύονται σαν πλαστές, αλλά εάν έχουν γίνει περίτεχνα τότε είναι αδιαχώριστες από τα πραγματικά αντικείμενα.

Κατά καιρούς έχουν προταθεί διάφοροι τρόποι ασφάλειας ενός πληροφοριακού συστήματος. Οι τρόποι αυτοί χρησιμοποιούνται στην συνέχεια ως βάση για την δημιουργία των μηχανισμών και των μέτρων προστασίας, των οποίων ο συνδυασμός θα μας δώσει το μοντέλο ασφαλείας.

3.6.3 Πολιτική Αντιγράφων Ασφαλείας

Η δημιουργία αντιγράφων ασφαλείας των αρχείων στοχεύει στην προστασία τους από τη μόνιμη απώλεια ή αλλαγή τους σε περίπτωση ακούσιας διαγραφής, επίθεσης από ιό ή σε περίπτωση

αστοχίας του λογισμικού ή του υλικού. Εάν συμβεί κάτι από τα παραπάνω η εταιρεία έχοντας αντίγραφα ασφαλείας, θα είναι σε θέση να κάνει επαναφορά των δεδομένων της. Τα αντίγραφα εξυπηρετούν σε πολύ μεγάλο βαθμό την ασφάλεια των δεδομένων και των συστημάτων της εταιρείας, καθώς πολλά από τα δεδομένα αυτά είναι ιδιαίτερα ευαίσθητα και είναι πολύ σημαντική η προστασία του απορρήτου τους.

Η πολιτική αντιγράφων ασφαλείας περιλαμβάνει τις διαδικασίες και τους ελέγχους που εξασφαλίζουν ότι ο τηλεπικοινωνιακός εξοπλισμός μπορεί να ανακτήσει τη λειτουργία εντός μια λογικής χρονικής περιόδου μετά από οποιαδήποτε ζημιά από κακόβουλες επιθέσεις. Στόχος της πολιτικής αυτής είναι να καθορίζει τους κανόνες και τις διαδικασίες αντιγράφων ασφαλείας και ανάκτησης δεδομένων.

Πιο συγκεκριμένα η πολιτική αντιγράφων ασφαλείας καθορίζει και περιλαμβάνει τα εξής:

- Μια διαδικασία ανάλυσης της ευαισθησίας, των ευπαθειών και της ασφάλειας των προγραμμάτων και των πληροφοριών που λαμβάνουν, χειρίζονται, αποθηκεύουν ή μεταδίδουν, ώστε να προσδιοριστεί ο λόγος για τον οποίον θα πρέπει να αποθηκεύονται τα δεδομένα.
- Ένα σχέδιο ανάκτησης δεδομένων που θα ενημερώνεται σε τακτά χρονικά διαστήματα για να δημιουργήσει και να διατηρήσει, για καθορισμένη χρονική περίοδο ακριβή αντίγραφα των πληροφοριών.
- Ένα σχέδιο αποκατάστασης έτσι ώστε να επιτρέπει τον πάροχο την επαναφορά των στοιχείων που ζημιώθηκαν σε κάποια περίπτωση κακόβουλης επίθεσης ή κάποιας διακοπής της λειτουργίας του συστήματος.
- Ένα σχέδιο λειτουργίας τρόπου έκτακτης ανάγκης το οποίο θα επιτρέπει την άμεση λειτουργία σε περίπτωση αποτυχίας του συστήματος.

Διαδικασίες αναθεώρησης και δοκιμών των σχεδίων έκτακτης ανάγκης με στόχο την κάλυψη αδυναμιών.

- Διαδικασία ελέγχου των εφεδρικών αντιγράφων καθώς και διαδικασία προσδιορισμού του τρόπου δημιουργίας τους.
- Τα αντίγραφα θα πρέπει να έχουν ίδιο επίπεδο ασφαλείας με τα αρχικά στοιχειά και θα πρέπει να διατηρούνται σε διαφορετικό χώρο/φυσική τοποθεσία από τα αρχικά δεδομένα.

3.6.4 Πολιτική διαχείρισης και εγκατάστασης Τηλεπικοινωνιακής Υποδομής – Κίνδυνοι Δικτύου

Με στόχο την ελαχιστοποίηση των κινδύνων προσβολής του κατανεμημένου συστήματος, μέσω της δικτυακής υποδομής θα πρέπει να εφαρμοστεί μία συνεπής πολιτική ασφάλειας. Το πλαίσιο της πολιτικής αυτής διαφοροποιείται ανάλογα με την έκταση και τη λειτουργία του συστήματος. Σε περιπτώσεις εκτεταμένων συστημάτων (π.χ. δημόσια δίκτυα), όπου οι χρήστες καλύπτουν ιδιωτικές - προσωπικές ανάγκες είναι υπό αμφισβήτηση η έκταση και η φύση του διαχειριστικού ελέγχου.

Προκύπτει δηλαδή το ερώτημα, αν είναι θεμιτή η παρακολούθηση των εργασιών ενός χρήστη από το διαχειριστή του δικτύου ή αν το γεγονός αυτό θεωρείται παραβίαση της ιδιωτικής του δραστηριότητας. Για να αποφύγουμε πιθανά παρόμοια προβλήματα περιορίζουμε την έκταση των συστημάτων, που εξετάζουμε, σε αυτά που καλύπτουν τις πληροφοριακές ανάγκες μίας μεγάλης επιχείρησης- οργανισμού.

Οι χρήστες των συστημάτων αυτών δεσμεύονται με κάποια σύμβαση, στην οποία θα πρέπει να καταγράφονται οι πληροφοριακές απαιτήσεις και το επιτρεπτό επίπεδο πρόσβασης για την εκτέλεση της καθημερινής εργασίας τους.

Τα συστήματα αυτά υποστηρίζονται επικοινωνιακά από τοπικά, μητροπολιτικά και δημόσια δίκτυα περιορισμένης όμως πρόσβασης.

Η πολιτική ασφάλειας, που θα πρέπει να εφαρμόζεται στις περιπτώσεις αυτές θα πρέπει να περιέχει τις ακόλουθες βασικές οδηγίες :

Η πρόσβαση στις επικοινωνιακές υπηρεσίες περιορίζεται σε συγκεκριμένες οντότητες (χρήστες, διαδικασίες, διεργασίες) και για καθορισμένο χρονικό διάστημα. Κάθε λειτουργία, που έχει τη δυνατότητα να εκτελεστεί τοπικά, δε θα επιτρέπεται να χρησιμοποιεί απομακρυσμένους πόρους.

- Οι διαθέσιμες διαδικασίες ταυτοποίησης και εξακρίβωσης γνησιότητας θα πρέπει να ελέγχουν όλες τις οντότητες, που χρησιμοποιούν την επικοινωνιακή υποδομή. Για την εξακρίβωση της ορθότητας των μηνυμάτων είναι χρήσιμη η μέθοδος των ψηφιακών υπογραφών. Ειδικά κατά τη διάρκεια πρόσβασης σε κρίσιμους πόρους του συστήματος (π.χ. εξυπηρετητές), θα πρέπει οι διαδικασίες ταυτοποίησης και εξακρίβωσης γνησιότητας να είναι διπλές.
- Κάθε πρόσβαση στο δίκτυο θα πρέπει να καταγράφεται (ημερομηνία, ώρα, κόμβος, χρήστης, εφαρμογή, διάρκεια, αρχεία και συσκευές πρόσβασης). Η λειτουργία κατάλληλων εφαρμογών παρακολούθησης και καταγραφής των επικοινωνιακών δραστηριοτήτων και του προκαλούμενου φόρτου είναι αναγκαία, καθώς και η επισήμανση καταστάσεων συναγερμού σε πραγματικό χρόνο.

- Τα συνθηματικά των χρηστών των επικοινωνιακών υπηρεσιών θα πρέπει να αλλάζουν σε τακτικά χρονικά διαστήματα.
- Βελτιστοποιημένες μέθοδοι κρυπτογράφησης θα πρέπει να χρησιμοποιούνται για την αποφυγή διαρροής πληροφοριών. Θα πρέπει να τονιστεί ότι στην περίπτωση που δεν εφαρμόζονται κρυπτογραφικές μέθοδοι σε όλα τα μηνύματα, θα πρέπει να εφαρμόζονται τουλάχιστο στα μηνύματα, που μεταφέρουν ταυτότητες και συνθηματικά. Είναι γνωστό ότι η πλειοψηφία των εφαρμογών υπηρεσιών δικτύου (rlogin, ftp, κλπ) μεταφέρουν αυτούσια τις ταυτότητες - συνθηματικά μέσω δικτύου σε μορφή κειμένου. Το ίδιο ισχύει και στις εφαρμογές πρόσβασης βάσεων δεδομένων, που λειτουργούν σύμφωνα με το μοντέλο πελάτη-εξυπηρετητή, καθώς και στις κατανεμημένες βάσεις δεδομένων.
- Κάθε χρήστης, συνεπώς, που έχει δυνατότητα πρόσβασης στις εφαρμογές παρακολούθησης του δικτύου ή έχει γνώσεις προγραμματισμού κατανεμημένων εφαρμογών (RPC), είναι δυνατό να υποκλέψει σταδιακά τα μεταφερόμενα συνθηματικά.
- Στις περιπτώσεις συνεχών αποτυχημένων προσπαθειών πρόσβασης θα πρέπει να απενεργοποιείται η μέθοδος πρόσβασης (πχ getty-login στο Unix) και να ειδοποιείται ο διαχειριστής του συστήματος, κρατώντας παράλληλα την ταυτότητα με την οποία επιχειρήθηκε η πρόσβαση. Σαν εναλλακτική τακτική προτείνεται η εισαγωγή του εισβολέα σε φαινομενικό περιβάλλον-κέλυφος (μετά από συνεχή εισαγωγή λανθασμένων συνθηματικών) με παράλληλη ενεργοποίηση διαδικασιών συναγερμού του διαχειριστή. Με τη μέθοδο αυτή είναι δυνατός ο φυσικός εντοπισμός του εισβολέα.
- Παράλληλα με τα μέτρα ασφάλειας του συστήματος από τους χρήστες, θα πρέπει να διασφαλίζονται και οι χρήστες έναντι του συστήματος. Συγκεκριμένα, όπως οι χρήστες ταυτοποιούνται στο σύστημα, με τον ίδιο τρόπο το σύστημα θα πρέπει να ταυτοποιείται στον χρήστη. Συνηθισμένη πρακτική των εισβολέων είναι η δημιουργία προγραμμάτων ταυτοποίησης παρόμοια με αυτά των λειτουργικών- δικτυακών συστημάτων με στόχο την υφαρπαγή των συνθηματικών, κατά τη διαδικασία καταχώρησης τους από τους τελικούς χρήστες.
- Θα πρέπει να μελετηθεί στατιστικά η κυκλοφορία που εισάγει στο δίκτυο κάθε χρήστης. Με τον τρόπο αυτό θα είναι δυνατός ο εντοπισμός του υπερβολικού κυκλοφοριακού φόρτου, τον οποίο προκαλούν οι εισβολείς, με τελικό σκοπό τη δημιουργία καθυστερήσεων και την πιθανή πλήρη κατάρρευση του δικτύου.
- Θα πρέπει να υπάρχουν διπλές διαδικασίες επιβεβαίωσης (από δύο τουλάχιστον διαχειριστές), για κάθε ζωτική αλλαγή της σύνθεσης (νέος κόμβος, νέοι χρήστες, διαδικασίες συντήρησης), καθώς και για τις διαδικασίες παρακολούθησης (monitoring) του συστήματος.

Σε κάθε εγκατάσταση νέου κόμβου, νέου λογισμικού θα πρέπει να αλλάζουν τα συνθηματικά που δίδονται από τις κατασκευάστριες εταιρίες, τα οποία συνήθως καλύπτουν βασικές λειτουργίες των συστατικών αυτών του κατανεμημένου συστήματος (εγκατάσταση, συντήρηση).

- Σταθμοί εργασίας χωρίς δισκέτες ή σκληρούς δίσκους θα πρέπει να χρησιμοποιούνται όπου είναι δυνατόν. Με τη μέθοδο αυτή θα αποφεύγεται η εισαγωγή προγραμμάτων ιών και η ανεπιθύμητη αντιγραφή μηνυμάτων-πληροφοριών. Οι διαδικασίες εκκίνησης των συστημάτων (boot) αυτών θα ενεργοποιούνται από μνήμες EPROM ή από απομακρυσμένους κόμβους (remote boot).
- Όλα τα ενεργά συστατικά του δικτύου (κόμβοι, εξυπηρετητές, συσκευές διαδικτύωσης, συγκεντρωτές, επαναλήπτες), θα πρέπει να είναι φυσικά προστατευμένα. Σε εκτεταμένες εγκαταστάσεις είναι αναγκαία η προστασία των συσκευών, οι οποίες δεν ελέγχονται από απομακρυσμένους κόμβους.

Τέτοιες συσκευές είναι οι παθητικοί επαναλήπτες χωρίς υποστήριξη SNMP πρωτοκόλλου, καθώς και οι εξυπηρετητές 'κουτών' τερματικών (terminal servers). Οι καλωδιώσεις πρέπει να διασχίζουν χώρους μη προσβάσιμους από το κοινό και να ευρίσκονται σε μεταλλικές σωληνώσεις. Τα κιβώτια διακλαδώσεων θα πρέπει να προστατεύονται από κλειδαριές. Η χρήση οπτικών ινών συστήνεται λόγω δυσκολίας στη διακλάδωσή τους, καθώς επίσης και η ύπαρξη εναλλακτικών καλωδιώσεων - διαδρομών με αυτόματη ενεργοποίηση των εφεδρικών φυσικών διαδρομών. Επίσης, συνίσταται να αποφεύγεται η χρήση δημοσίων δικτύων. Αν αυτό δεν είναι δυνατόν θα πρέπει να χρησιμοποιούνται αποκλειστικές γραμμές και να δεσμεύεται ο τηλεπικοινωνιακός οργανισμός, με κατάλληλη σύμβαση, σχετικά με πιθανή εισβολή με δική του υπαιτιότητα. Οι οδηγίες, που αναφέραμε, αφορούν την προστασία της δικτυακής υποδομής από πιθανές εισβολές. Για την πλήρη διαθεσιμότητα και σωστή λειτουργία του συστήματος θα πρέπει να ληφθούν επιπρόσθετα μέτρα.

Καταλογισμός ευθύνης, όπου ένας εξουσιοδοτημένος χρήστης μπορεί να απαρνηθεί την ευθύνη αποστολής ή παραλαβής ενός συγκεκριμένου μηνύματος ή ακόμη να κατασκευάσει ένα μη έγκυρο μήνυμα.

- Άρνηση εξυπηρέτησης κατά την οποία το δίκτυο δεν ανταποκρίνεται στο απαιτούμενο επίπεδο εξυπηρέτησης ή και λειτουργικότητας.
- Επανάληψη, όπου ένας εξουσιοδοτημένος χρήστης προβαίνει στην επανάληψη ενός μηνύματος με στόχο να θεωρηθεί από τον αποδέκτη του ως πρωτότυπο.
- Ανάλυση επικοινωνίας κατά την οποία παρακολουθείται η μετάδοση των μηνυμάτων στο δίκτυο για τον εντοπισμό κυρίως της προέλευσή τους ή και της αποστολής τους.

- Ιοί. Ένα σημαντικό πρόβλημα των υπολογιστικών συστημάτων είναι το λογισμικό που σχεδιάζεται για να προκαλέσει προβλήματα στην ομαλή λειτουργία του συστήματος. Ο τρόπος λειτουργίας τους είναι η επαναλαμβανόμενη αντιγραφή τους σε σημεία που ήδη βρίσκονται καταχωρημένα άλλα δεδομένα.

Οι προσπάθειες εισόδου στη δικτυακή δομή ανάλογα με τον στόχο τους μπορούν να διακριθούν σε δύο κατηγορίες εισβολών, τις παθητικές και τις ενεργητικές.

Στις παθητικές εισβολές, ο εισβολέας παρατηρεί τα μηνύματα, που διέρχονται στο φυσικό μέσον, χωρίς να παρεμβαίνει στη φύση και τη ροή τους. Αυτού του είδους εισβολές διακρίνονται σε δυο υποκατηγορίες παθητικής εισβολής.

- Παρατήρηση του περιεχομένου των μηνυμάτων, κατά την οποία ο εισβολέας υποκλέπτει μέρος ή τον σύνολο των διακινουμένων πληροφοριών.
- Ανάλυση της κυκλοφορίας, κατά την οποία ο εισβολέας καταγράφει και αναλύει τα διερχόμενα μηνύματα με σκοπό τη συγκέντρωση άμεσων ή επαγωγικών πληροφοριών. Οι πληροφορίες αυτές αφορούν τη δομή του συστήματος, τα χρησιμοποιούμενα πρωτόκολλα, την ονοματολογία, τους ενεργούς χρήστες, τους ενεργούς κόμβους, τις εκτελούμενες εφαρμογές και τις υπηρεσίες του συστήματος.

Στις ενεργητικές εισβολές ο εισβολέας επεξεργάζεται τα διερχόμενα μηνύματα και πιθανά εισάγει νέα. Αυτού του είδους εισβολές διακρίνονται σε τέσσερις υποκατηγορίες :

- Τη μεταβολή των μηνυμάτων. Κατά την παραβίαση αυτή μεταβάλλεται το περιεχόμενο των μηνυμάτων (δεδομένα, διευθύνσεις, τμήματα ελέγχου), εισάγονται νέα μηνύματα ή μεταβάλλεται η σειρά των αποστελλόμενων μηνυμάτων.
- Τη διαγραφή μηνυμάτων. Κατά την οποία καταστρέφεται μέρος ή το σύνολο των μηνυμάτων, που ανταλλάσσονται κατά τη διάρκεια των συνόδων.
- Την καθυστέρηση επικοινωνίας. Ο εισβολέας άμεσα με την κατακράτηση και επαναποστολή μηνυμάτων ή έμμεσα με την εισαγωγή υψηλού φόρτου στο δίκτυο προκαλεί καθυστέρηση της επικοινωνιακής κυκλοφορίας.
- Μεταμφίεση του εισβολέα. Στην περίπτωση αυτή ο εισβολέας δημιουργεί μία, ή περισσότερες συνόδους με ψευδή ταυτότητα. Αυτό επιτυγχάνεται με την υποκλοπή των στοιχείων ταυτότητας ενός 'νόμιμου' χρήστη, καθώς και με την επανάληψη μηνυμάτων που έχουν αντιγραφεί από μία προηγούμενη 'νόμιμη' σύνοδο.

3.6.5 Διαδικασία χειρισμού περιστατικών ασφαλείας

Με στόχο την άμεση αντιμετώπιση των κινδύνων μιας προσβολής του συστήματος, θα πρέπει να εφαρμοστεί μία πολιτική διαχείρισης έκτακτων περιστατικών ασφαλείας. Σύμφωνα με την Πολιτική Διαχείρισης Περιστατικών Ασφάλειας, ορίζεται μια διαδικασία χειρισμού περιστατικών ασφαλείας που έχει ως στόχο της:

- Να καταγραφούν οι λεπτομέρειες κάθε περιστατικού ασφάλειας,
- Να διερευνηθούν τα αίτια και να προσδιοριστούν οι τεχνικές ή/και οργανωτικές αδυναμίες στις οποίες οφείλεται το περιστατικό ασφάλειας,
- Να καθοριστούν και να υλοποιηθούν οι ενέργειες αποκατάστασης καθώς και να σχεδιαστεί κατάλληλο χρονοδιάγραμμα και
- Να ενημερωθούν ο υπεύθυνος Διασφάλισης του Απορρήτου των Επικοινωνιών και τα αρμόδια στελέχη του προσώπου που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών, οι αρμόδιες Αρχές καθώς και οι θιγόμενοι χρήστες των παρεχόμενων δικτύων ή υπηρεσιών.

Η Διαδικασία Διαχείρισης έκτακτων περιστατικών προϋποθέτει τα εξής:

Κάθε πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να καταρτίζει και να εφαρμόζει Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας, η οποία θα ενεργοποιείται σε κάθε περίπτωση παραβίασης ή ιδιαίτερου κινδύνου παραβίασης του απορρήτου των επικοινωνιών ή όταν διαπιστώνεται ότι δεν εφαρμόζεται ή υφίσταται ιδιαίτερος κίνδυνος μη εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών.

Στη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας προβλέπεται η καταγραφή όλων των παραπάνω στοιχείων, που αποτελούν τα στάδια για τη διαχείριση των περιστατικών ασφάλειας, καθώς και η σύνταξη και διατήρηση σε αρχείο όλων των σχετικών με τα περιστατικά ασφάλειας εγγράφων, από τα οποία θα τεκμηριώνεται και η τέλεση των προαναφερόμενων βημάτων.

Στη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας ορίζονται τα αρμόδια στελέχη του προσώπου που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών στα οποία θα πρέπει να αναφέρονται άμεσα τα περιστατικά ασφάλειας από τους εργαζόμενους και τους συνεργάτες του, καθώς και τα σχετικά στοιχεία επικοινωνίας αυτών (τηλέφωνα, fax, email ή άλλο μέσο που κρίνεται πρόσφορο).

Το πρόσωπο που ασχολείται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να παρέχει στους συνδρομητές ή χρήστες των δικτύων ή υπηρεσιών του τη

δυνατότητα να καταγγέλλουν με απλά μέσα (π.χ. μέσω της ιστοθέσης του) την ενδεχόμενη παραβίαση του απορρήτου των επικοινωνιών τους.

3.6.6 Τεχνικές διασφάλισης εμπιστευτικότητας

Οι βασικές τεχνικές διασφάλισης εμπιστευτικότητας στα πληροφοριακά συστήματα είναι δύο. Μια τεχνική είναι ο έλεγχος ταυτότητας, μέσω του οποίου εξασφαλίζεται ότι η οντότητα που παρουσιάζεται με κάποια ταυτότητα είναι όντως αυτή που ισχυρίζεται, η τεχνική αυτή στηρίζεται στην χρήση κωδικών για την επαλήθευση της ταυτότητας.

Υπάρχουν τρεις βασικοί τρόποι για την διακρίβωση της ταυτότητας οι οποίοι μπορούν να χρησιμοποιηθούν μεμονωμένα ή συνδυαστικά:

- Να ζητείται κάτι που ο χρήστης γνωρίζει (ένα μυστικό, π.χ. ένα συνθηματικό, ένας προσωπικός αριθμός αναγνώρισης ή ένα κρυπτογραφικό κλειδί)
- Να ζητείται κάτι που βρίσκεται υπό την κατοχή του χρήστη, όπως μία έξυπνη κάρτα, μία κάρτα αυτόματων ταμειακών συναλλαγών κ.λπ.
- Να εξετάζεται κάποιο βιομετρικό χαρακτηριστικό του χρήστη, όπως π.χ. δακτυλικά αποτυπώματα, σχήμα ίριδας, τρόπος γραφής κ.τ.λ.

Η δεύτερη τεχνική είναι ο έλεγχος προσπέλασης που χρησιμοποιείται για να επιτρέψει σε κάποια διακριβωμένη πια οντότητα να προσπελάσει μόνο τα αντικείμενα και τις υπηρεσίες για τα οποία είναι εξουσιοδοτημένη.

3.6.7 Πολιτική Χρήσης Κωδικών Ασφαλείας

Το βασικό δομικό στοιχείο της ασφάλειας συστημάτων, αποτελεί η διακρίβωση ταυτότητας καθώς είναι τη βάση για τους περισσότερους τύπους ελέγχου πρόσβασης και καταλογισμού ευθυνών. Το σύστημα θα πρέπει να έχει τη δυνατότητα να ταυτοποιεί τους χρήστες και να μπορεί να τους ξεχωρίζει.

Για παράδειγμα, ο έλεγχος πρόσβασης συχνά βασίζεται στην αρχή των ελάχιστων προνομίων, δίνοντας στους χρήστες μόνο τα δικαιώματα που τους είναι απολύτως απαραίτητα για την επιτέλεση των εργασιών τους.

Με τον όρο καταλογισμό ευθυνών εννοούμε τη σύνδεση των δραστηριοτήτων σε ένα υπολογιστικό σύστημα με συγκεκριμένα άτομα, έτσι ώστε το σύστημα να μπορεί να γνωρίζει την ταυτότητα των χρηστών. Κατά τη διακρίβωση ταυτότητας, η οντότητα αρχικά παρουσιάζει στο σύστημα έναν ισχυρισμό περί της ταυτότητας της και ακολούθως το σύστημα εξετάζει αν αυτός ο ισχυρισμός είναι αληθής.

Στη διαδικασία αυτή υπάρχουν τα εξής βήματα: η συλλογή των πληροφοριών που δίνει ο χρήστης, η ασφαλής μετάδοσή τους και ο προσδιορισμός του αν ο χρήστης που αρχικά διακριβώθηκε εξακολουθεί να είναι ο ίδιος που τώρα χρησιμοποιεί το σύστημα. Για παράδειγμα, αν ένας χρήστης συνδεθεί σε κάποιο τερματικό και στη συνέχεια το εγκαταλείψει προσωρινά, είναι δυνατόν κάποιος άλλος χρήστης να το χρησιμοποιήσει υπό την ταυτότητα του πρώτου.

Μολονότι φαίνεται ότι οποιοδήποτε από αυτά τα μέσα μπορεί να παρέχει ισχυρή διακρίβωση ταυτότητας, υπάρχουν και κάποια προβλήματα: τα συνθηματικά μπορεί να διαρρεύσουν ή να μαντευθούν, οι έξυπνες κάρτες μπορεί να κλαπούν ή να κατασκευαστούν πλαστές ακόμη και τα βιομετρικά συστήματα μπορούν να ξεγελασθούν.

Κάθε μέθοδος έχει πλεονεκτήματα αλλά και κάποια μειονεκτήματα για τους διαχειριστές και τους νόμιμους χρήστες, για παράδειγμα οι χρήστες ξεχνάνε τα συνθηματικά ή χάνουν τις έξυπνες κάρτες, και η διαχειριστική επιβάρυνση για την αντιμετώπιση αυτών των ζητημάτων μπορεί να είναι σημαντική.

Επίσης, τα βιομετρικά συστήματα συναντούν προβλήματα αποδοχής από πλευράς χρηστών, έχουν υψηλό κόστος και τεχνικές δυσκολίες. Οι τεχνικές αυτές αλλά και οι δυσκολίες τους αναλύονται παρακάτω.

Τεχνικές όπου ζητείται κάτι που ο χρήστης γνωρίζει. Η πιο συνηθισμένη τεχνική διακρίβωσης ταυτότητας συσχετίζει κάθε ταυτότητα χρήστη με ένα συνθηματικό. Η τεχνική αυτή βασίζεται αποκλειστικά σε κάτι που ο χρήστης γνωρίζει. Υπάρχουν και άλλες τεχνικές που ζητούν κάτι που γνωρίζει ο χρήστης, όπως π.χ. ένα κρυπτογραφικό κλειδί.

- Συνθηματικά: Εδώ απαιτείται από τον χρήστη να εισάγει την ταυτότητά του μαζί με ένα συνθηματικό. Το σύστημα συγκρίνει το συνθηματικό με αυτό που είναι αποθηκευμένο στο αρχείο συνθηματικών για τον συγκεκριμένο χρήστη. Αν είναι ίδια, η ταυτότητα έχει διακριβωθεί επιτυχώς. Η χρήση συνθηματικών έχει παράσχει ασφάλεια σε υπολογιστικά συστήματα για μεγάλο χρονικό διάστημα. Οι σχετικοί μηχανισμοί είναι ενσωματωμένοι στα λειτουργικά συστήματα και οι χρήστες, αλλά και οι διαχειριστές συστημάτων είναι εξοικειωμένοι με αυτά. Με κατάλληλη διαχείριση σε ένα ελεγχόμενο περιβάλλον μπορούν να αποτελέσουν αποτελεσματικό μηχανισμό διακρίβωσης ταυτότητας.
- Κρυπτογραφικά κλειδιά: Σε αυτή την προσέγγιση θα λέγαμε ότι πραγματεύεται η διακρίβωση ταυτότητας βάσει αντικειμένων που έχει στην κατοχή του ο χρήστης. Αν και η δυνατότητα διακρίβωσης της ταυτότητας μέσω κρυπτογραφικού κλειδιού βασίζεται σε κάτι που γνωρίζει ο χρήστης, αυτός πρέπει συνήθως να έχει στη διάθεσή του κάποια συσκευή (π.χ. έξυπνη κάρτα ή PC), η οποία θα εκτελέσει τους κρυπτογραφικούς υπολογισμούς.

Μειονεκτήματα της τεχνικής αυτής είναι αρκετά. Η λειτουργία αυτής της τεχνικής βασίζεται στο ότι δεν θα διαρρεύσουν τα συνθηματικά. Δυστυχώς, υπάρχουν πολλοί τρόποι με τους οποίους είναι δυνατόν να αποκαλυφθούν όπως το μάντεμα του συνθηματικού, ο διαμοιρασμός του συνθηματικού , η ηλεκτρονική παρακολούθηση ή ακόμα και η πρόσβαση στο αρχείο των συνθηματικών.

Όσον αφόρα την ηλεκτρονική παρακολούθηση ούτε η κρυπτογράφηση λύνει το πρόβλημα, καθώς η επανακρυπτογράφηση του ίδιου συνθηματικού θα δώσει το ίδιο κρυπτογραφημένο κείμενο. Συνεπώς, σε ό,τι αφορά το σύστημα που λαμβάνει το συνθηματικό, αν του σταλεί ξανά το κρυπτογραφημένο κείμενο που υπεκλάπη θα το θεωρήσει ως σωστό συνθηματικό.

Όσον αφόρα την πρόσβαση στο αρχείο συνθηματικών τα περισσότερα αρχεία συνθηματικών συνήθως προστατεύονται με μονόδρομη κρυπτογράφηση. Πάραυτα με εξαντλητική αναζήτηση και την αυξημένη υπολογιστική ισχύ των σύγχρονων υπολογιστών, εξακολουθεί να είναι δυνατή η εύρεση των συνθηματικών.

Τεχνικές όπου ζητείται κάτι που ο χρήστης κατέχει. Αν και αρκετές τεχνικές βασίζονται αποκλειστικά σε κάτι που ο χρήστης κατέχει, συνήθως ζητείται παράλληλα και κάτι που ο χρήστης γνωρίζει. Ο συνδυασμός αυτός συνήθως αποφέρει υψηλότερα επίπεδα ασφάλειας. Τα αντικείμενα που κατέχει ο χρήστης για σκοπούς διακρίβωσης ταυτότητας καλούνται διακριτικά (tokens). Τα Διακριτικά διαχωρίζονται σε διακριτικά μνήμης και σε έξυπνα διακριτικά.

- Διακριτικά μνήμης: Τα διακριτικά μνήμης αποθηκεύουν αλλά δεν επεξεργάζονται πληροφορίες. Η εγγραφή και η ανάγνωση δεδομένων σε/από αυτά διενεργείται μέσω ειδικών συσκευών. Ο πιο διαδεδομένος τύπος διακριτικών μνήμης είναι οι κάρτες που είναι εφοδιασμένες με μία μαγνητική ταινία, οι οποίες διαβάζονται από ειδικούς αναγνώστες όπως οι κάρτες τραπεζών για ανάληψη μετρητών από αυτόματες ταμειακές μηχανές – ΑΤΜ. Οι χρήστες απαιτείται, πέρα από το ίδιο το διακριτικό, να εισάγουν και έναν προσωπικό αριθμό αναγνώρισης. Σε μερικά συστήματα η διακρίβωση ταυτότητας γίνεται αποκλειστικά μέσω ενός διακριτικού, χωρίς να ζητείται κάτι που ο χρήστης γνωρίζει. Τα συστήματα αυτά είναι σχετικά λίγα και κυρίως αφορούν τον έλεγχο φυσικής πρόσβασης σε χώρους.
- Έξυπνα διακριτικά: Ένα έξυπνο διακριτικό επεκτείνει τη λειτουργικότητα ενός διακριτικού μνήμης, ενσωματώνοντας ένα ή περισσότερα ολοκληρωμένα κυκλώματα. Όταν χρησιμοποιείται για διακρίβωση ταυτότητας, ένα έξυπνο διακριτικό εμπίπτει στην κατηγορία τεχνικών όπου ζητείται κάτι που ο χρήστης κατέχει, ενώ είναι δυνατόν παράλληλα να ζητείται κάτι που ο χρήστης γνωρίζει όπως π.χ. ένας προσωπικός αριθμός αναγνώρισης. Υπάρχουν πολλά διαφορετικά είδη έξυπνων διακριτικών.

Πλεονεκτήματα των διακριτικών μνήμης είναι ότι αν συνδυαστούν με προσωπικούς αριθμούς αναγνώρισης είναι πολύ πιο ασφαλή από τα συνθηματικά. Επίσης, είναι ιδιαίτερα φθηνά, ενώ για να καταφέρει ένας μη εξουσιοδοτημένος χρήστης να αποκτήσει πρόσβαση πρέπει και να έχει στην κατοχή του και το διακριτικό και να γνωρίζει τον αριθμό. Ο συνδυασμός αυτός είναι πιο δύσκολο να αποκτηθεί απ' ό,τι ένα ζεύγος (ταυτότητα χρήστη, συνθηματικό), ειδικότερα αν λάβουμε υπόψη ότι οι ταυτότητες χρήστη δεν είναι μυστικές. Ένα ακόμα πλεονέκτημα των διακριτικών είναι ότι μπορούν να χρησιμοποιηθούν για παραγωγή αρχείων καταγραφής, χωρίς να είναι απαραίτητο να εισάγει ο χρήστης την ταυτότητά του για κάθε δοσοληψία ή συμβάν που πρέπει να καταγραφεί, καθώς το σύστημα αντλεί τη σχετική πληροφορία από το διακριτικό. Αν το διακριτικό χρησιμοποιείται, εκτός από την διακρίβωση ταυτότητας στον υπολογιστή, και για είσοδο και έξοδο από τον φυσικό χώρο, τότε οι χρήστες αναγκαστικά το αφαιρούν από τον υπολογιστή όταν απομακρύνονται από τον χώρο. Με τον τρόπο αυτό μηδενίζεται η πιθανότητα να χρησιμοποιήσει κανείς κάποιο τερματικό που άφησε ανεπιτήρητο ένας χρήστης.

Η χρήση διακριτικών μνήμης όμως έχει και κάποια μειονεκτήματα. Αν και είναι τελικά δυνατή η πραγματοποίηση πολύ καλά προετοιμασμένων επιθέσεων ενάντια σε συστήματα που χρησιμοποιούν αυτή τη μέθοδο, τα περισσότερα προβλήματα ανάγονται στο κόστος, τη διαχείριση, την απώλεια των διακριτικών, τη δυσαρέσκεια των χρηστών και τη διαρροή των προσωπικών αριθμών αναγνώρισης. Όσον αφόρα το κόστος τα διακριτικά μνήμης απαιτούν εξειδικευμένες συσκευές ανάγνωσης του προσωπικού αριθμού του χρήστη καθώς και την χρήση κρυπτογραφίας για την μετάδοση των δεδομένων. Από την άλλη αν ένας χρήστης χάσει το διακριτικό του, δεν θα μπορεί να συνδεθεί στο σύστημα μέχρι να αντικατασταθεί το διακριτικό. Με τον τρόπο αυτό αυξάνεται το διαχειριστικό κόστος και η επιβάρυνση.

Το απολεσθέν διακριτικό μπορεί να έχει κλαπεί ή μπορεί να βρεθεί από κάποιον και ο νέος κάτοχός του μπορεί να επιχειρήσει να εισέλθει στο σύστημα. Επίσης, έχουμε και την δυσαρέσκεια των χρηστών, οι οποίοι επιθυμούν υπολογιστές εύκολους στη χρήση. Πολλοί από αυτούς το βρίσκουν άβολο να κουβαλάνε και να χρησιμοποιούν ένα διακριτικό. Οι αντιδράσεις ωστόσο περιορίζονται αν είναι προφανής η αναγκαιότητα για αυξημένη ασφάλεια.

Όσον αφορά τα έξυπνα διακριτικά μπορούν να καταταχθούν σε κατηγορίες βάσει των φυσικών χαρακτηριστικών τους, της διεπαφής τους και των πρωτοκόλλων που χρησιμοποιούν. Οι κατηγοριοποιήσεις αυτές δεν είναι αμοιβαία αποκλειόμενες.

<u>Φυσικά χαρακτηριστικά</u>: Τα έξυπνα διακριτικά μπορεί να είναι «έξυπνες κάρτες», οι οποίες μοιάζουν με πιστωτικές κάρτες αλλά περιλαμβάνουν επίσης και κάποιον μικροεπεξεργαστή. Οι έξυπνες κάρτες περιγράφονται από ένα πρότυπο του διεθνούς οργανισμού προτύπων (ISO). Τα έξυπνα διακριτικά που δεν είναι «έξυπνες κάρτες» μοιάζουν συνήθως με μικρές αριθμομηχανές.

Διεπαφή: Τα έξυπνα διακριτικά έχουν μία διεπαφή που μπορεί να τους επιτρέπει να επικοινωνούν είτε με ανθρώπους είτε με ηλεκτρονικά συστήματα. Τα διακριτικά που έχουν διεπαφή για επικοινωνία με ανθρώπους ενσωματώνουν οθόνες ή/και πληκτρολόγια για να επιτρέπουν την εισαγωγή και την προβολή στοιχείων. Τα διακριτικά με διεπαφές για επικοινωνία με ηλεκτρονικά συστήματα ανταλλάσσουν δεδομένα με ειδικές διατάξεις ανάγνωσης/εγγραφής. Τα διακριτικά που έχουν τη μορφή αριθμομηχανών συνήθως διαθέτουν διεπαφή για επικοινωνία με ανθρώπους.

Πρωτόκολλο: Ένα έξυπνο διακριτικό μπορεί να χρησιμοποιήσει διάφορα πρωτόκολλα για την διακρίβωση ταυτότητας.

Τα έξυπνα διακριτικά που χρησιμοποιούν πρωτόκολλα ανάλογα με το είδος πρωτοκόλλου που χρησιμοποιούν μπορούν να διακριθούν σε τρεις κατηγορίες:

- Στατική ανταλλαγή συνθηματικών. Βάσει του πρωτοκόλλου αυτού οι χρήστες εισάγουν το συνθηματικό τους στο έξυπνο διακριτικό, το οποίο κατόπιν συνεργάζεται με τον υπολογιστή για τη διακρίβωση της ταυτότητας του χρήστη.
- Δυναμική γέννηση συνθηματικών. Βάσει του πρωτοκόλλου αυτού, το έξυπνο διακριτικό δημιουργεί μία μοναδική τιμή, π.χ. έναν οκταψήφιο αριθμό, ο οποίος αλλάζει περιοδικά. Αν το διακριτικό έχει διεπαφή προσανατολισμένη σε επικοινωνία με ανθρώπους, ο χρήστης απλά διαβάζει τον αριθμό από την οθόνη του διακριτικού και το εισάγει στον υπολογιστή για διακρίβωση της ταυτότητάς του. Αν το διακριτικό έχει διεπαφή προσανατολισμένη σε επικοινωνία με ηλεκτρονικές διατάξεις, ο αριθμός αποστέλλεται αυτομάτως. Αν η εισαχθείσα τιμή είναι σωστή (δηλαδή είναι ανάμεσα στις παραδεκτές τιμές που ο υπολογιστής γνωρίζει ότι μπορεί να παράγει το συγκεκριμένο διακριτικό για τη δεδομένη χρονική περίοδο), θεωρείται ότι η ταυτότητα του χρήστη έχει διακριβωθεί.
- Πρωτόκολλα ερωταποκρίσεων. Βάσει του πρωτοκόλλου αυτού ο υπολογιστής δημιουργεί μία ερώτηση π.χ. μία τυχαία ακολουθία από αριθμούς. Το έξυπνο διακριτικό παράγει μία απάντηση, ως συνάρτηση της ερώτησης, η οποία αποστέλλεται στον υπολογιστή, και ο υπολογιστής διακριβώνει την ταυτότητα του χρήστη βάσει της απάντησης. Οι αλγόριθμοι υπολογισμού της απάντησης από την ερώτηση στηρίζονται σε κρυπτογραφικές μεθόδους. Τα πρωτόκολλα ερωταποκρίσεων μπορούν να χρησιμοποιηθούν είτε με διεπαφές προσανατολισμένες σε επικοινωνία με ανθρώπους είτε με διεπαφές για επικοινωνία με ηλεκτρονικές διατάξεις.

Τα έξυπνα διακριτικά παρέχουν μεγάλη ευελιξία και μπορούν να λύσουν πολλά προβλήματα διακρίβωσης ταυτότητας. Τα πλεονεκτήματα που αποκομίζουμε από τη χρήση τους ποικίλλουν, ανάλογα με το είδος των διακριτικών που χρησιμοποιούνται, στη γενική περίπτωση πάντως

προσφέρουν μεγαλύτερη ασφάλεια από τα διακριτικά μνήμης. Τα έξυπνα διακριτικά μπορούν να λύσουν και το πρόβλημα της υποκλοπής των συνθηματικών κατά τη δικτυακή επικοινωνία, ακόμη και αν αυτή πραγματοποιείται μέσα από ανοικτά δημόσια δίκτυα, καθώς μπορούν να εφαρμόσουν τεχνικές συνθηματικών μίας χρήσης (π.χ. στην περίπτωση του πρωτοκόλλου ερωταποκρίσεων).
Να εξετάζεται κάποιο βιομετρικό χαρακτηριστικό του χρήστη, όπως π.χ. δακτυλικά αποτυπώματα, σχήμα ίριδας, τρόπος γραφής κ.τ.λ.

3.7 Κανόνες και μέτρα υλοποίησης της πολιτικής ασφαλείας

3.7.1 Κανόνες Πολιτικής Ασφαλείας

Γενικά, στο πλαίσιο της λειτουργίας ενός οργανισμού, μια πολιτική αποτελεί το σύνολο των οδηγιών της διοίκησης για τον τρόπο με τον οποίο πρέπει να λειτουργεί ο οργανισμός. Περιλαμβάνει δηλαδή γενικές προτάσεις (high-level statements) που έχουν στόχο να καθοδηγήσουν τη λήψη αποφάσεων σχετικά με τα τρέχοντα και μελλοντικά ζητήματα που αντιμετωπίζουν τα μέλη του οργανισμού. Πολλές φορές στον όρο ‘πολιτική’ αποδίδεται η έννοια των γενικευμένων απαιτήσεων, στις οποίες θα πρέπει να ανταποκρίνεται η δράση και οι επιλογές των ανθρώπων τους οποίους αφορά η πολιτική.

Για τη σχεδίαση της πολιτικής ασφαλείας απαιτείται η ικανοποίηση των παρακάτω προϋποθέσεων :

Πολιτική εξασφάλισης (security policy): Πρέπει να υπάρχει μια σαφής δέσμη βασικών αρχών, η οποία περιλαμβάνει τους στόχους των σχεδιαστών του Λειτουργικού συστήματος.

Ταυτοποίηση (identification): Κάθε αντικείμενο του συστήματος πρέπει να μπορεί να αναγνωρισθεί θετικά.

Σήμανση (marking): Κάθε αντικείμενο του συστήματος πρέπει να συνοδεύεται από μια ένδειξη του βαθμού εμπιστευτικότητας του.

Ελεγκτικότητα (accountability): Το σύστημα πρέπει να καταγράφει όλες τις ενέργειες που αφορούν ή μπορούν να επηρεάσουν την ασφάλεια του.

Διαβεβαίωση (assurance): Το σύστημα πρέπει να παρέχει τεχνικές ρυθμίσεις για την υλοποίηση της πολιτικής εξασφάλισής του, οι οποίες να μπορούν να εκτιμηθούν ως προς την αποτελεσματικότητά τους.

Συνεχής προστασία (continuous protection): Οι τεχνικές εξασφάλισης του Λ.Σ. πρέπει να προστατεύονται από κάθε ανεπιθύμητη μετατροπή.

Επίσης, θα πρέπει να πληροί τις παρακάτω ιδιότητες:

- Ευχρηστία (Usability). Το σύστημα πρέπει να είναι σχεδιασμένο με στόχο την διευκόλυνση του χρήστη.
- Γενικότητα (Generality). Το σύστημα πρέπει να μπορεί να εκτελέσει ποικίλες διαδικασίες, σύμφωνα με τις ανάγκες του χρήστη.
- Αποδοτικότητα (Effeciency). Το σύστημα πρέπει να λειτουργεί γρήγορα και ορθά, χρησιμοποιώντας κατά βέλτιστο τρόπο τους διατιθέμενους πόρους.
- Ευελιξία (Flexibility). Το σύστημα πρέπει να μπορεί να προσαρμόζεται σε διαρκώς μεταβαλλόμενες καταστάσεις
- Αδιαφάνεια (Opacity). Ο χρήστης πρέπει να γνωρίζει μόνο ότι είναι απαραίτητο για να διεκπεραιώσει την εργασία του .
- Ασφάλεια (Security). Το σύστημα πρέπει να διαφυλάσσει τα δεδομένα ενός χρήστη από μη εξουσιοδοτημένη χρήση τους από άλλους.
- Ακεραιότητα (Integrity). Οι χρήστες και τα δεδομένα τους πρέπει να διαφυλάσσονται από απρόβλεπτες μετατροπές από μη εξουσιοδοτημένους χρήστες.
- Ευκινησία (Capacity). Οι χρήστες δεν πρέπει να υφίστανται άσκοπους περιορισμούς στις ενέργειές τους.
- Αξιοπιστία (Reliability). Τα συστήματα πρέπει να λειτουργούν σωστά, για όσο το δυνατόν μεγαλύτερο χρονικό διάστημα.
- Συντηρησιμότητα (Serviceability). Πιθανά προβλήματα στη λειτουργία του συστήματος πρέπει να μπορούν να ξεπεραστούν εύκολα και γρήγορα.
- Επεκτασιμότητα (Extentability). Το σύστημα πρέπει να μπορεί να αναβαθμισθεί εύκολα, με επέκταση των δυνατοτήτων που διαθέτει.
- Διαθεσιμότητα (Availability). Το σύστημα πρέπει να εξυπηρετεί τους χρήστες όσο το δυνατόν πληρέστερα.

3.7.2 Μέτρα Υλοποίησης Πολιτικής Ασφαλείας

Τα μέτρα υλοποίησης της Πολιτικής Ασφαλείας των ΠΣ μπορούν να κατηγοριοποιηθούν ανάλογα με τον στόχο προστασίας τους σε μέτρα για την

- Προστασία Χώρων και υποδομών
- Προστασία Πληροφοριακών Συστημάτων
- Προστασία Δεδομένων

- Προστασία Δικτύων

3.7.3 Προστασία Χώρων και Υποδομών

Η προστασία των χώρων και των υποδομών αναφέρεται στα μέτρα που υποστηρίζουν τη φυσική ασφάλεια και έχουν ως κύριο στόχο την αποτροπή της μη εξουσιοδοτημένης πρόσβασης στους χώρους όπου είναι εγκατεστημένα τα πληροφοριακά συστήματα και της καταστροφής των αγαθών τους. Αφορά κυρίως τον Έλεγχο φυσικής πρόσβασης σε κρίσιμους χώρους όπως το Computer Room και στην Προστασία της υγείας των χρηστών των πληροφοριακών συστημάτων (safety).

Όσον αφόρα τους κρίσιμους χώρους της εταιρείας, η πρόσβαση εξαρτάται από τους ρόλους και τις δραστηριότητες του προσωπικού της εταιρείας. Με στόχο την αποφυγή και την προφύλαξη των συστημάτων και των δεδομένων της εταιρείας από κλοπή έχει εγκατασταθεί αντικλεπτικό σύστημα συναγερμού.

Η αντιμετώπιση φυσικών απειλών όπως οι πυρκαγιές, οι πλημμύρες, οι σεισμοί κ.α., που είναι σημαντικές απειλές και για τους ίδιους τους χρήστες των συστημάτων, εξαρτάται και από τον σχεδιασμό του κτιρίου ή του χώρου όπου είναι εγκατεστημένα τα συστήματα. Επίσης, η φυσική ασφάλεια των συστημάτων σχετίζεται άμεσα και με την κατάλληλη εκπαίδευση του προσωπικού και των κατάλληλων μηχανισμών προστασίας, όπως συσκευών πυρόσβεσης.

Απαραίτητη επίσης είναι η συστηματική συντήρηση των ηλεκτρικών εγκαταστάσεων καθώς χρήσιμη είναι η ύπαρξη μιας γεννήτριας παροχής ηλεκτρικής ενέργειας ή συστήματος αδιάλειπτης παροχής τάσεως (UPS), για να αποφεύγονται πιθανές απώλειες του λογισμικού και να υποστηρίζεται η καλή λειτουργία του μηχανολογικού εξοπλισμού κατά την πτώση της τάσης του ρεύματος ή διακοπής της παροχής του ηλεκτρικού ρεύματος.

3.8 Προστασία Πληροφοριακών Συστημάτων

3.8.1 Έλεγχος Πρόσβασης

Βασική προϋπόθεση στην ασφάλεια των συστημάτων της εταιρείας είναι ο έλεγχος πρόσβασης στα συστήματα της τόσο από φυσική άποψη στο υλικό κομμάτι, φυλάσσοντας και προστατεύοντας τους servers της και τα υπόλοιπα υπολογιστικά συστήματα σε ασφαλείς χώρους, εξασφαλίζοντας περιορισμένη και ελεγχόμενη πρόσβαση σε αυτά, όσο και ο έλεγχος πρόσβασης των απομακρυσμένων χρηστών της στις υπηρεσίες της και της εφαρμογές της. Η πρόσβαση θα πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες καθότι απειλές μπορεί να δεχτούν τα συστήματα και από εσωτερικούς χρήστες, όχι μόνο από εξωτερικούς. Οι απειλές εκ των έσω μπορεί να είναι η διαρροή ευαίσθητων πληροφοριών, κρούσματα ιών, απάτες από κακόβουλους χρήστες κ.α τα οποία

χρήζουν αντίστοιχης αντιμετώπισης. Για αυτό απαραίτητη προϋπόθεση για ολοκληρωμένη ασφάλεια είναι και η προστασία από εσωτερικές απειλές.

Η πρόσβαση θα επιτρέπεται μόνο μέσω διαδικασιών αυθεντικοποίησης και ταυτοποίησης. Η έξυπνη κάρτα (smart card) είναι μια κάρτα που ενσωματώνει ένα μικροεπεξεργαστή, ο οποίος βρίσκεται κάτω από μια επαφή από χρυσό, προσαρμοσμένο στη μια πλευρά της. Τα δεδομένα στην έξυπνη κάρτα δεν είναι εύκολο να παραλλαχθούν ή και να διαγραφούν, γιατί ο μικροεπεξεργαστής της δεν περιέχει δεδομένα για το χρήστη. Ο μικροεπεξεργαστής της κάρτας και ο υπολογιστής, με τον οποίο συνδέεται, επικοινωνούν πριν ο μικροεπεξεργαστής επιτρέψει την πρόσβαση στα δεδομένα που περιέχονται στη μνήμη της κάρτας. Με τον τρόπο αυτό αποτρέπεται η παραχάραξη των δεδομένων κι έτσι ο χρήστης διασφαλίζεται, αν η κάρτα του βρεθεί σε διαφορετικά από τα δικά του χέρια.

Η τροφοδοσία της κάρτας με ενέργεια εξασφαλίζεται από τον αναγνώστη έξυπνης κάρτας (smart card reader), στον οποίο εισάγεται η κάρτα προκειμένου να χρησιμοποιηθεί. Αυτός μπορεί να επικοινωνήσει με κάποιο κεντρικό υπολογιστή, όπου υπάρχουν τα στοιχεία του χρήστη, προκειμένου να εξασφαλιστεί η πρόσβαση σε δεδομένα.

3.8.2 Έλεγχος Προσπέλασης

Απαραίτητη προϋπόθεση ασφαλής λειτουργίας των πληροφοριακών συστημάτων είναι ο έλεγχος. Από τη στιγμή που έχει διακριβωθεί η ταυτότητα ενός χρήστη μέσω του έλεγχου πρόσβασης, το σύστημα θα πρέπει να φροντίζει έτσι ώστε ο χρήστης αυτός να μπορεί να ενεργήσει μόνο στα πλαίσια των κανόνων που καθορίζονται από την πολιτική ασφάλειας. Αυτό επιτυγχάνεται εφαρμόζοντας ελέγχους προσπέλασης. Σχετικά με τους ελέγχους προσπέλασης ισχύουν οι ακόλουθες έννοιες:

- Υποκείμενα. Πρόκειται για τις ενεργές οντότητες στο σύστημα (χρήστες, διεργασίες, υπηρεσίες)
- Αντικείμενα. Με τον όρο αυτό περιγράφονται οι πόροι ή οι παθητικές οντότητες στο σύστημα (αρχεία, συσκευές, προγράμματα)
- Τρόπος προσπέλασης. Ο όρος αυτός αναφέρεται στην ενέργεια που πραγματοποιεί ένα υποκείμενο σε ένα αντικείμενο π.χ. ανάγνωση, εγγραφή, εκτέλεση, αναφορά ιδιοχαρακτηριστικών.

Ο έλεγχος προσπέλασης συνίσταται στην εξέταση αν το υποκείμενο έχει δικαίωμα για τον συγκεκριμένο τρόπο προσπέλασης στο αντικείμενο, και στην απαγόρευση της ενέργειας, αν τελικά δεν υπάρχει το σχετικό δικαίωμα. Η επιλογή της πολίτικης έλεγχου προσπέλασης εξαρτάται από τα επιμέρους χαρακτηριστικά του περιβάλλοντος που πρόκειται να προστατευτεί .

Οι τρεις βασικές προσεγγίσεις ελέγχου προσπέλασης είναι οι εξής:

- Η κατά-διάκριση (Discretionary Access Control - DAC). Μια αρκετά διαδεδομένη προσέγγιση κυρίως σε στρατιωτικούς οργανισμούς, από όπου και προέρχεται, είναι η υποχρεωτική (mandatory) προσέγγιση. Σύμφωνα με αυτή την προσέγγιση, επιτρεπτές είναι μόνο οι ενέργειες που προβλέπονται και προδιαγράφονται στην πολιτική ασφάλειας. Οτιδήποτε δεν περιλαμβάνεται στην πολιτική ασφάλειας απαγορεύεται, ανεξάρτητα από τις συνθήκες ή τις συνέπειες που η απαγόρευση αυτή μπορεί να επιφέρει. Η προσέγγιση αυτή είναι αρκετά δημοφιλής στην ανάπτυξη πολιτικών ασφάλειας πληροφοριακών συστημάτων, παρόλο που οι πολιτικές ασφάλειας που την ακολουθούν συχνά αποδεικνύονται άκαμπτες και αναποτελεσματικές. Είναι προφανές ότι οι προδιαγραφές και οδηγίες ασφάλειας δε μπορούν να είναι τόσο λεπτομερείς, ούτε τέτοιες που να μπορούν να καλύψουν το σύνολο των δυνατών περιπτώσεων που απαιτείται κάποια ενέργεια από τους χρήστες του πληροφοριακού συστήματος. Ειδικά σε δυναμικά περιβάλλοντα με συχνές αλλαγές, η προσέγγιση αυτή είναι λιγότερο αποτελεσματική από τις άλλες προσεγγίσεις .
- Η κατά-απαίτηση (Mandatory Access Control - MAC). Για τις πολιτικές ασφάλειας που διαμορφώνονται με βάση την προσέγγιση διακριτού (discretionary) ελέγχου, όλες οι ενέργειες που δεν περιλαμβάνονται στις απαγορευμένες θεωρούνται επιτρεπτές και σύμφωνες με την πολιτική.

Έτσι, στην περίπτωση που απαιτείται κάποια ενέργεια η οποία δεν περιλαμβάνεται στην πολιτική ασφάλειας, θεωρείται ότι ο χρήστης θα δράσει με τρόπο που συμβαδίζει με τους στόχους της πολιτικής ασφάλειας. Η προσέγγιση αυτή, είναι ευκολότερα να γίνει αποδεκτή από τους χρήστες των πληροφοριακών συστημάτων που καλούνται να εφαρμόσουν την πολιτική ασφάλειας, διότι είναι αντίστοιχη με τον τρόπο που ισχύει η νομοθεσία ενός κράτους: οι πολίτες γνωρίζουν ότι οι ενέργειες τους θεωρούνται νόμιμες, εκτός αν ανήκουν σε αυτές που απαγορεύονται. Το προτέρημα της προσέγγισης αυτής έναντι των υπολοίπων είναι η μεγαλύτερη αποδοχή των πολιτικών ασφάλειας από τους χρήστες των πληροφοριακών συστημάτων.

Από την άλλη πλευρά, η μεγάλη ευελιξία των πολιτικών αυτών μπορεί να οδηγήσει σε μείωση του επιπέδου ασφάλειας, αυξάνοντας την επικινδυνότητα.

- Η βασισμένη-σε-ρόλους (Role-Based Access Control). Σύμφωνα με την προσέγγιση αυτή, οι οδηγίες ασφάλειας που προδιαγράφονται στην πολιτική εφαρμόζονται, μπορούν και να παρακαμφθούν όμως όταν υπάρχουν αντικρουόμενες απαιτήσεις. Επίσης οι πολιτικές αυτές μπορεί να παρακαμφθούν και στην περίπτωση που τα προσδοκώμενα οφέλη από τη μη τήρηση των οδηγιών αυτών (εξαιρουμένου του προσωπικού-ατομικού οφέλους) υπερτερούν των οφελών που θα προκύψουν από την εφαρμογή των οδηγιών της πολιτικής ασφάλειας, σε

όρους επιχειρηματικών στόχων και στόχων ασφάλειας. Τα πλεονεκτήματα αυτής της προσέγγισης γίνονται περισσότερο φανερά σε ειδικές περιπτώσεις που δε θα μπορούσαν να έχουν προβλεφθεί και συμπεριληφθεί στις οδηγίες μιας πολιτικής ασφάλειας. Στις περιπτώσεις αυτές, η δράση των χρηστών είναι πιο ευέλικτη, σε σχέση με τις άλλες προσεγγίσεις. Το μειονέκτημα της 'κατά περίπτωση' πολιτικής ασφάλειας συνδέεται με τη δυνατότητα παράκαμψης της πολιτικής κατά την κρίση των χρηστών του πληροφοριακού συστήματος. Η δυνατότητα επιλογής για τη συμμόρφωση ή μη με την πολιτική ασφάλειας σε σχέση με τα αναμενόμενα οφέλη από την εφαρμογή της πολιτικής εισάγει το στοιχείο της υποκειμενικότητας, καθώς εναπόκειται στους χρήστες του πληροφοριακού συστήματος να αξιολογήσουν και να κρίνουν τις πιθανές συνέπειες και τα πιθανά οφέλη από την εφαρμογή των οδηγιών ασφάλειας.

Οι δυο πρώτες κατηγορίες χαρακτηρίζονται ως κλασσικές, καθώς έχουν αναγνωρίσει και εφαρμοστεί από τους ερευνητές και επαγγελματίες ασφάλειας για πολύ καιρό. Τα τελευταία χρόνια κατά γενική ομολογία υπάρχουν μοντέλα έλεγχου προσπέλασης που έχουν τα χαρακτηριστικά και των δυο προσεγγίσεων όπως τα βασισμένα σε ρόλους μοντέλα., τα οποία έχουν μονοπωλήσει τα τελευταία χρόνια το ενδιαφέρον των ερευνητών.

3.8.3 Προστασία Βάσεων Δεδομένων

Όσον αφορά την ασφάλεια βάσεων δεδομένων, θα πρέπει να λαμβάνεται υπ' όψιν ότι η βάση δεδομένων είναι ένα σύστημα που εκτελείται σε έναν υπολογιστή, πάνω από ένα λειτουργικό σύστημα, και έτσι επηρεάζεται άμεσα από τους μηχανισμούς ασφάλειας που παρέχει ο συνδυασμός αυτός υλικού/λογισμικού. Αν για παράδειγμα το λειτουργικό σύστημα δεν παρέχει επαρκείς μηχανισμούς διακρίβωσης ταυτότητας, η βάση δεδομένων θα πρέπει να υλοποιήσει δικούς της. Επίσης, αν η βάση δεδομένων αποθηκεύεται σε αρχεία που δεν προστατεύονται επαρκώς από το λειτουργικό σύστημα, οι μηχανισμοί ελέγχου πρόσβασης που υλοποιούνται από τη βάση δεδομένων μπορούν να παρακαμφθούν, απλά διαβάζοντας ή τροποποιώντας τα αρχεία σε επίπεδο λειτουργικού συστήματος.

Βασικοί κανόνες για την προστασία των βάσεων είναι ότι τόσο κατά τη φάση της επεξεργασίας των πληροφοριών όσο και κατά τη φάση της μετάδοσης πρέπει αφενός να εκτελεστούν στο σύνολο τους όλες οι δοσοληψίες και αφετέρου ότι να εφαρμόζονται όλοι οι κανόνες ακεραιότητας που έχουν ορισθεί για τη βάση δεδομένων.

Σε γενικές γραμμές μία βάση δεδομένων θα πρέπει να διαφυλάσσει την εμπιστευτικότητα των πληροφοριών την παρέχοντα πρόσβαση σε εξουσιοδοτημένους χρήστες, την ακεραιότητα των πληροφοριών της καθώς και την διαθεσιμότητα τους.

Η εμπιστευτικότητα των πληροφοριών επιτυγχάνεται με τον έλεγχο πρόσβασης στις Βάσεις Δεδομένων, ώστε να διαπιστώνεται αν ένας χρήστης έχει το δικαίωμα να χρησιμοποιήσει το σύστημα βάσεων δεδομένων ή όχι.

Για διακρίβωση της ταυτότητας των χρηστών διατίθενται οι παρακάτω τεχνικές:

- Διακρίβωση ταυτότητας με όνομα χρήστη-συνθηματικό.

Η βάση δεδομένων διαθέτει κατάλογο με τις έγκυρες αντιστοιχίες ονομάτων χρηστών και συνθηματικών ώστε να αποφασίζει για το αν τα παρουσιασθέντα διαπιστευτήρια είναι έγκυρα. Η τεχνική αυτή είναι χρήσιμη όταν το λειτουργικό σύστημα δεν παρέχει αξιόπιστους μηχανισμούς διακρίβωσης ταυτότητας των χρηστών ή όταν πραγματοποιούνται συνδέσεις μέσω δικτύου στη βάση δεδομένων, οπότε η ταυτότητα του χρήστη στο λειτουργικό σύστημα δεν είναι διαθέσιμη ή αξιόπιστη.

- Διακρίβωση ταυτότητας από το λειτουργικό σύστημα.

Σ' αυτή την περίπτωση η πρόσβαση στην ΒΔ στηρίζεται στους μηχανισμούς του λειτουργικού συστήματος για την διακρίβωση ταυτότητας. Από τη στιγμή που ένας χρήστης έχει αναγνωριστεί από το λειτουργικό σύστημα και ο χρήστης λειτουργικού συστήματος είναι εξουσιοδοτημένος να χρησιμοποιεί τη βάση δεδομένων, δεν ζητείται κανένα πρόσθετο στοιχείο για την προσπέλαση του χρήστη στη βάση δεδομένων.

Η τεχνική αυτή δεν μπορεί να χρησιμοποιείται ως αποκλειστικός μηχανισμός διακρίβωσης ταυτότητας σε συστήματα όπου επιτρέπεται δικτυακή πρόσβαση στη βάση δεδομένων, καθώς χρειάζεται κάθε χρήστης να έχει λογαριασμό στο λειτουργικό σύστημα. Επίσης, πρέπει να χρησιμοποιείται μόνον όταν το λειτουργικό σύστημα έχει επαρκώς αξιόπιστους μηχανισμούς διακρίβωσης ταυτότητας.

- Διακρίβωση ταυτότητας μέσω καθολικών υπηρεσιών καταλόγου.

Ο χρήστης εισάγει ένα όνομα και ένα συνθηματικό και για διακρίβωση του το σύστημα διασυνδέεται με καθολικές υπηρεσίες καταλόγου. Η προσέγγιση αυτή έχει το πλεονέκτημα ότι προωθεί τη χρήση κεντρικού σημείου φύλαξης των διαπιστευτηρίων σύνδεσης. Έχοντας ένα κεντρικό σημείο φύλαξης, είναι δυνατόν όλες οι ενότητες λογισμικού που απαιτούν πιστοποίηση (λειτουργικό σύστημα, βάση δεδομένων κ.λπ.) να συνδιαλέγονται με το σημείο αυτό, ούτως ώστε κάθε χρησιμοποιεί ένα μόνο ζεύγος διαπιστευτηρίων για προσπέλαση σε όλους τους πόρους.

Η ακεραιότητα των δεδομένων στα συστήματα βάσεων δεδομένων αποτελεί βασική προϋπόθεση για αυτό και τα δεδομένα πρέπει να διασώζονται σε περιπτώσεις βλαβών υλικού και δυσλειτουργιών του λογισμικού, οι τροποποιήσεις πρέπει να γίνονται μόνο από εξουσιοδοτημένους χρήστες και κάθε φορά να επιστρέφονται τα δεδομένα που έχουν αποθηκευτεί. Σε περίπτωση παραβίασης της ακεραιότητας, οι ενδιαφερόμενοι χρήστες πρέπει τουλάχιστον να ειδοποιούνται.

Η φυσική ακεραιότητα της βάσης δεδομένων συσχετίζεται με τη φθορά που μπορούν να υποστούν τα μαγνητικά μέσα αποθήκευσης από διακοπές ρεύματος, βλάβες κυκλωμάτων ή φυσιολογική φθορά. Το σύστημα θα πρέπει να παρέχει μηχανισμούς ανάκαμψης από το σφάλμα και ανάκτησης των δεδομένων. Ένα τρόπος διαφύλαξης της φυσικής ακεραιότητας είναι η τήρηση εφεδρικών αντιγράφων. Για τα εφεδρικά αντίγραφα είναι σημαντικό να μπορούν να λαμβάνονται ενόσω η βάση δεδομένων βρίσκεται εν λειτουργία.

Υπάρχουν δύο είδη εφεδρικών αντιγράφων βάσεων δεδομένων:

- Τα φυσικά αντίγραφα αποτυπώνουν τα περιεχόμενα των δίσκων, όπως ακριβώς τα αποθηκεύει η βάση δεδομένων, χωρίς να ενδιαφέρονται για τη λογική τους δομή, λαμβάνονται σε μικρότερο χρόνο και αποκαθίστανται ταχύτερα. Συνήθως όμως απαιτούν να διακόπτεται η λειτουργία της βάσης δεδομένων κατά τη λήψη τους και είναι πιθανόν να λειτουργούν μόνο σε σύστημα «όμοιο» με αυτό από το οποίο ελήφθησαν.
- Τα λογικά αντίγραφα αποτυπώνουν τα δεδομένα της βάσης σε μορφή που αντικατοπτρίζει τη λογική τους δομή, χωρίς να αποτυπώνουν τον επακριβή τρόπο αποθήκευσης των δεδομένων στους δίσκους, απαιτούν περισσότερο χρόνο για να ληφθούν και η αποκατάστασή τους διαρκεί περισσότερο. Μπορούν να λαμβάνονται κατά την διάρκεια λειτουργίας της βάσης δεδομένων και μπορούν να λειτουργήσουν και σε συστήματα «ανόμοια» προς αυτό από το οποίο ελήφθησαν.

Τέλος, η διαθεσιμότητα των πληροφοριών επίσης μία σημαντική διάσταση που ορίζει ότι τα δεδομένα πρέπει να είναι πάντα διαθέσιμα στους εξουσιοδοτημένους χρήστες. Για το λόγο αυτό σε τακτά χρονικά σημεία, πρέπει να διενεργούνται στη βάση δεδομένων έλεγχοι ορθότητας (audits) για εντοπισμό πιθανών προβλημάτων. Οι έλεγχοι αυτοί πρέπει να είναι κατά το δυνατόν λεπτομερείς και διεξοδικοί χωρίς να επηρεάζεται την απόδοση του συστήματος.

3.8.4 Προστασία Δικτύων Υπολογιστικών Συστημάτων

Βασική προϋπόθεση για ορθή υλοποίηση της πολιτικής ασφαλείας μιας εταιρείας είναι ότι θα πρέπει να διασφαλίζει την ασφάλεια των δικτύων των υπολογιστικών συστημάτων της εταιρείας. Τα δίκτυα της εταιρείας συνίσταται από τη διασύνδεση δυο ή περισσοτέρων υπολογιστικών συστημάτων κατά τρόπο ώστε να παρέχεται η δυνατότητα στους χρήστες να επωφελούνται από ολόκληρο το υπολογιστικό δυναμικό. Αυτό πραγματοποιείται μέσω της ανταλλαγής πληροφοριών μεταξύ των χρηστών και της κοινής χρήσης των διαθέσιμων υπολογιστικών πόρων. Για αυτό το λόγο η εταιρεία πρέπει να προνοεί και για την προστασία από απειλές των δικτύων της.

Η διασύνδεση ενός εταιρικού δικτύου με το Διαδίκτυο ή άλλα εξωτερικά μη έμπιστα δίκτυα, καθιστά ολόκληρη την εταιρική πληροφορική υποδομή ευάλωτη σε μια σειρά από απειλές που

δύναται να προσβάλλουν την ασφάλεια της επιχείρησης. Για αυτό τον λόγο συνίσταται η χρήση πρωτόκολλων για ασφαλή επικοινωνία όπως το HTTPS και SSL.

Η χωρίς προστασία παροχή υπηρεσιών επιτρέπει την εκμετάλλευση πιθανών υπαρκτών αδυναμιών από τρίτους, με σκοπό την παραβίαση της ασφάλειας. Για το λόγο αυτό, κρίνεται απαραίτητη η υλοποίηση εξειδικευμένων μηχανισμών ασφάλειας όπως Firewall, Web Access Systems, Mail Security Systems, Network IPS/IDS.

Η εταιρεία εξασφαλίζει την προστασία των δικτύων της μέσω ενός ολοκληρωμένου πακέτου ασφαλείας το End Point Security System, το οποίο στοχεύει στην υλοποίηση υπηρεσιών ασφάλειας στην πύλη του δικτύου (Gateway Security) από και προς το διαδίκτυο.

Οι βασικές υπηρεσίες είναι:

- Firewall
- Antivirus
- Antisyare
- Antispam
- URL Filtering
- DMZ (De Military Zone)
- Intrusion Detection / Prevention Systems

3.8.5 Παραδείγματα Πρωτόκολλων Ασφαλής Επικοινωνίας

Απαραίτητο μέτρο για ασφαλή σύνδεση και ανταλλαγή πληροφοριών ιδίως μέσω διαδικτύου είναι η χρήση και εφαρμογή πρωτόκολλων για ασφαλή επικοινωνία. Τα πρωτόκολλα αυτά παρέχουν επιπλέον ασφάλεια στην διακίνηση πληροφοριών μέσω δικτύων και στηρίζονται κυρίως στη μέθοδο της κρυπτογράφησης.

3.8.5.1 Πρωτόκολλο HTTPS (Secure HTTP)

Το σύστημα αυτό σχεδιάστηκε αρχικά από την εταιρία Netscape Communications Corporation για να χρησιμοποιηθεί σε sites όπου απαιτείται αυθεντικοποίηση χρηστών και κρυπτογραφημένη επικοινωνία. Σήμερα χρησιμοποιείται ευρέως στο διαδίκτυο όπου χρειάζεται αυξημένη ασφάλεια διότι διακινούνται ευαίσθητες πληροφορίες. Το HTTPS δεν είναι ξεχωριστό πρωτόκολλο όπως μερικοί νομίζουν, αλλά αποτελεί συνδυασμό του απλού HTTP πρωτοκόλλου και των δυνατοτήτων κρυπτογράφησης που παρέχει το πρωτόκολλο Secure Sockets Layer (SSL). Η κρυπτογράφηση που χρησιμοποιείται διασφαλίζει ότι τα κρυπτογραφημένα δεδομένα δεν θα μπορούν να υποκλαπούν από άλλους κακόβουλους χρήστες ή από επιθέσεις man-in-the-middle.

Για να χρησιμοποιηθεί το HTTPS σε έναν εξυπηρετητή (server), θα πρέπει ο διαχειριστής του να εκδώσει ένα πιστοποιητικό δημοσίου κλειδιού. Στην συνέχεια το πιστοποιητικό αυτό θα πρέπει να υπογραφεί από μία αρχή πιστοποίησης (certificate authority), η οποία πιστοποιεί ότι ο εκδότης του πιστοποιητικού είναι νομότυπος και ότι το πιστοποιητικό είναι έγκυρο. Με τον τρόπο αυτό οι χρήστες μπορούν να δουν την υπογραφή της αρχής πιστοποίησης και να βεβαιωθούν ότι το πιστοποιητικό είναι έγκυρο και ότι κανένας κακόβουλος χρήστης δεν το έχει πλαστογραφήσει.

Όπως αναφέρθηκε προηγουμένως, το HTTPS χρησιμοποιείται κυρίως όταν απαιτείται μεταφορά ευαίσθητων προσωπικών δεδομένων. Το επίπεδο προστασίας των δεδομένων εξαρτάται από το πόσο σωστά έχει εφαρμοστεί η διαδικασία ασφάλειας και από το πόσο ισχυροί είναι οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται.

Όσον αφορά την χρήση και τις συναλλαγές μέσω πιστωτικών καρτών, πολλοί χρήστες θεωρούν ότι το HTTPS προστατεύει ολοκληρωτικά τον αριθμό της πιστωτικής τους κάρτας από κατάχρηση, αυτό όμως δεν ισχύει. Το HTTPS χρησιμοποιεί την κρυπτογράφηση για να μεταδώσει τον αριθμό από τον υπολογιστή του πελάτη προς τον εξυπηρετητή. Η μετάδοση είναι ασφαλής και τα δεδομένα φτάνουν στον εξυπηρετητή χωρίς κανείς να μπορέσει να τα υποκλέψει. Παρόλα αυτά υπάρχει το ενδεχόμενο διάφοροι χάκερ να έχουν επιτεθεί στον εξυπηρετητή και από εκεί να έχουν υποκλέψει τα ευαίσθητα προσωπικά δεδομένα.

3.8.5.2 Πρωτόκολλο SSL (Secure Sockets Layer)

Το πρωτόκολλο SSL αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από την Netscape το 1996 και αποτέλεσε την βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security), το οποίο πλέον τείνει να αντικαταστήσει το SSL. Τα δύο αυτά πρωτόκολλα χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου.

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP, το telnet κοκ.

Το SSL προσφέρει συνοπτικά τις ακόλουθες υπηρεσίες:

- Πιστοποίηση του server από τον client.
- Πιστοποίηση του client από τον server

- Εγκαθίδρυση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών.

Ένα μειονέκτημα της χρήσης του πρωτοκόλλου SSL είναι ότι αυξάνει τα διακινούμενα πακέτα μεταξύ των δύο μηχανών και συνεπώς καθυστερεί την μετάδοση των πληροφοριών επειδή χρησιμοποιεί μεθόδους κρυπτογράφησης και αποκρυπτογράφησης. Ειδικότερα οι διάφορες καθυστερήσεις εντοπίζονται στα εξής σημεία:

Στην αρχική διαδικασία χειραψίας όπου κανονίζονται οι λεπτομέρειες της σύνδεσης και ανταλλάσσονται τα κλειδιά της συνόδου.

Στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης που γίνεται στους δύο υπολογιστές με αποτέλεσμα να δαπανώνται υπολογιστικοί πόροι και χρόνος.

Στην καθυστέρηση μετάδοσης των κρυπτογραφημένων δεδομένων αφού αυτά αποτελούνται από περισσότερα bytes σε σχέση με την αρχική μη κρυπτογραφημένη πληροφορία.

Λόγω αυτών των επιβαρύνσεων που εισάγει το πρωτόκολλο SSL, χρησιμοποιείται πλέον μονάχα σε περιπτώσεις όπου πραγματικά χρειάζεται ασφαλής σύνδεση (πχ μετάδοση κωδικών χρήστη ή αριθμών πιστωτικών καρτών μέσω του διαδικτύου) και όχι σε περιπτώσεις απλής επίσκεψης σε μία ιστοσελίδα.

3.8.5.3 End point Security Systems

Αποτελεί πολύ βασικό μέτρο για την ασφάλεια των συστημάτων της εταιρείας. Στόχος του πακέτου αυτού είναι να προστατεύει όλους τους υπολογιστές και τα δεδομένα της εταιρείας, να ελέγχει τις εξωτερικές συσκευές και τις εφαρμογές καθώς και την πρόσβαση στο δίκτυο, παρέχοντας στην εταιρεία ασφάλεια και συμβατότητα με τις κανονιστικές ρυθμίσεις και εσωτερικές πολιτικές.

Επίσης ασφαλίζει τους υπολογιστές και τα ευαίσθητα δεδομένα με τεχνολογίες anti-virus, anti-spyware και firewall.

Ελαχιστοποιεί τις επιπτώσεις στους υπολογιστές προσφέροντας προστασία δεδομένων και προστασία από ιούς και malware.

Ελέγχει αυτόματα τόσο τους υπολογιστές υπό διαχείριση, όσο και τους ''άγνωστους'' υπολογιστές επισκεπτών για τυχόν μη ενημερωμένα προγράμματα ασφάλειας, πριν αποκτήσουν πρόσβαση στο δίκτυο.

Σταματά τους hackers με το ενσωματωμένο client firewall που υποστηρίζει κεντρική διαχείριση και είναι ενσωματωμένο στον anti-virus agent. Και γενικότερα βοηθά στην αύξηση της παραγωγικότητας των συστημάτων χωρίς να τα επιβραδύνει, ή να καταλύει πόρους του συστήματος. Η εταιρεία για την ακρίβεια χρησιμοποιεί το Synematic Endpoint Protection 11.

3.8.5.4 Firewall

Το firewall είναι απαραίτητο μέτρο προστασίας των δικτύων και των συστημάτων ης εταιρείας. Τα firewalls μπορεί να ενσωματώνουν όλες τις υπηρεσίες Antivirus, URL Filtering, Antispam κλπ. καθότι μπορούν να περιλαμβάνουν πλήθος των χαρακτηριστικών ασφάλειας τους σε ένα σύνολο που ονομάζεται UTM (Unified Threat Management)

Το firewall μπορεί να είναι εκτός από software και hardware, μια συσκευή δηλαδή που τοποθετείται στην σύνδεση του ηλεκτρονικού υπολογιστή με το διαδίκτυο. Επίσης μέσω αυτών μπορεί να καθορίσει ποίοι υπολογιστές και με ποιόν τρόπο θα ανταλλάσσουν πληροφορίες. Αυτό επιτυγχάνεται με την χρήση διάφορων φίλτρων τα οποία αναλύουν τα εισερχόμενα πακέτα και ανάλογα με τις οδηγίες που υπάρχουν τα αφήνουν να περάσουν ή όχι. Η μεγάλη σημασία του firewall έγκειται στο ότι συγκεντρώνει τον πλήρη έλεγχο των πακέτων που εισέρχονται στον υπολογιστή αποτελώντας ουσιαστικά έναν πύργο ελέγχου της πληροφορίας.

Επίσης, με το firewall η εταιρεία μπορεί να προλαμβάνει πιθανές εισβολές στο δίκτυό της όπως από:

- Απομακρυσμένη Είσοδος (Remote login): Με απομακρυσμένο έλεγχο μπορεί κάποιος να εισβάλει σε κάποιον υπολογιστή και να τον ελέγχει με οποιαδήποτε μορφή. Αυτό μπορεί να ποικίλει ανάλογα με το πόσο εύκολη είναι η πρόσβαση στα δεδομένα του υπολογιστή και σε ποια δεδομένα μπορεί να έχει πρόσβαση.
- Εφαρμογές backdoors (Application backdoors): Κάποια προγράμματα έχουν τη δυνατότητα απομακρυσμένου ελέγχου και πρόσβασης ή μπορεί να έχουν κάποιες «τρύπες» στο λογισμικό τους τις οποίες να εκμεταλλεύονται κακόβουλα κάποιοι για να εισβάλουν παράνομα στον υπολογιστή που θέλουν.
- Βομβαρδισμοί με e-mail (E-mail bombs): Πρόκειται για προσωπική-ατομική επίθεση κατά την οποία αποστέλλονται στον ίδιο παραλήπτη(mail server ή e-mail) εκατοντάδες ηλεκτρονικά μηνύματα με αποτέλεσμα το σύστημα να μη μπορεί να δεχτεί άλλα και έτσι να υπολειτουργεί ή να καταρρέει κάνοντας έτσι πιο εύκολη τη πρόσβαση στον υπολογιστή ή στο δίκτυο.
- Μακροεντολές (Macros): Κάποια προγράμματα για να απλοποιηθούν ορισμένες λειτουργίες τους επιτρέπουν τη σύνταξη μακροεντολών. Οι χάκερς εκμεταλλεύονται αυτή την ιδιότητα των προγραμμάτων και δημιουργούν τις δικιές τους μακροεντολές κάνοντας έτσι τη πρόσβασή τους στο σύστημα εύκολη υπόθεση.
- Ιοί (Viruses): Ίσως η πιο γνωστή απειλή των υπολογιστών στις μέρες μας. Οι ιοί είναι μικρές συνήθως εφαρμογές οι οποίες έχουν την ικανότητα να δημιουργούν κλώνους και με αυτό τον τρόπο να εξαπλώνονται γρήγορα από υπολογιστή σε υπολογιστή. Έχουν την ικανότητα να

«κρύβονται» μέσα σε άλλα προγράμματα ή να εγκαθίστανται σε αυτά. Οι ιοί μπορούν να προκαλέσουν μια μικρή ζημιά μέχρι και την ολική απώλεια των δεδομένων του συστήματος.

- Spam: Είναι τα ενοχλητικά e-mail, όπως τα διαφημιστικά, τα οποία από μόνα τους συνήθως δεν αποτελούν απειλή. Συνήθως περιέχουν υπερσυνδέσεις από άλλες σελίδες οι οποίες όμως μπορεί να σου μεταφέρουν ιούς.

3.8.5.5 Λογισμικό Antivirus

Στόχος του Antivirus είναι να ανιχνεύονται όλα τα αρχεία ή η μνήμη του υπολογιστή για αρχεία που μπορεί να έχουν κάποιον ιό. Τα αρχεία που ψάχνει είναι βασισμένα στις υπογραφές, ή τους ορισμούς, των γνωστών ιών. Ένας από τους τρόπους κατηγοριοποίησης των μηχανισμών Antivirus είναι ο ακόλουθος:

- Λογισμικό που εγκαθίσταται στους Servers ή στους Η/Υ και αφενός δεν επιτρέπει τη μόλυνση από κακόβουλο κώδικα, αφενός καθαρίζει τυχόν ήδη μολυσμένους Η/Υ
- Λογισμικό που εγκαθίσταται στη είσοδο ενός δικτύου (mail servers, proxy servers κλπ.) και ελέγχει την κίνηση που διέρχεται μέσω αυτών από και προς τους Η/Υ
- Συσκευές που διαθέτουν φίλτρα ελέγχου και λειτουργούν ως Gateways του δικτύου.

Συνήθως, αναλόγως του μεγέθους του δικτύου υλοποιείται ένας συνδυασμός των ανωτέρω λύσεων και γενικότερα συνίσταται η ενσωμάτωση μηχανισμών ελέγχου σε όλα τα σημεία πιθανής εισόδου ιών.

3.8.5.6 Λογισμικό Antispyware

Είναι ένας μηχανισμός που αποτρέπει τη μόλυνση του Η/Υ με προγράμματα που ελέγχουν και καταγράφουν τον τρόπο χρήσης του. Επίσης τα προγράμματα Spyware καταναλώνουν το εύρος (bandwidth) της σύνδεσης με το διαδίκτυο.

Υπάρχουν δύο τρόποι υλοποίησης που μπορούν να λειτουργούν παράλληλα.

- Ο ένας, είναι η υλοποίηση του μηχανισμού Antispyware στη πύλη δικτύου (Gateway) συνήθως με την εγκατάσταση κατάλληλης συσκευής που λειτουργεί ως διακομιστής μεσολάβησης (proxy).
- Ο άλλος τρόπος, είναι η υπηρεσία να υπάρχει στον κάθε ένα Η/Υ του δικτύου.

Καθώς η συντριπτική πλειοψηφία των περιπτώσεων μόλυνσης με Spyware γίνεται από επίσκεψη σε ακατάλληλα sites, οι υπηρεσία Antispyware τείνει να ταυτιστεί με την υπηρεσία URL Filtering και ενίοτε να προσφέρεται από τον ίδιο μηχανισμό.

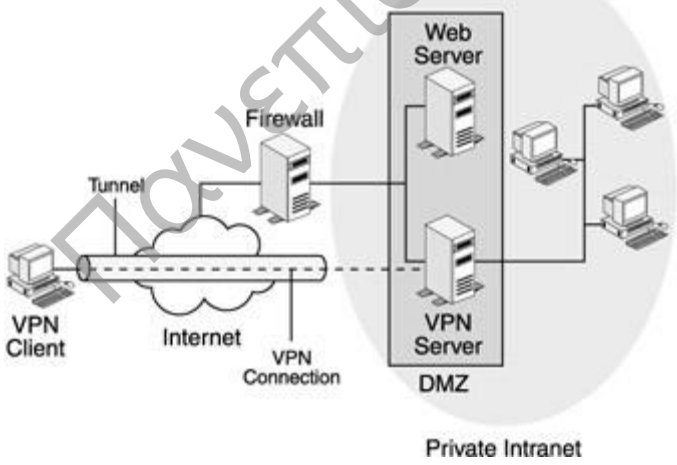
3.8.5.7 Λογισμικό Antispam

Το Antispam είναι πλέον απαραίτητο για την ασφαλή και παραγωγική χρήση των emails, ενώ όπως όλα δείχνουν το πρόβλημα του spam θα συνεχίσει να εντείνεται. Για αυτό το λόγο διατίθενται πολλοί μηχανισμοί και τεχνολογίες για την αντιμετώπισή του. Ο πιο οικονομικός, αλλά και αποτελεσματικός τρόπος είναι η παροχή υπηρεσίας Antispam μέσω των μηχανισμών firewall.

Βασικό μειονέκτημα αυτών των λύσεων είναι ότι δεν έχουν πληρότητα παραμετροποίησης ώστε η λειτουργία του Antispam να προσαρμοστεί στις ανάγκες του δικτύου. Αντίστοιχης αποτελεσματικότητας και κόστους λύσεις είναι και αυτές που υλοποιούν ελέγχους Antispam στα mails πριν φτάσουν στο εταιρικό δίκτυο. Και πάλι δεν προσφέρονται πλήρεις δυνατότητες παραμετροποίησης της υπηρεσίας.

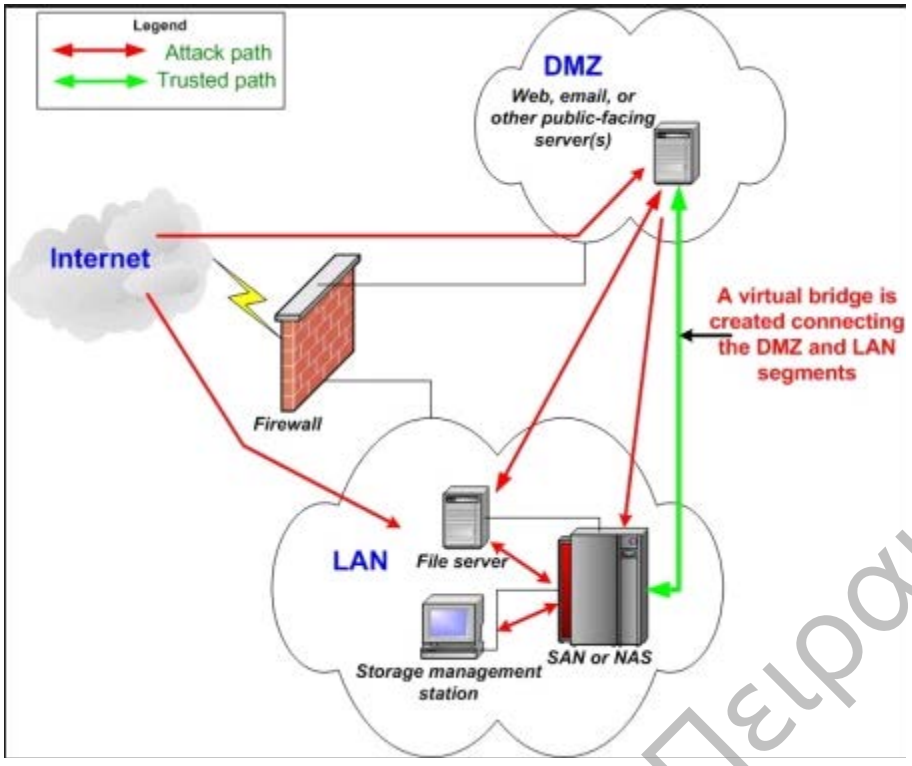
3.8.5.8 DMZ (De Militirized Zone)

Το DMZ σημαίνει DeMilitirised Zone και είναι χαρακτηριστικό ενός hardware firewall. Σε ένα hardware firewall υπάρχουν τρείς κάρτες δικτύου (interfaces). Στη μία συνδέεται το εσωτερικό δίκτυο της εταιρίας και εκεί υπάρχουν όλοι οι χρήστες. Στη δεύτερη συνδέεται το internet. Το firewall ελέγχει τι εισέρχεται και τι εξέρχεται μεταξύ των δύο αυτών θέσεων, δηλαδή μεταξύ του Internet και του εσωτερικού δικτύου. Χρειάζεται όμως και μία τρίτη θέση για παράδειγμα για να μπορούν οι χρήστες από το internet να έχουν πρόσβαση σε κάποια δεδομένα της εταιρείας, μέσα από το site της, χωρίς όμως να έχουν οποιαδήποτε σχέση με τη εσωτερικό δίκτυό της.



Εικόνα 1: Παράδειγμα αρχιτεκτονικής DMZ (De Militirized Zone)

Γενικά το DMZ χρησιμοποιείται για να εφαρμοστεί μια πολιτική ασφαλείας όσον αφορά τα δίκτυα της εταιρείας. Στην ουσία το DMZ λειτουργεί ως απομονωτής μεταξύ των ασφαλών τοπικών δικτύων της εταιρείας και του Διαδικτύου.

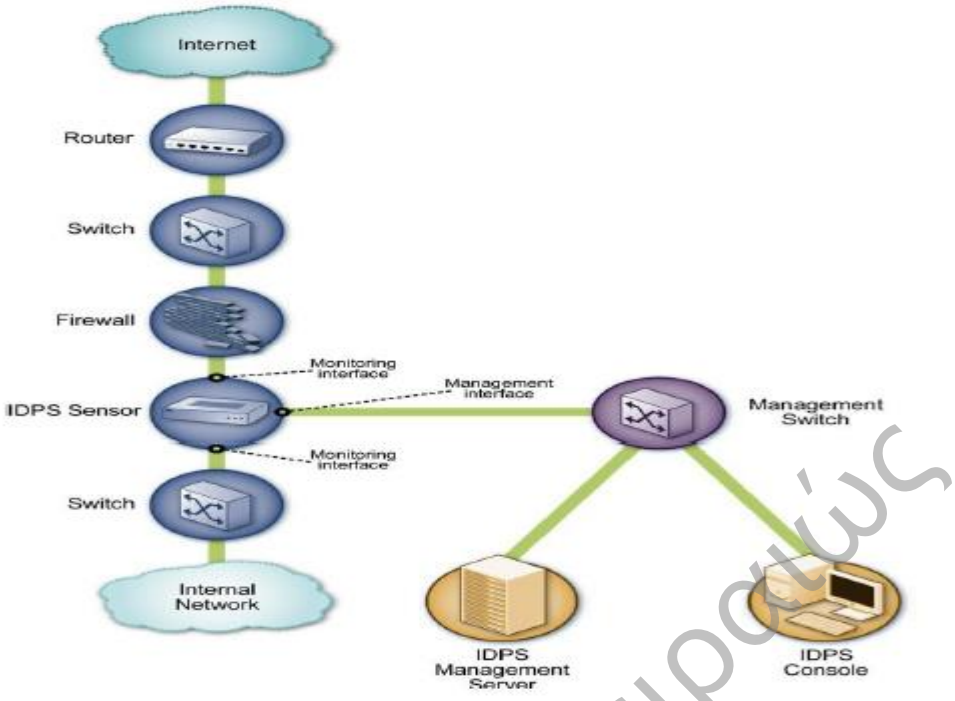


Εικόνα 2: DMZ (De Militirized Zone)

3.8.5.9 IDS/IPS (Introdusion Detective/Prevention System)

Για επιπλέον ασφάλεια στο δίκτυο συνίσταται η χρήση IDS/IPS συστημάτων, είναι μηχανισμός προστασίας που αποτρέπει δικτυακές επιθέσεις και επιθέσεις σε επίπεδο εφαρμογής όπως worms, Trojans, spyware, keyloggers κλπ. Η λειτουργία τους βασίζεται σε ενσωματωμένα φίλτρα ελέγχου (zero day protection) και σε σύγκριση της ενδεχόμενης απειλής με ήδη γνωστές απειλές (signature & pattern matching). Για την ακρίβεια το σύστημα αυτό εντοπίζει πιθανές διεισδύσεις, στόχος του είναι η ανίχνευση επιθέσεων κατά του υπολογιστή ή την κακή χρήση του υπολογιστή και ειδοποίηση των αρμόδιων ατόμων όταν ανιχνευτεί κάτι περίεργο. Η εγκατάσταση ενός IDS σε ένα δίκτυο παρέχει το ίδιο αποτέλεσμα με την εγκατάσταση ενός συναγερμού σε ένα σπίτι.

Με διάφορες μεθόδους και τα δύο ανιχνεύουν την παρουσία ενός εισβολέα/διαρρήκτη και τα δύο στη συνέχεια εκδίδουν κάποιο είδος προειδοποίησης και συναγερμού.



Εικόνα 3: Παράδειγμα αρχιτεκτονικής αισθητήρων IDPS

Η διαφορά τους από τις τεχνολογίες των Firewall είναι ότι τα IPS συστήματα ελέγχουν την πρόσβαση σε επίπεδο εφαρμογής, πέρα από τη διεύθυνση IP ή τις πόρτες. Πολλαπλές μελέτες έχουν δείξει ότι παραδοσιακοί μηχανισμοί ασφάλειας (π.χ. Firewalls) μπορούν να παρακαμφθούν λόγω ύπαρξης / παρουσίασης αδυναμιών. Ένα σφάλμα, ελάττωμα, σφάλμα προγραμματισμού ή ακόμη μια λανθασμένη παραμετροποίηση μπορεί να γίνει αντικείμενο εκμετάλλευσης από χάκερς ή από κάποιο κακόβουλο πρόγραμμα, και παράνομα να αποκτηθεί πρόσβαση σε δίκτυα ηλεκτρονικών υπολογιστών.

Προτείνεται λοιπόν, ένα σύστημα ανίχνευσης και αποτροπής εισβολέων το οποίο παρακολουθεί την εξωτερική και εσωτερική κίνηση ενός δικτύου, με σκοπό την έγκαιρη ανίχνευση πιθανών επιθέσεων και την αποτροπή τους πριν την είσοδο τους στο εσωτερικό δίκτυο και τα συστήματα του οργανισμού.

Το εργαλείο αυτό αποτελεί αναπόσπαστο μέρος της λεπτομερούς και πλήρης ασφάλειας του συστήματος. Δεν εγγυάται πλήρως την ασφάλεια αλλά όταν συνδυαστεί με την πολιτική ασφαλείας τρωτών σημείων, την κρυπτογράφηση δεδομένων, την ταυτοποίηση του χρήστη, τον έλεγχο πρόσβασης και τα τείχη προστασίας, μπορεί να ενισχύσει σημαντικά την ασφάλεια του δικτύου.

ΚΕΦΑΛΑΙΟ 4

4.1 Το σύστημα υγείας στην Ελλάδα

4.1.1 Η έννοια της κοινωνικής ασφάλειας στην Ελλάδα

Η έννοια της κοινωνικής ασφάλειας στην Ελλάδα αντιστοιχεί στον κύριο στόχο του εθνικού μοντέλου κοινωνικής προστασίας, ο οποίος εξυπηρετείται μέσω τριών συστημάτων: του συστήματος κοινωνικής ασφάλισης για την προστασία των εργαζομένων, του συστήματος κοινωνικής πρόνοιας για την φροντίδα των ατόμων που βρίσκονται σε κατάσταση ανάγκης και του εθνικού συστήματος υγείας για την κάλυψη όλων των ατόμων που διαμένουν στην Ελληνική επικράτεια. Από διοικητική άποψη, το σύστημα κοινωνικής ασφάλισης συντονίζεται και εποπτεύεται κατά κύριο λόγο από το Υπουργείο Εργασίας και Κοινωνικών Ασφαλίσεων, ενώ τα συστήματα υγείας και πρόνοιας συντονίζονται από το Υπουργείο Υγείας και Κοινωνικής Αλληλεγγύης .

Το Σύστημα Κοινωνικής Ασφάλισης αποτελεί τον κύριο άξονα του Ελληνικού μοντέλου κοινωνικής προστασίας. Η λειτουργία του, όπως έχει διαμορφωθεί ιστορικά από τη δεκαετία του 1950 μέχρι σήμερα, επιδιώκει την κάλυψη των κινδύνων που αντιμετωπίζουν οι εργαζόμενοι, χορηγώντας παροχές και υπηρεσίες που αναπληρώνουν τη μείωση ή την απώλεια εισοδήματος από απασχόληση. Πρόκειται για ένα σύστημα κύριας και επικουρικής δημόσιας ασφάλισης, το οποίο λειτουργεί με βάση αυτόνομους ασφαλιστικούς φορείς. Οι φορείς αυτοί συγκροτούν τον πρώτο πυλώνα ασφάλισης στην Ελλάδα.

Ο δεύτερος και ο τρίτος πυλώνας ασφάλισης δεν είναι ιδιαίτερα αναπτυγμένοι σε σχέση με την εφαρμογή τους σε άλλα Κράτη μέλη της Ευρωπαϊκής Ένωσης. Πρόσφατα όμως η Ελληνική Κυβέρνηση προχώρησε στη θεσμική κατοχύρωση των επαγγελματικών ταμείων, τα οποία αναμένεται να συμβάλουν στη διεύρυνση του επιπέδου προστασίας του ασφαλιστικού συστήματος και στη βελτίωση των ασφαλιστικών παροχών, αποτελώντας ουσιαστικά το δεύτερο πυλώνα ασφάλισης.

Το Εθνικό Σύστημα Υγείας θεσμοθετήθηκε μόλις στις αρχές της δεκαετίας του 1980, αποβλέποντας στην ιατροφαρμακευτική και νοσηλευτική κάλυψη των αναγκών του ελληνικού πληθυσμού μέσω της παροχής δωρεάν υπηρεσιών. Η λειτουργία του εξυπηρετεί όλα τα άτομα που διαμένουν στην Ελληνική επικράτεια. Ειδικά όμως για τους ασφαλισμένους σε φορείς δημόσιας ασφάλισης προβλέπεται η παροχή υπηρεσιών υγείας και από τους κλάδους υγείας των ταμείων τους. Η Κυβέρνηση προωθεί την περίοδο αυτή συγκεκριμένα μέτρα εκσυγχρονισμού των δημόσιων πολιτικών υγείας.

Οι εκσυγχρονιστικές παρεμβάσεις στον τομέα της υγείας εγκαινιάστηκαν ουσιαστικά με την υιοθέτηση του Ν. 2519/1997 για την «Ανάπτυξη και εκσυγχρονισμό του Εθνικού Συστήματος Υγείας, οργάνωση των υγειονομικών υπηρεσιών, ρυθμίσεις για το φάρμακο και άλλες διατάξεις» και

συνεχίζονται κατά τη διάρκεια της δεκαετίας του 2000 με την υιοθέτηση του Ν. 2889/2001 «Βελτίωση και εκσυγχρονισμός του Εθνικού Συστήματος Υγείας και άλλες διατάξεις» και του Ν. 2955/2001 «Προμήθειες Νοσοκομείων και λοιπών μονάδων υγείας των ΠεΣΥ και άλλες διατάξεις». Ο Ν.2889/01 εισήγαγε σημαντικές τροποποιήσεις στην οργανωτική διάρθρωση του συστήματος υγείας, καθώς προχώρησε στην ίδρυση των Περιφερειακών Συστημάτων Υγείας (ΠεΣΥ), τα οποία αποτελούν αποκεντρωμένα νομικά πρόσωπα δημοσίου δικαίου που εποπτεύουν όλα τα νοσηλευτικά ιδρύματα του ΕΣΥ. Τα ΠεΣΥ διέπονται από ένα ιδιαίτερο θεσμικό πλαίσιο το οποίο αποτυπώνεται στις ρυθμίσεις του Π.Δ. 357/2001 «Οργανισμός Κεντρικής Υπηρεσίας των Περιφερειακών Συστημάτων Υγείας (ΠεΣΥ)».

Το Σύστημα Κοινωνικής Πρόνοιας συνθέτει το τελικό δίκτυο ασφάλειας για τα άτομα εκτός αγοράς εργασίας που βρίσκονται σε κατάσταση ανάγκης. Λειτουργεί με βάση κατηγοριακά προγράμματα προστασίας για συγκεκριμένες ομάδες του πληθυσμού, τα οποία εγκαινιάστηκαν στις αρχές της δεκαετίας του 1960 και επεκτάθηκαν ουσιαστικά καθ'όλη τη διάρκεια της δεκαετίας του 1980. Το σύστημα χορηγεί χρηματικά επιδόματα, παροχές σε είδος και κοινωνικές υπηρεσίες φροντίδας μέσω αποκεντρωμένων νομικών προσώπων που εποπτεύονται από το Υπουργείο Υγείας και Κοινωνικής Αλληλεγγύης. Κοινωνικές υπηρεσίες σε μικρότερη έκταση παρέχονται επίσης από τους οργανισμούς τοπικής αυτοδιοίκησης και από ένα πλέγμα εθελοντικών οργανισμών και μη κυβερνητικών οργανώσεων που δραστηριοποιούνται έντονα ιδίως στο πεδίο προστασίας των παιδιών, των προσφύγων και των ατόμων με ειδικές ανάγκες.

Η θεσμοθέτηση ενός σύγχρονου Εθνικού Συστήματος Κοινωνικής Φροντίδας εξασφαλίστηκε το 1998 με την ψήφιση του Ν.2646/98 και προωθήθηκε το 2001 με την επεξεργασία του Εθνικού Σχεδίου Δράσης για την Κοινωνική Ενσωμάτωση 2001-2003. Ο Ν. 2646/98 θέτει τις βάσεις για τη δημιουργία ενός σύγχρονου μοντέλου προνοιακής παρέμβασης που αποβλέπει τόσο στην εξυπηρέτηση νέων αναγκών όσο και στον εξορθολογισμό της διοικητικής και οργανωτικής λειτουργίας των παραδοσιακών προνοιακών φορέων. Το μοντέλο αυτό στηρίζεται σε ένα ενιαίο και αποκεντρωμένο πλαίσιο που ενεργοποιείται μέσω της δράσης των φορέων του δημόσιου τομέα που εποπτεύονται από το Υπουργείο Υγείας και Κοινωνικής Αλληλεγγύης, των ιδιωτικών φορέων μη κερδοσκοπικού χαρακτήρα που αναγνωρίζονται ως ειδικώς πιστοποιημένοι φορείς του συστήματος και εγγράφονται στο αντίστοιχο μητρώο της οικείας Νομαρχιακής Αυτοδιοίκησης και των οργανώσεων εθελοντικού χαρακτήρα.

4.1.2 Η ιστορική εξέλιξη του συστήματος κοινωνικής ασφάλισης στο πλαίσιο λειτουργίας του Ελληνικού μοντέλου κοινωνικής ασφάλειας

Η κοινωνική ασφάλιση στην Ελλάδα πρωτοεμφανίζεται ως θεσμός με το διάταγμα της 15ης Δεκεμβρίου 1836, με το οποίο συστήθηκε το Ναυτικό Απομαχικό Ταμείο (ΝΑΤ), που όμως άρχισε να λειτουργεί από το 1861. Η νομοθετική κατοχύρωση του θεσμού εξασφαλίστηκε το 1922 με την ψήφιση του Ν. 2868/1922 «Περί υποχρεωτικής ασφαλίσεως των εργατών και ιδιωτικών υπαλλήλων». Ο νόμος αυτός αποτέλεσε τη βάση για την ίδρυση κατά τη διάρκεια του μεσοπολέμου κλαδικών ασφαλιστικών ταμείων.

Το 1934 ψηφίστηκε ο βασικός νόμος 6298/1934 «Περί Κοινωνικών Ασφαλίσεων». Την ίδια περίοδο προωθήθηκαν επίσης νομοθετικά μέτρα για την ίδρυση φορέων κύριας ασφάλισης, όπως του Ταμείου Ασφαλίσεως Εμπόρων (ΤΑΕ) και του Ταμείου Επαγγελματιών και Βιοτεχνών (ΤΕΒΕ), που άρχισαν να λειτουργούν το 1940.

Το 1935 καθιερώθηκε η υποχρεωτική ασφάλιση όλων των μισθωτών στο Ίδρυμα Κοινωνικών Ασφαλίσεων (ΙΚΑ), που αποτέλεσε το γενικό φορέα κοινωνικής ασφάλισης των μισθωτών. Η λειτουργία του ΙΚΑ άρχισε την 1.1.1937, αλλά η χορήγηση παροχών ρυθμίστηκε το 1951 με τον Αναγκαστικό Νόμο 1846/51, ο οποίος με τις διαδοχικές του τροποποιήσεις συνθέτει και το ισχύον θεσμικό πλαίσιο του φορέα.

Η επέκταση της ασφαλιστικής προστασίας του πληθυσμού εξασφαλίστηκε το 1961 με την ίδρυση του Οργανισμού Γεωργικών Ασφαλίσεων (ΟΓΑ), ο οποίος κάλυψε σχεδόν το σύνολο του αγροτικού πληθυσμού.

Κατά τη διάρκεια της δεκαετίας του 1990 προωθήθηκαν σημαντικές παρεμβάσεις για τη μεταρρύθμιση και τον εκσυγχρονισμό του συστήματος κοινωνικής ασφάλισης, οι οποίες ουσιαστικά ολοκληρώθηκαν το 2002 με την έκδοση του Ν. 3029/2002 για τη μεταρρύθμιση του συστήματος κοινωνικής ασφάλισης. Οι παρεμβάσεις αυτές επικεντρώθηκαν σε ζητήματα οργάνωσης, χρηματοδότησης και χορήγησης των ασφαλιστικών παροχών με έμφαση στις συνταξιοδοτικές παροχές.

Η μεταρρύθμιση του συστήματος κοινωνικής ασφάλισης αποτελεί έναν από τους κύριους στόχους εκσυγχρονισμού του ελληνικού μοντέλου κοινωνικής προστασίας. Συνδυάστηκε μάλιστα με εκτεταμένες παρεμβάσεις και στα άλλα συστήματα κοινωνικής κάλυψης στη χώρα μας, οι οποίες επιδιώκουν την αποκέντρωση του εθνικού συστήματος υγείας και την κατοχύρωση ενός σύγχρονου εθνικού συστήματος κοινωνικής φροντίδας.

4.2 Ε.Ο.Π.Υ.Υ

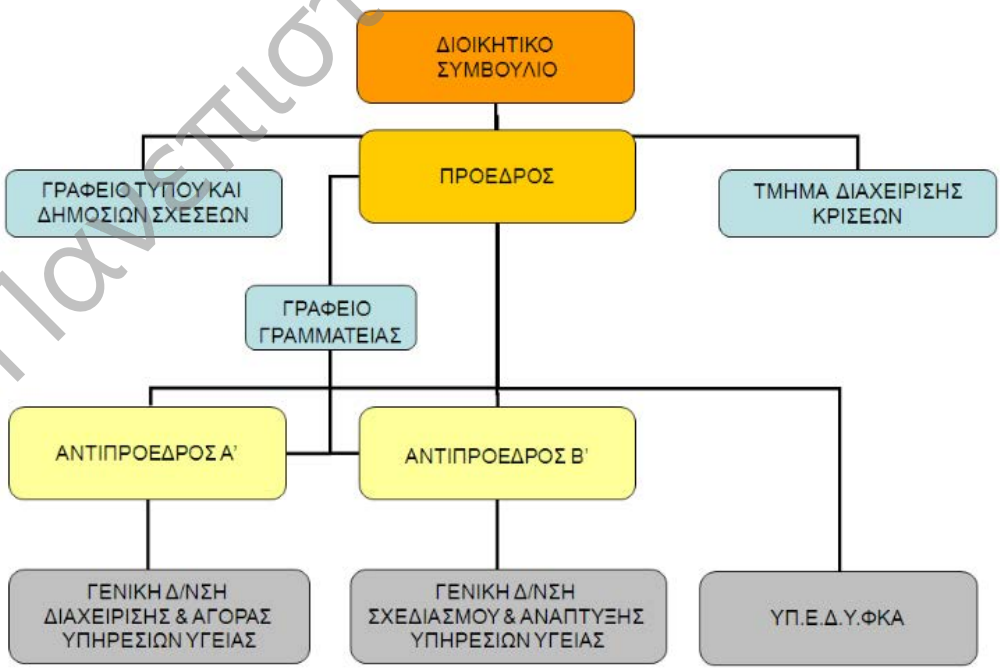
4.2.1 Ορισμός

Είναι ο Εθνικός Οργανισμός Παροχής Υπηρεσιών Υγείας, με φιλοδοξία να επαναφέρει τον ασφαλισμένο στο επίκεντρο των υπηρεσιών υγείας.

Συστήνεται ως νομικό πρόσωπο δημοσίου δικαίου υπό την εποπτεία των Υπουργείων Εργασία και Κοινωνικής Ασφάλισης και Υγείας και Κοινωνικής Αλληλεγγύης σύμφωνα με τον Ν. 3918/2011. Στο πλαίσιο αυτού του νόμου ορίζεται η μεταφορά και ένταξη στον οργανισμό σε επίπεδο υπηρεσιών , αρμοδιοτήτων αλλά και προσωπικού, του ιδρύματος Κοινωνικών Ασφαλίσεων – Ενιαίου Ταμείου Ασφάλισης Μισθωτών (Ι.Κ.Α-Ε.Τ.Α.Μ), του Οργανισμού Γεωργικών Ασφαλίσεων (Ο.Γ.Α), του Οργανισμού Ασφάλισης Ελεύθερων Επαγγελματιών (Ο.Α.Ε.Ε), καθώς και του Οργανισμού Περίθαλψης Ασφαλισμένων Δημοσίου (Ο.Π.Α.Δ.).

Αποστολή του οργανισμού είναι η παροχή υπηρεσιών υγείας σε ασφαλισμένους, συνταξιούχους και στα προστατευόμενα μέλη των οικογενειών τους, των παραπάνω μεταφερόμενων φορέων. Ορισμένες από τις παροχές υγείας είναι: η ιατρική περίθαλψη και οι διαγνωστικές ιατρικές πράξεις, οι παρακλινικές εξετάσεις, η φαρμακευτική περίθαλψη και η νοσοκομειακή περίθαλψη.

Ο Ε.Ο.Π.Υ.Υ διοικείται από τον πρόεδρο του οργανισμού, τους δύο (2) Αντιπροέδρους και το Διοικητικό Συμβούλιο (Δ.Σ). Στο σημείο αυτό παραθέτουμε το οργανόγραμμα του οργανισμού.



Εικόνα 4: Οργανόγραμμα του Ε.Ο.Π.Υ.Υ

Σύμφωνα με το παραπάνω σχήμα η κεντρική υπηρεσία του εν λόγω οργανισμού διακρίνεται στη Γενική Διεύθυνση Διαχείρισης και Αγοράς Υπηρεσιών Υγείας και την Υπηρεσία Ελέγχου Δαπανών Υγείας Φορέων Κοινωνικής Ασφάλισης, ή εν συντομία ΥΠ.Ε.Δ.Υ.Φ.Κ.Α. Σημειώνεται πως η τελευταία μεταφέρεται στον Ε.Ο.Π.Υ.Υ από την έναρξη της λειτουργίας του. Οι περιφερειακές Υπηρεσίες Υγείας των Ι.Κ.Α-Ε.Τ.Α.Μ, Ο.Γ.Α, Ο.Α.Ε.Ε και Ο.Π.Α.Δ εντάσσονται αργότερα (από την 1/1/2012) στον οργανισμό.

4.2.2 Σκοπός του Ε.Ο.Π.Υ.Υ

Με την δημιουργία του ΕΟΠΥΥ επιδιώκεται να εξασφαλισθεί η ισότιμη πρόσβαση όλων των ασφαλισμένων σε ενιαίο σύστημα παροχής υπηρεσιών υγείας, που έχει ως σκοπό την πρόληψη, διατήρηση, προαγωγή, βελτίωση, αποκατάσταση και προστασία της υγείας των δικαιούχων, όπου και όποτε τις έχουν ανάγκη.

4.3 Το φαρμακείο στην εποχή του διαδικτύου

Χαρακτηριστικά της εποχής μας είναι η ραγδαία ανάπτυξη της τεχνολογίας, η ευρεία χρήση του διαδικτύου. Αυτά έχουνε συμβάλλει στη βελτίωση της ποιότητας και της αποτελεσματικότητας των παρεχομένων υπηρεσιών υγείας.

Επίσης η αύξηση των δαπανών υγείας καθώς και η αύξηση της φαρμακευτικής δαπάνης είναι επιπλέον χαρακτηριστικά της εποχής μας τα οποία χρήζουν ιδιαίτερη προσοχή στη διαχείρισή τους.

4.3.1 Φαρμακευτική δαπάνη

Η φαρμακευτική δαπάνη των ασφαλιστικών ταμείων ανήλθε για το 2009 σε 5 δις
Ευρώ, ποσό που ισοδυναμεί με το 40% της ετήσιας κρατικής επιχορήγησης προς αυτά.

- Το ύψος της δαπάνης οφείλεται σε πολλούς παράγοντες. Ενδεικτικά αναφέρονται η κατευθυνόμενη, η προκλητή, η παράνομη συνταγογράφηση, η εικονική χρήση συνταγών ή η χρήση τους για άλλους σκοπούς.
- Το μερίδιο των παραπάνω στη δαπάνη ισοδυναμεί με το 20-25% του συνόλου της.
- Ο έλεγχός τους μέσω της ηλεκτρονικής συνταγογράφησης αναμένεται να προκαλέσει εξοικονομήσεις της τάξεως του 1 δις. Ευρώ κατά έτος.

Σύμφωνα με μια μελέτη του ΙΟΒΕ (Απρίλιος,2010) διαπιστώθηκε ότι η αύξηση των δαπανών υγείας οφείλεται στην υπερκατανάλωση των υπηρεσιών. Η Ελλάδα βρίσκεται σε χαμηλή θέση ως προς το δείκτη τιμών των φαρμακευτικών σκευασμάτων σε σύγκριση με τις άλλες Ευρωπαϊκές χώρες.

Η αύξηση της φαρμακευτικής δαπάνης πρέπει να αναζητηθεί στην κατανάλωση των φάρμακων και όχι στις τιμές τους.

Το φάρμακο είναι ένα προϊόν που κάποιοι το παράγουν και κάποιοι το καταναλώνουν.

Η ζήτηση του όμως έχει 4 στάδια:

- Ο γιατρός συνταγογραφεί
- Ο φαρμακοποιός εκτελεί
- Ο ασθενής καταναλώνει
- Ο ασφαλιστικός φορέας πληρώνει

Εδώ πρέπει να σημειωθεί ότι ο αγοραστής (ασφαλιστικός φορέας) και ο καταναλωτής (ασθενής) του φαρμάκου δεν έχουν καμία σχέση με την επιλογή του φαρμάκου, αφού αυτή γίνεται από τον πελάτη (γιατρό) έτσι λοιπόν πρέπει να βρεθούν μέθοδοι ελέγχου της συνταγογράφησης.

Η συνταγογράφηση είναι η πιο κοινή ιατρική πράξη.

Σύμφωνα με μελέτη του Wang et. al (2009), στη Μεγάλη Βρετανία 1,5 εκατομμύρια συνταγές γράφονται από επιστήμονες υγείας την ημέρα και υπολογίζεται ότι ο αριθμός αυτός θα αυξάνεται 5% κάθε χρόνο.

Στις Ηνωμένες Πολιτείες Αμερικής 4 στους 5 πολίτες που επισκέπτονται το γιατρό φεύγουν με μια συνταγή.

Σύμφωνα με τη μελέτη του Alkensee et. al. (2008) το 2007 γράφτηκαν 3,5 δισεκατομμύρια συνταγές και το 2010 4,5-5 δισεκατομμύρια συνταγές.

Σύμφωνα με τα παραπάνω το συμπέρασμα είναι ότι η ανεξέλεγκτη συνταγογράφηση οδηγεί σε αύξηση της φαρμακευτικής δαπάνης.

Η συνταγογράφηση μπορεί να ελεγχθεί σύμφωνα με τον ΙΟΒΕ (Απρίλιος,2010) με:

- Εφαρμογή θεραπευτικών πρωτοκόλλων
- Ηλεκτρονική συνταγογράφηση
- Εξέταση της εφαρμογής διπλής τιμής των φαρμάκων δηλαδή καθιέρωση ασφαλιστικής τιμής ως ποσοστό της ελεύθερης τιμής.
- Λίστα συνταγογραφούμενων φαρμάκων
- Την αλλαγή του τρόπου τιμολόγησης των γενόσημων.
- Την διαμόρφωση της αποζημίωσης των νοσηλευτικών ιδρυμάτων με βάση διαγνωστικές κατηγορίες

Στα πλαίσια της τεχνολογικής εξέλιξης και ως αποτέλεσμα των παραπάνω διαπιστώσεων και αναγκών δημιουργήθηκε ο φορέας Η.ΔΙ.Κ.Α (Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλειας).

4.4 Ο Η.ΔΙ.Κ.Α. Α.Ε. (πρώην Κ.Η.Υ.Κ.Υ.)

Είναι φορέας παροχής Υπηρεσιών Πληροφορικής. Έχει κοινωφελή χαρακτήρα, σκοπός της είναι η πληροφορική εξυπηρέτηση των φορέων κοινωνικής ασφάλισης και υγείας. Λειτουργεί σαν ανώνυμη εταιρία, μη κερδοσκοπικού χαρακτήρα Εποπτεύεται από την ΓΓΚΑ(Γενική Γραμματεία Κοινωνικών Ασφαλίσεων).

Ο Η.ΔΙ.Κ.Α. Α.Ε είναι ΔΕΚΟ με αποστολή να παρέχει ολοκληρωμένες λύσεις υψηλής ποιότητας στον τομέα της πληροφορικής και επικοινωνιών, οι οποίες θα υποστηρίζουν την ορθή, πλήρη και αποτελεσματική λειτουργία των φορέων κοινωνικής ασφάλισης και παροχής υγείας σε βάθος χρόνου και την εξυπηρέτηση των πολιτών, μέσω της παροχής σύγχρονων ηλεκτρονικών υπηρεσιών και πληροφοριών. Είναι βάσει νόμου υπεύθυνη για την λειτουργία της Ηλεκτρονικής Συνταγογράφησης στην Ελλάδα. Λειτουργεί ήδη με επιτυχία και είναι το πρώτο εθνικής εμβέλειας πιλοτικό σύστημα Η.Σ.

4.4.1 Η.ΔΙ.Κ.Α. και Ηλεκτρονική Συνταγογράφηση

Τον Οκτώβριο 2010 – Μάιο 2012 ξεκίνησαν οι πιλοτικές εφαρμογές του συστήματος Ηλεκτρονικής Συνταγογράφησης. Από το Μάιο του 2012 η εφαρμογή της ηλεκτρονικής συνταγογράφησης λειτουργεί στην ΗΔΙΚΑ.

Ο ρόλος της ΗΔΙΚΑ περιλαμβάνει:

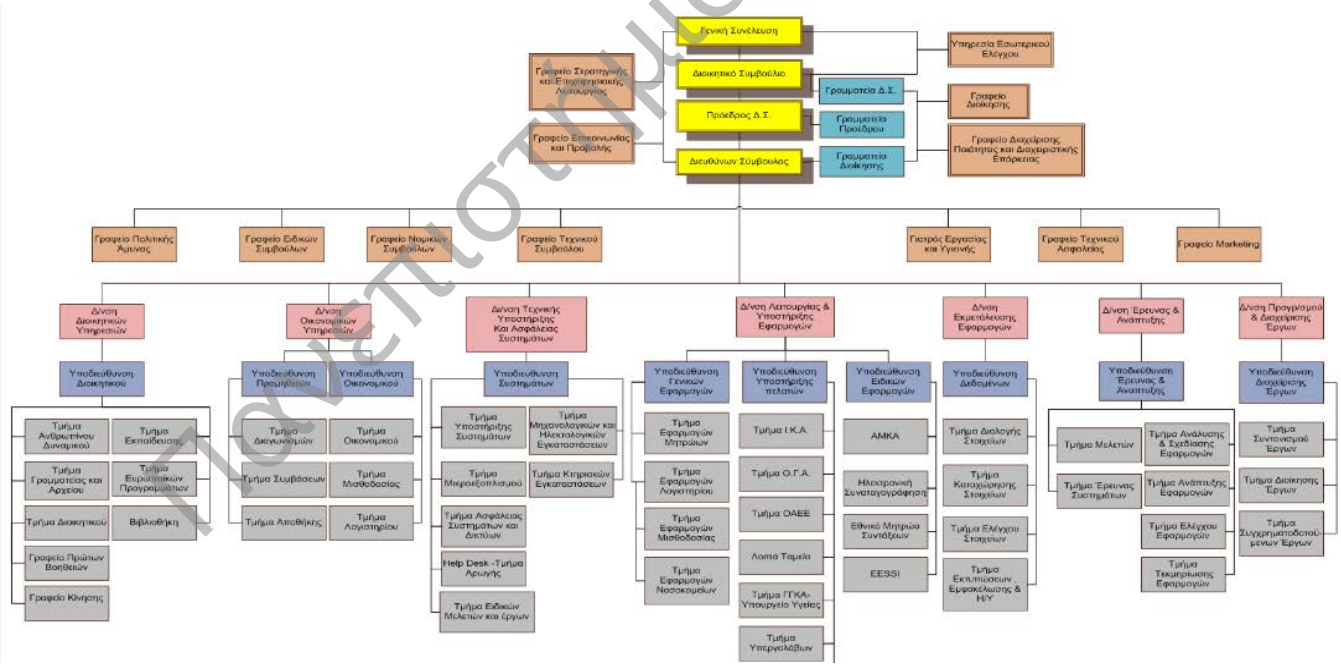
- Ανάπτυξη της εφαρμογής, συντήρηση και συνεχείς αναβαθμίσεις (INN, διαγνωστικές εξετάσεις, ακύρωση κουπονιών, κοινωνικό εισιτήριο, κλπ).
- Αγορά, εγκατάσταση και συντήρηση εξοπλισμού λειτουργίας και ασφαλείας.
- Λειτουργία γραφείου αρωγής (Help Desk) για ιατρούς και φαρμακοποιούς.
- Υποστήριξη ελεγκτικών μηχανισμών (ΥΠΕΔΥΦΚΑ, Δίωξη Ηλεκτρονικού Εγκλήματος κλπ).
- Παραγωγή εκθέσεων.

Το πλαίσιο δραστηριοποίησης της Η.ΔΙ.Κ.Α Α.Ε. περιλαμβάνει τους ακόλουθους βασικούς τομείς:

- Μελέτη, ανάπτυξη, λειτουργία, εκμετάλλευση, διαχείριση και συντήρηση Συστημάτων Πληροφορικής & Επικοινωνιών - εξοπλισμού, λογισμικού και υπηρεσιών - για την εξυπηρέτηση όλων των Φορέων Κοινωνικής Ασφάλισης και Υγείας καθώς και του δημόσιου ή ευρύτερου δημόσιου φορέα.
- Εκτέλεση και διαχείριση έργων στον τομέα της πληροφορικής, των επικοινωνιών και των νέων τεχνολογιών και της διοικητικής μεταρρύθμισης για τη βελτίωση της κοινωνικής ασφάλισης και των υπηρεσιών υγείας στο πλαίσιο του Ε.Σ.Π.Α.

- Διενέργεια διαγωνισμών για έργα που αφορούν στη βελτίωση της ποιότητας των παρεχόμενων υπηρεσιών των φορέων κοινωνικής ασφάλισης και υγείας καθώς και στη βελτίωση δομών της διοικητικής και οικονομικής τους διαχείρισης.
- Ηλεκτρονική εξυπηρέτηση των πολιτών στις συναλλαγές τους με τους Φορείς Κοινωνικής Ασφάλισης (E-government).
- Διασφάλιση και υποστήριξη της διαλειτουργικότητας των Συστημάτων Πληροφορικής & Επικοινωνιών των Φορέων Κοινωνικής Ασφάλισης οι οποίοι τελούν υπό την εποπτεία του Υπουργείου Εργασίας & Κοινωνικής Ασφάλισης καθώς και φορέων που δραστηριοποιούνται σε θέματα υγείας, πρόνοιας και κοινωνικής πολιτικής.
- Ενοποίηση πληροφορίας στο χώρο της Κοινωνικής Ασφάλισης και της Υγείας στην Ελλάδα.
- Παροχή συμβουλών προς τους Φορείς Κοινωνικής Ασφάλισης.
- Συνεργασία-διασύνδεση με αντίστοιχους φορείς της Ευρωπαϊκής Ένωσης.
- Παροχή πληροφοριών στατιστικών ή άλλου τύπου και αξιολογήσεων για την Κοινωνική Ασφάλιση στην Ελλάδα

Το νέο οργανόγραμμα της Η.ΔΙ.Κ.Α. Α.Ε. σύμφωνα με τον Κανονισμό Εσωτερικής Λειτουργίας διαρθρώνεται σε Διευθύνσεις και Γραφεία ως εξής:



Εικόνα 5: Οργανόγραμμα της Η.ΔΙ.Κ.Α. Α.Ε.

Οι εταίροι της ΕΕ έχουν δεσμευτεί στην ανάπτυξη μεθόδων και υπηρεσιών που θα είναι ωφέλιμες και για τα 27 κράτη μέλη της ΕΕ καθώς και για τις λοιπές ενδιαφερόμενες χώρες της Ευρώπης και παγκοσμίως όσον αφορά την ηλεκτρονική συνταγογράφηση.

Κάθε κράτος μέλος είναι υπεύθυνο για ένα τουλάχιστον πακέτο εργασίας και υποστηρίζεται από τα υπόλοιπα ώστε να επιτευχθεί η επιτυχής ολοκλήρωση του εν λόγω πακέτου εργασίας. Επίσης τοπικά υπουργεία, κέντρα ικανότητας και πολλοί βιομηχανικοί εταίροι εργάζονται ως ομάδα για να βρουν τις κατάλληλες μεθόδους και διαδικασίες για τους Ευρωπαίους ασθενείς. Δεδομένου ότι όλα τα ευρωπαϊκά συστήματα υγείας αντιμετωπίζουν παρόμοιες προκλήσεις, η στενότερη διασυνοριακή συνεργασία θα συμβάλει στη δημιουργία μιας πιο αποτελεσματικής δομής των υπηρεσιών υγείας. Ο αριθμός των ασθενών που κάνουν χρήση ιατρικής περίθαλψης σε άλλα κράτη μέλη της ΕΕ, εκτός από εκείνο της κατοικίας τους, αυξάνεται. Η κοινή χρήση της τεχνολογίας της πληροφορικής θα αυξήσει τη διαθεσιμότητα και την ποιότητα της θεραπείας για τους ασθενείς.

Σύμφωνα με τα παραπάνω η δημιουργία της ηλεκτρονικής συνταγογράφησης στην Ελλάδα, εκτός των πλεονεκτημάτων που περιγράφονται, οδηγεί και την διασύνδεση της χώρας με τις ηλεκτρονικές υπηρεσίες υγείας της ΕΕ και πιο συγκεκριμένα με το πρόγραμμα epSOS που περιγράφεται στη συνέχεια.

4.5 EpSOS

Ορισμός

Ηλεκτρονικά συστήματα αναφορικά με τα αρχεία των ασθενών αναπτύσσονται ήδη από πολλά κράτη της Ευρωπαϊκής Ένωσης, με στόχο την βελτίωση της ποιότητας και της αποτελεσματικότητας της υγειονομικής περίθαλψης. Ο ηλεκτρονικός ιατρικός φάκελος του Ασθενούς ή ένα Σύνολο Δεδομένων Έκτακτης Ανάγκης (emergency data set) από αυτόν, καθώς επίσης και τα αρχεία φαρμακευτικής αγωγής και οι ηλεκτρονικές συνταγές (ePrescription), μπορούν να βοηθήσουν να βελτιωθεί σημαντικά και να καταστεί πιο ασφαλής η ιατροφαρμακευτική περίθαλψη μέσω της πρόληψης των ιατρικών λαθών. Μπορούν ακόμη να τροφοδοτήσουν τους γιατρούς με δυνητικά σωτήριες πληροφορίες σε καταστάσεις έκτακτης ανάγκης.

Παρά το γεγονός ότι πολλά ευρωπαϊκά κράτη έχουν δεσμευτεί να εφαρμόσουν εθνικά ηλεκτρονικά συστήματα που αφορούν τα μητρώα των ασθενών, η διαλειτουργικότητα μεταξύ των διαφόρων εθνικών συστημάτων δεν προέκυψε σαν ζήτημα για μεγάλο χρονικό διάστημα. Δεδομένου όμως ότι τα κράτη μέλη της Ευρωπαϊκής Ένωσης συνεργάζονται και λειτουργούν μαζί με όλο και πιο γρήγορους ρυθμούς, η κινητικότητα των πολιτών (και κατά συνέπεια των ασθενών) έχει καταστεί σημαντικός παράγοντας. Για να μπορέσουν όμως να διατίθενται οι υπηρεσίες ηλεκτρονικής υγείας πανευρωπαϊκά, χωρίς δηλαδή περιορισμούς εθνικών ή περιφερειακών συνόρων, απαραίτητη προϋπόθεση είναι η διαλειτουργικότητα – δηλαδή η δυνατότητα επικοινωνίας και συνεργασία -

μεταξύ των συστημάτων και υπηρεσιών αυτών. Μεταξύ δηλαδή των διαφόρων εθνικών και/ή περιφερειακών συστημάτων ηλεκτρονικής υγείας.

Το epSOS είναι ένα έργο για τη διαλειτουργικότητα της ηλεκτρονικής υγείας που χρηματοδοτείται από την Ευρωπαϊκή Ένωση και έχει σαν στόχο να κατασκευάσει και να αξιολογήσει μια υποδομή υπηρεσιών η οποία θα επιτρέπει τη διασυνοριακή διαλειτουργικότητα των συστημάτων ηλεκτρονικών μητρώων υγείας στην Ευρώπη, χωρίς να υπερβαίνει νομοθετικές ρυθμίσεις και ήδη υφιστάμενα εθνικά συστήματα.

4.5.1 Στόχος του epSOS

Ο κύριος στόχος του epSOS είναι να αναπτύξει ένα πρακτικό πλαίσιο ηλεκτρονικής υγείας και κατάλληλες υποδομές στον τομέα της Πληροφορικής και Επικοινωνιών που θα επιτρέπουν την ασφαλή πρόσβαση των διάφορων μη εθνικών ευρωπαϊκών συστημάτων υγειονομικής περίθαλψης στις πληροφορίες αναφορικά με την υγεία του ασθενούς. Επίσης να δοκιμάσει τις μεθόδους αυτές στα πλαίσια ενός Πιλοτικού Έργου Μεγάλης Κλίμακας.

Το epSOS έχει εντοπίσει δύο χωριστές υπηρεσίες ηλεκτρονικής υγείας για τις οποίες αναζητούνται διαλειτουργικές μέθοδοι στη διασυνοριακή επικοινωνία: Τον Φάκελο Ασθενούς (patient medical record) και Ηλεκτρονικές Συνταγές (e-prescription / e-dispensation).

4.5.2 Ηλεκτρονικές Συνταγές

Σε αυτό το πλαίσιο, οι υπηρεσίες Ηλεκτρονικών Συνταγών (ePrescription and eDispensation) αφορούν τη συνταγογράφηση των φαρμάκων μέσω χρήσης του λογισμικού και την ηλεκτρονική διαβίβαση της συνταγής από το Παραπέμποντα (επαγγελματία υγειονομικής περίθαλψης), στο Διανεμητή (π.χ., φαρμακείο), όπου η συνταγή ανακτάται ηλεκτρονικά, το φάρμακο δίνεται στον ασθενή και οι πληροφορίες σχετικά με το διανεμημένο φάρμακο διαβιβάζονται ηλεκτρονικά.

Η διαλειτουργικότητα μεταξύ των εθνικών συστημάτων είναι αναγκαία στην περίπτωση ενός ασθενή που χρειάζεται κάποιο φάρμακο που έχει ήδη συνταγογραφηθεί στη χώρα καταγωγής, όταν πάει σε μια άλλη χώρα. Σε αυτή την περίπτωση ο φαρμακοποιός πρέπει να είναι σε θέση να έχει ηλεκτρονική πρόσβαση στη συνταγή, και όταν το φάρμακο έχει αποσταλεί, το σύστημα θα πρέπει να ενημερώνει το σύστημα υγειονομικής περίθαλψης της χώρας του ασθενούς σχετικά με τα διανεμημένα φάρμακα.

ΚΕΦΑΛΑΙΟ 5

5.1 Ηλεκτρονική Συνταγογράφηση

5.1.1 Ορισμός

Διεθνώς με τον όρο « Ηλεκτρονική Συνταγογράφηση» εννοούμε: την δημιουργία, διακίνηση και έλεγχο των ιατρικών συνταγών και παραπεμπτικών, με την χρήση τεχνολογίας Τ.Π.Ε και με τρόπο που διασφαλίζει την εγκυρότητα, την ασφάλεια και την διαφάνεια των διακινούμενων πληροφοριών.

5.2 Ιστορική εξέλιξη του συστήματος της Ηλεκτρονικής Συνταγογράφησης

Η λειτουργία του συστήματος της Ηλεκτρονικής Συνταγογράφησης ξεκίνησε πιλοτικά από τον οργανισμό Ασφάλισης Ελεύθερων Επαγγελματιών (ΟΑΕΕ) το 2010.

Σε αυτό το διάστημα είχαν ενταχθεί στο σύστημα

- 9500 Φαρμακεία
- 4100 Ιατροί
- 8000 συνταγές το μήνα.

Το 2013 το σύστημα της Ηλεκτρονικής Συνταγογράφησης άρχισε να εφαρμόζεται στο σύνολο των ασφαλιστικών ταμείων.

- 98% των φαρμακείων (11.500 Φαρμακεία)
- 90% των Ιατρών (41.000 Ιατροί)
- 92% του συνόλου των συνταγών (5.5 εκ. Συνταγές/Μήνα)

5.3 Σημαντικά σημεία του έργου

Οκτώβριος 2012: Πραγματοποιήθηκε η διασύνδεση των πληροφοριακών συστημάτων των φαρμακείων με το σύστημα Ηλεκτρονικής Συνταγογράφησης.

Νοέμβριος 2012: Εισαγωγή της δραστικής ουσίας για το σύνολο των φαρμάκων .

Ιανουάριος 2013: E-prescription-Παραγωγική λειτουργία του ενοποιημένου συστήματος ηλεκτρονικής συνταγογράφησης με την καταχώρηση της επίσκεψης και την έκδοση παραπεμπτικών ιατρικών εξετάσεων (Διασύνδεση e diagnosis & e-syntagografisi).

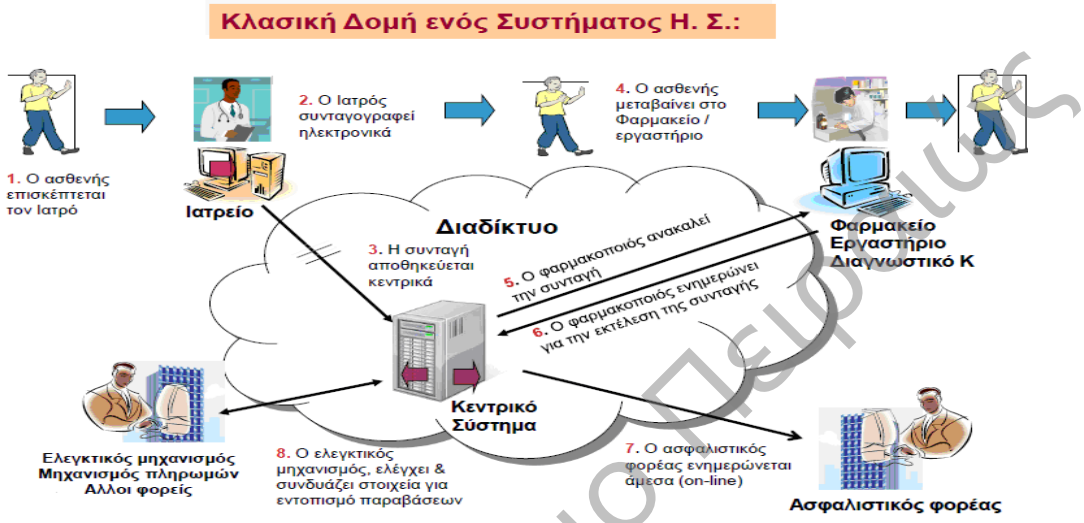
Μάρτιος 2013: Ενσωμάτωση θετικής λίστας στο σύστημα ηλεκτρονικής συνταγογράφησης.

Απρίλιος 2013: Διασύνδεση με e ΔΑΡΥ (Ηλεκτρονική υπηρεσία δήλωσης αναλυτικών παραστατικών υγείας).

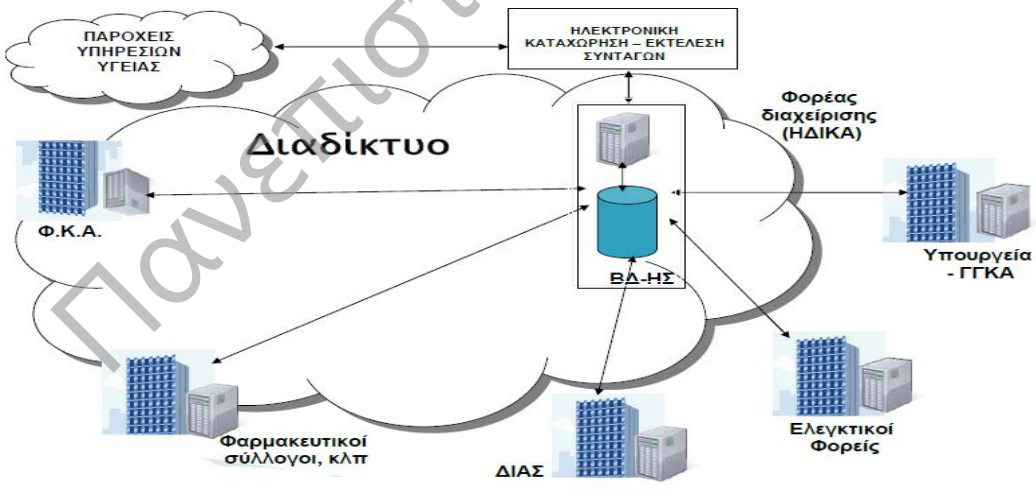
Μάιος 2013: Ανάπτυξη web services υπηρεσιών και διασύνδεση με τον ΕΟΦ για την ακύρωση της ταινίας γνησιότητας των φαρμάκων.

Ιούνιος 2013: Εισαγωγή μηδενικής συμμετοχής για 50.000 ασφαλισμένους με το χαμηλότερο εισόδημα.

Ιούλιος 2013: Κοινωνικό Εισιτήριο (voucher). Δωρεάν διαγνωστικές εξετάσεις για 200.000 ανέργους.



Εικόνα 6: Δομή του συστήματος Η.Σ



Εικόνα 7: Γενική Εικόνα – Ροή Πληροφορίας Η.Σ.

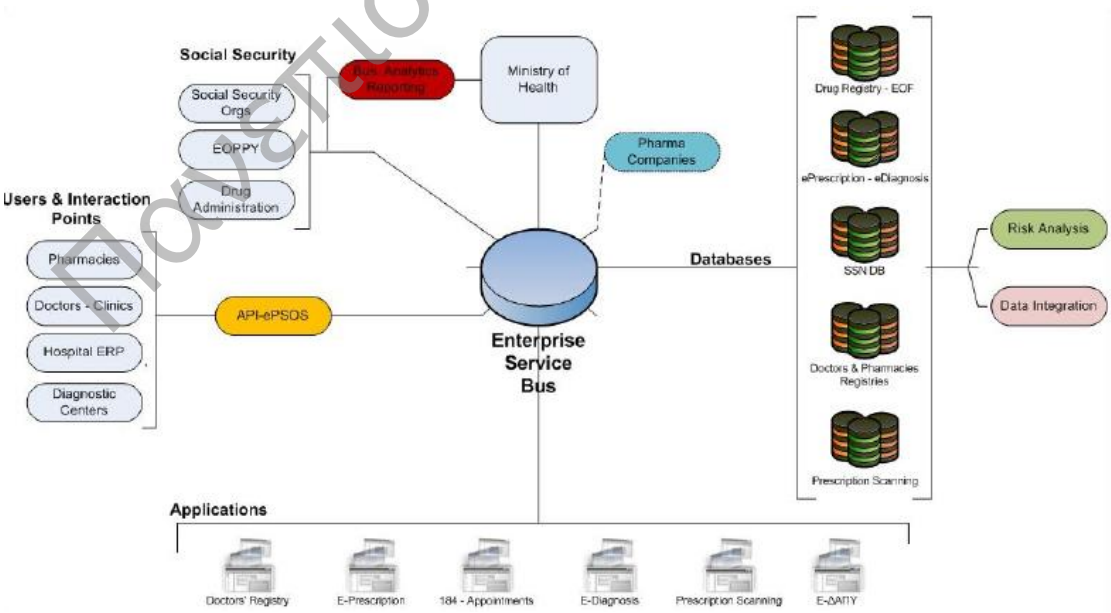
5.4 Οι σκοποί της ηλεκτρονικής συνταγογράφησης είναι:

- Η υποστήριξη των Φορέων Κοινωνικής Ασφάλισης για την εκκαθάριση των συνταγών και την κάλυψη των δαπανών φαρμακευτικής περίθαλψης
- Η υποστήριξη της παρακολούθησης της συνταγογράφησης, της συγκέντρωσης και στατιστικής αξιολόγησης στοιχείων που έχουν σχέση με παροχές υγείας και φαρμακευτικής περίθαλψης
- Η υποστήριξη της εποπτείας και του συντονισμού ενεργειών για τον έλεγχο των δαπανών του συστήματος υγειονομικής περίθαλψης όλων των Φορέων και Κλάδων Ασθένειας αρμοδιότητας της Γενικής Γραμματείας Κοινωνικής Ασφάλισης

Με το σύστημα της ηλεκτρονικής συνταγογράφησης μπορούμε να γνωρίζουμε άμεσα:

- Ποιος ιατρός έγραψε…
- Σε ποιον ασθενή…
- Για ποιο λόγο (ασθένεια)
- Ποια φάρμακα (κόστος, αριθμός κουτιού, φαρμακείο, κτλ)
- Ποιες διαγνωστικές εξετάσεις
- Δυνατότητα συνταγογράφησης με βάση τη δραστική ουσία σε συνεργασία με Ε.Ε (Task Force)/Συμβατότητα με epSOS

5.5 Αρχιτεκτονική και λειτουργία του συστήματος

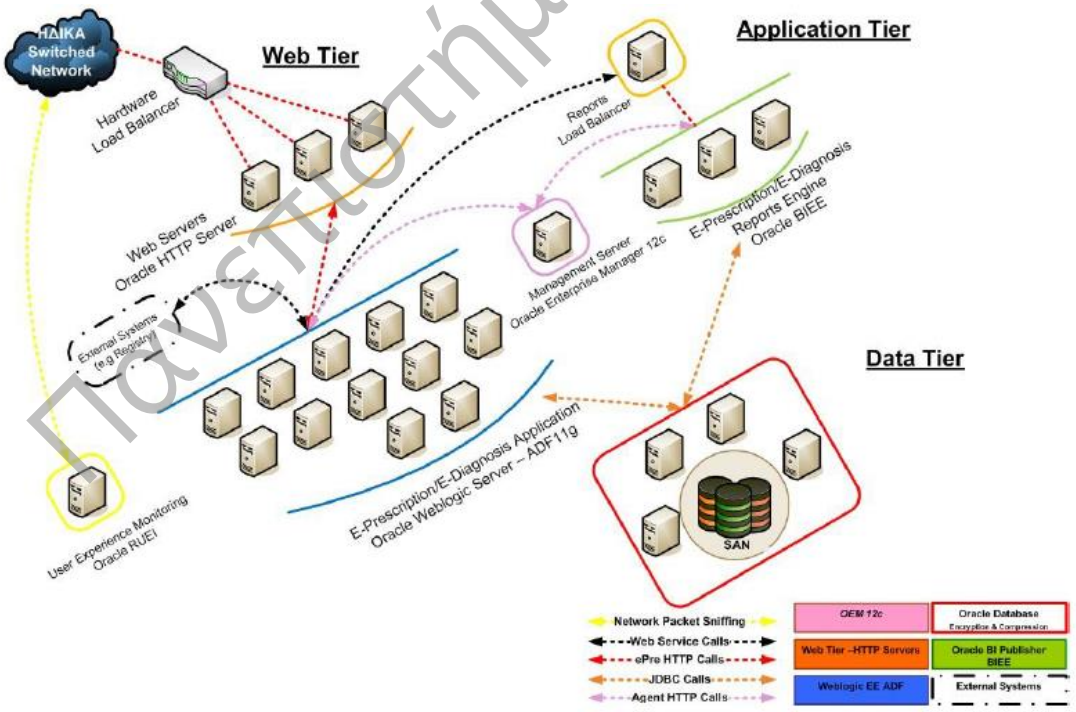


Εικόνα 8: Τεχνολογική δομή συστήματος Ηλεκτρονικής Συνταγογράφησης

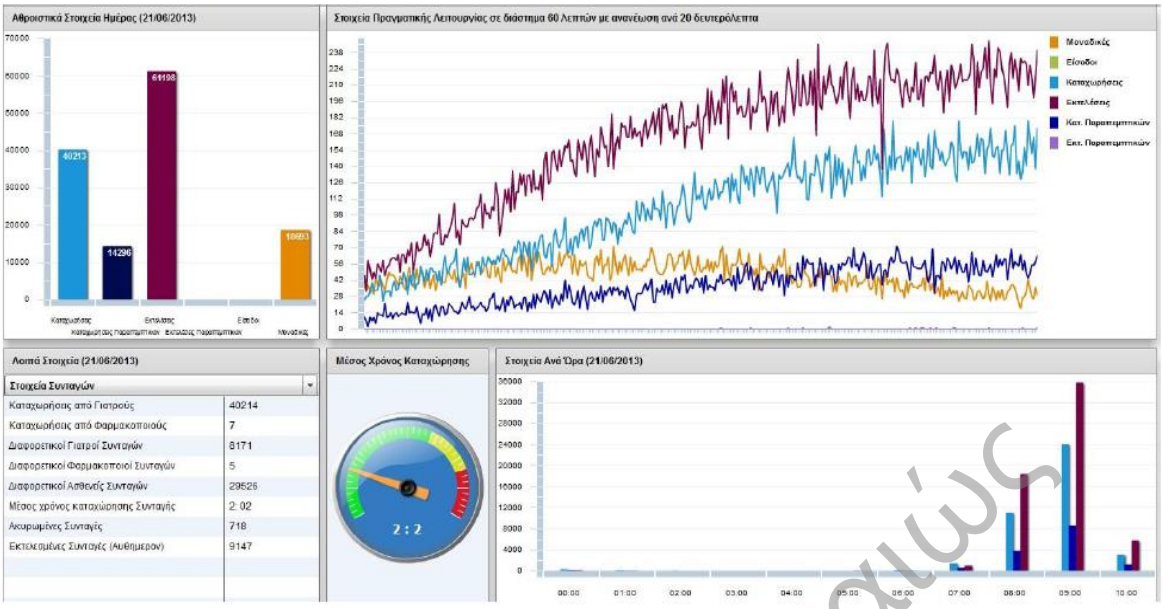
5.5.1 Τεχνολογία Υλοποίησης

Component	Technology
Application Framework	**Oracle ADF**
Web/Application Server	**Oracle Web Tier/Oracle Weblogic 11g Ent. Edition/WLS EE Management Pack**
Database	**Oracle Database 11g Ent. Edition/Partitioning/Adv. Compression/Tuning/Diagnostics**
Authentication	**Simple Authentication (Embedded)**
Auditing	**Oracle Platform Security Services**
Data Encryption	**Oracle Advanced Security Option**
Business Intelligence	**Oracle BI Ent. Edition**
Systems/Applications Management	**Oracle Enterprise Manager 12c Cloud Control**
Performance Monitoring	**Oracle Enterprise Manager 12c Cloud Control**
User Experience Management	**Oracle Real User Experience Insight**
Hypervisor	**Oracle VM 3.1**
OS	**Oracle Linux 5**
Hardware	**IBM (Data Tier), Fujitsu (Application Tier & Management)**

Πίνακας 1: Πίνακας με την τεχνολογία που χρησιμοποιείται στο σύστημα E-Prescription



Εικόνα 9: Διάγραμμα συστήματος E-Prescription

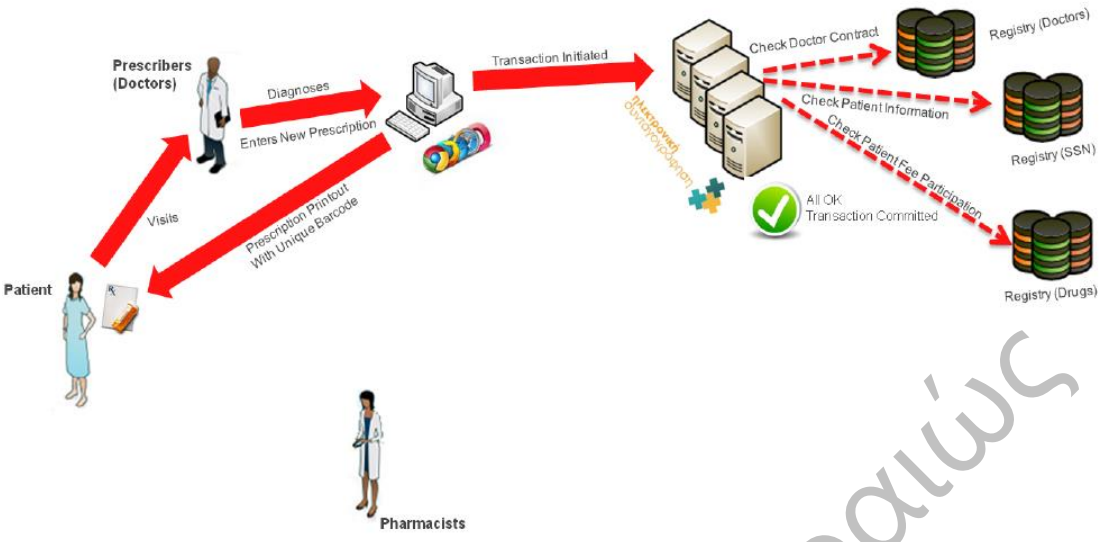


Εικόνα 10: Σύστημα ημερήσιας παρακολούθησης

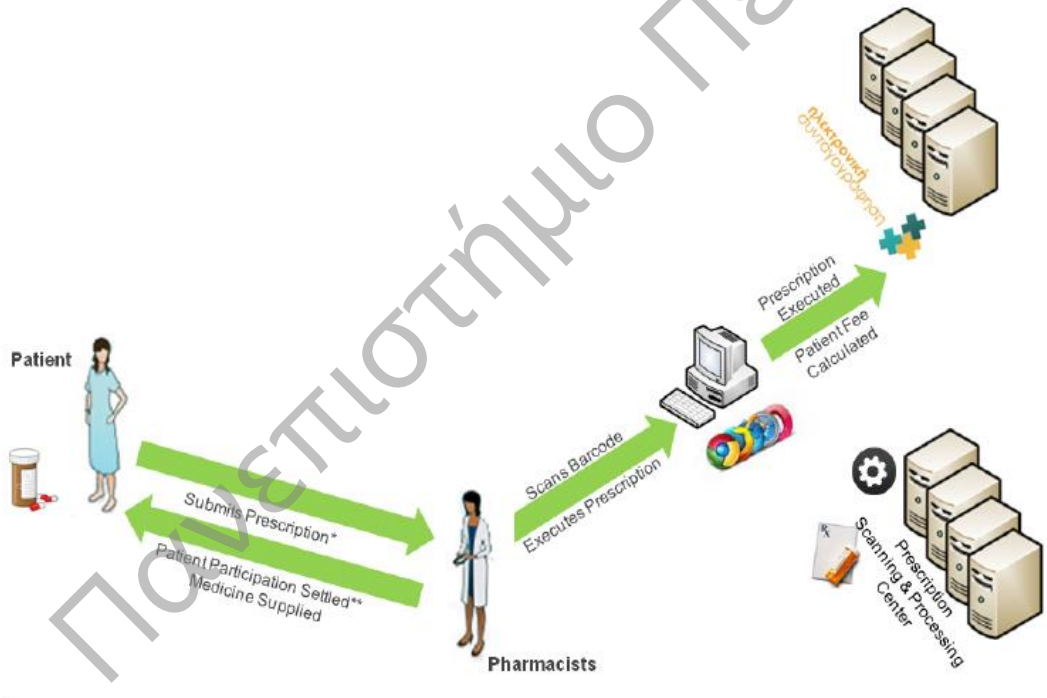
Ημερήσια Άντληση Πληροφοριών σχετικά με:

- Το σύνολο των συνταγών που καταχωρούνται & εκτελούνται ημερησίως
- Το μέσο χρόνο καταχώρησης της συνταγής
- Τον αριθμό των χρηστών & ασθενών που εξυπηρετούνται
- Τον αριθμό συνταγών ανά φορέα
- Στοιχεία συνταγών ανά μονάδα συνταγογράφησης
- Στοιχεία συνταγών ανά ειδικότητα ιατρού

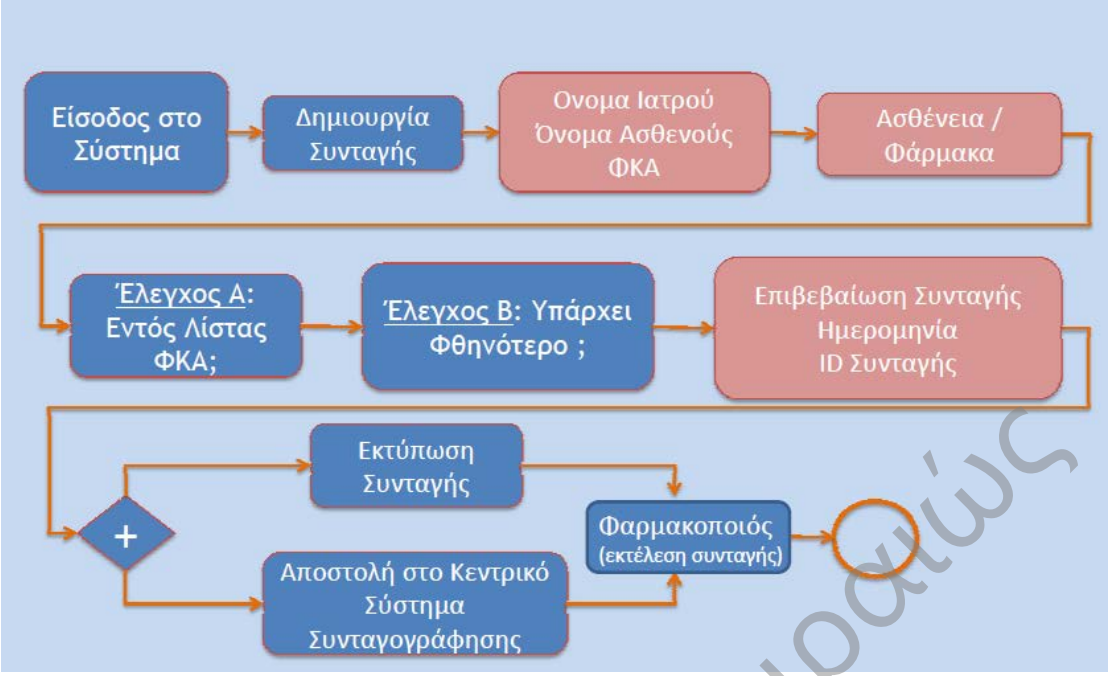
Η ροή της συνταγογράφησης



Εικόνα 11: Μεταξύ ασθενούς και ιατρού



Εικόνα 12: Μεταξύ ασθενούς και φαρμακοποιού



Εικόνα 13: Ροή πληροφορίας διεπαφής χρήστη

5.6 Στάδια της ηλεκτρονικής συνταγογράφησης

- Ο ασθενής επισκέπτεται το γιατρό του
- Ο γιατρός μπαίνει σε μια ηλεκτρονική πλατφόρμα και καταγράφει την επίσκεψη του ασθενούς, τη διάγνωση καθώς και την φαρμακευτική αγωγή του.
- Στην συνέχεια, αποστέλλει τη συνταγή σε μια βάση δεδομένων ή απευθείας στο φαρμακοποιό.
- Ο ασθενής επισκέπτεται το φαρμακοποιό, ο οποίος βρίσκει τη συνταγή στην ηλεκτρονική πλατφόρμα και την εκτελεί.

Οι ασφαλιστικοί φορείς μπορούν να:

- Παρακολουθούν την εκτέλεση των συνταγών.
- Ενημερώνονται άμεσα για το ποσό που πρέπει να καλύψουν μετά την εκτέλεση της συνταγής.
- Λαμβάνουν ηλεκτρονικά την κατάσταση συνταγών από κάθε φαρμακείο.

Μέσα από την ηλεκτρονική συνταγογράφηση

- Δίνεται η δυνατότητα στον γιατρό να έχει πρόσβαση στο ιατρικό αρχείο του ασθενούς.
- Δίνεται η δυνατότητα στο γιατρό να επιλέξει το φθηνότερο σκεύασμα.
- Υπάρχει έλεγχος στη ποσότητα των σκευασμάτων.
- Ενημερώνεται ο γιατρός για επανάληψη κάποιας συνταγής.

- Ενημερώνονται οι φαρμακοποιοί για την αποστολή μιας νέας συνταγής.

5.6.1 Πλεονεκτήματα e-prescription

Το e-prescribing φέρνει μεγαλύτερη ασφάλεια και βελτίωση της όλης διαδικασίας της «συνταγογράφησης και προμήθειας στον ασθενή» του φαρμάκου, χωρίς να αφήνει περιθώρια καταστρατήγησης του συστήματος από κανέναν. Τα οφέλη αφορούν τόσο τους ασθενείς όσο και τους ιατρούς, φαρμακοποιούς και τα Ταμεία.

Τους ασθενείς διότι αποφεύγονται λάθη που γίνονται από τις κακογραμμένες χειρόγραφες συνταγές και από τους αυτοματοποιημένους ελέγχους για την ασφάλεια των φαρμάκων που παρέχει το λογισμικό του e-prescribing.

Τους ιατρούς διότι το σύστημα θα τους παρέχει κλινικά στοιχεία για λήψη σωστών αποφάσεων στην επιλογή της θεραπείας, θα τους διευκολύνει με ενσωματωμένα ασφαλιστικά δεδομένα των ασθενών και κυρίως, διότι θα μειώσει δραστικά τις κλήσεις που λαμβάνουν σήμερα από τα φαρμακεία ζητώντας διευκρινίσεις για τις χειρόγραφες συνταγές τους. Δίνει τη δυνατότητα να αναπτυχθεί μια σωστή επικοινωνία- συνεργασία μεταξύ γιατρού και φαρμακοποιού κατά τη στιγμή της συνταγογράφησης που να οδηγεί στη χορήγηση της κατάλληλης θεραπευτικής αγωγής. Αυτό έχει ως αποτέλεσμα της μείωση των δαπανών υγείας.

Τα ταμεία διότι δεν θα είναι δυνατό να υπάρξουν καταστρατηγήσεις και διασπάθιση πόρων , όπως καταγγέλλεται ότι συμβαίνει σήμερα. Επίσης μέσα από αυτή τη διαδικασία τα Ταμεία θα μπορέσουν να παρακολουθήσουν μέσα από στατιστικές αναλύσεις τις τάσεις της συνταγογραφίας, τι γράφουν οι διάφορες ειδικότητες, που γράφονται οι διάφορες κατηγορίες φαρμάκων και να βγουν χρήσιμα συμπεράσματα που θα βοηθήσουν τις διοικήσεις να παίρνουν σωστότερες αποφάσεις για τη βελτίωση του συστήματος και της περίθαλψης.

Τα φαρμακεία διότι θα τα απαλλάξει από λάθη και την τεράστια γραφειοκρατία που είναι απαραίτητο να κάνουν σήμερα για να υποβάλλουν τις συνταγές στα Ταμεία για να πληρωθούν.

Αρκετές κυβερνήσεις ενθαρρύνουν ενεργά τη χρήση του e-prescribing όχι μόνο για τους λόγους που αναφέραμε παραπάνω αλλά και διότι θα επιτρέψει στα Ασφαλιστικά Ταμεία, στα Νοσοκομεία και γενικά στους φορείς που πληρώνουν για την υγειονομική περίθαλψη να επηρεάσουν τις αποφάσεις συνταγογράφησης με την παροχή προς τους ιατρούς κλινικών και οικονομικών πληροφοριών τη στιγμή ακριβώς που λαμβάνεται η απόφαση για το ποιο φάρμακο θα χορηγήσουν. Με τον τρόπο αυτό οι αποφάσεις για την επιλογή της φαρμακευτικής αγωγής θα είναι πιο σωστή με τελικό αποτέλεσμα την καλύτερη περίθαλψης των ασθενών. Επίσης θα έχουν τη δυνατότητα συλλογής και επεξεργασίας στατιστικών στοιχείων, ελέγχου διαδικασιών και λήψης στρατηγικών αποφάσεων βελτιστοποίησης συστήματος.

Η ηλεκτρονική συνταγογράφηση συμφέρει τέλος και τις φαρμακευτικές εταιρείες διότι η σωστή χρήση των φαρμάκων θα αναδείξει την αξία τους, θα μειώσει τις δαπάνες περίθαλψης έτσι ώστε να πάψουν να κατηγορούνται τα φάρμακα ότι ανεβάζουν το κόστος και να μειωθούν οι πιέσεις για μειώσεις τιμών.

Το e-prescribing λοιπόν θα μπορούσε να έχει τεράστιες θετικές επιπτώσεις σε όλους τους εμπλεκόμενους φορείς και να τους βοηθήσει όλους να λειτουργήσουν με ορθολογικότερο και πιο επωφελή τρόπο για τους ίδιους αλλά κυρίως για το σύστημα υγείας και τους ασθενείς.

Η νέα αυτή τεχνολογία είναι σήμερα καθιερωμένη στη Δανία, Σουηδία και Ολλανδία, όπου το 70% όλων των συνταγών γράφονται ηλεκτρονικά.

5.6.2 Μειονεκτήματα e-prescription

Για να εφαρμοσθεί, θα πρέπει να υπάρχουν ηλεκτρονικοί υπολογιστές τόσο στους γιατρούς όσο και στα φαρμακεία. Τα περισσότερα φαρμακεία έχουν, αλλά μόνο το 20% των γιατρών διαθέτει υπολογιστή. Απαραίτητη είναι και η μηχανοργάνωση των ασφαλιστικών οργανισμών. Τέλος η χρήση της προϋποθέτει τη γνώση ηλεκτρονικών υπολογιστών.

Σημαντική παράμετρος είναι η ασφάλεια των δεδομένων που θα διακινούνται μέσα από το σύστημα καθώς και της βάσης δεδομένων στην οποία θα αποθηκεύονται όλα τα στοιχεία.

5.6.3 Απαραίτητος Εξοπλισμός για τη σωστή λειτουργία του συστήματος

Σχετικά με τον εξοπλισμό που απαιτείται και το λογισμικό για τη χρήση της εφαρμογής Ηλεκτρονικής Καταχώρισης και Εκτέλεσης Συνταγών (ΗΚΕΣ) Φαρμάκων δεν απαιτείται η προμήθεια ειδικού λογισμικού. Η εφαρμογή Ηλεκτρονικής Καταχώρισης και Εκτέλεσης Συνταγών (ΗΚΕΣ) είναι διαδικτυακή και η πρόσβαση σε αυτήν επιτυγχάνεται μέσω οποιουδήποτε προγράμματος πλοήγησης στο Διαδίκτυο, όπως Internet Exprorer 7+, Mozilla Firefox, Google Chrome, Safari κλπ.

Θα πρέπει, όμως οι χρήστες να διαθέτουν τον κάτωθι εξοπλισμό:

Στο Ιατρείο:

- Έναν ηλεκτρονικό υπολογιστή (Desktop ή Laptop) τελευταίας 5-ετίας, με λειτουργικό σύστημα MS Windows (XP, Vista, Win7), ή Linux, ή MacOSX και ένα πρόγραμμα πλοήγησης στο Διαδίκτυο - web browser (IE7+, Mozilla, Opera κλπ.)
- Σύνδεση με το διαδίκτυο (ADSL, Mobile Internet)
- Έναν εκτυπωτή InkJet ή Laser με δυνατότητα εκτύπωσης τουλάχιστον στα 300dpi

Στο Φαρμακείο:

- Έναν ηλεκτρονικό υπολογιστή (Desktop ή Laptop) τελευταίας 5-ετίας, με λειτουργικό σύστημα MS Windows (XP, Vista, Win7), ή Linux, ή MacOSX και ένα πρόγραμμα πλοήγησης στο Διαδίκτυο - web browser (IE7+, Mozilla, Opera κλπ.)
- Σύνδεση με το Διαδίκτυο (ADSL, Mobile Internet)
- Έναν εκτυπωτή InkJet ή Laser με δυνατότητα εκτύπωσης τουλάχιστον στα 300dpi
- Ένα Bar Code Scanner για την ανάγνωση του γραμμωτού κώδικα των σκευασμάτων (να έχει τη δυνατότητα ανάγνωσης κωδικοποίησης EAN 13)

Επίσης, ο χρήστης θα χρειαστεί να εγκαταστήσει δωρεάν στον υπολογιστή του, το λογισμικό Adobe Acrobat Reader, το οποίο μπορεί να εγκαταστήσει από τον ιστότοπο (site) της Adobe (έκδοση 9 και νεότερη) (π.χ. τελευταία έκδοση http://get.adobe.com/reader)

5.7 Διαδικασία εγγραφής στο σύστημα

Εικόνα 14: Αρχική σελίδα εγγραφής-εισαγωγής στο σύστημα Η.Σ.

Για την εγγραφή και την είσοδο στο σύστημα οι χρήστες μπορούν μέσω της ιστοσελίδας www.e-syntagografisi.gr να επιλέξουν στα δεξιά "Είσοδος στην Εφαρμογή".

Η είσοδος, όμως, επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες. Θα πρέπει πρώτα να αποκτήσουν λογαριασμό χρήστη (όνομα και κωδικό πρόσβασης – username & password).

Για την απόκτηση του λογαριασμού στο σύστημα πρέπει να γίνει εγγραφή στο σύστημα. Για να μπορέσουν να εγγραφούν θα πρέπει να είναι ιατροί συμβεβλημένοι με τον ΟΑΕΕ ή κάτοχοι φαρμακείου (νόμιμοι εκπρόσωποι).

Στην ιστοσελίδα της υπηρεσίας «ηλεκτρονική συνταγογράφηση» www.e-syntagografisi.gr υπάρχει στα δεξιά επιλογή που λέει εγγραφή στην εφαρμογή.

Τα στοιχεία θα πρέπει να δηλώνονται όπως ακριβώς αναγράφονται στην αστυνομική ταυτότητα του χρήστη. Απαραίτητη προϋπόθεση η εισαγωγή όλων των στοιχείων τα οποία ζητούνται από την φόρμα εγγραφής και ο έλεγχος τους από την εφαρμογή για την ορθή ταυτοποίηση του χρήστη ιατρού ή φαρμακείου.

Οι βασικοί περιορισμοί για τη χρήση της εφαρμογής Ηλεκτρονικής Καταχώρισης και Εκτέλεσης Συνταγών (ΗΚΕΣ) είναι:

- Η χρήση της εφαρμογής γίνεται μόνο από εξουσιοδοτημένους χρήστες
- Ο ιατρός συνταγογραφεί, κατά δήλωσή του, παρουσία του ασθενή
- Ο φαρμακοποιός εκτελεί συνταγές, κατά δήλωση του, παρουσία του ασφαλισμένου
- Εάν ο ασφαλισμένος δεν έχει ΑΜΚΑ είναι αδύνατη η καταχώριση ηλεκτρονικής συνταγής άρα και η εκτέλεση συνταγών φαρμάκων

Η χρήση της εφαρμογής γίνεται μέσω του διαδικτύου (Internet). Σε περίπτωση που διακοπή η σύνδεση στο διαδίκτυο και δεν υπάρχει πρόσβαση στην εφαρμογή ο ιατρός θα δώσει στον ασθενή του χειρόγραφη συνταγή, εφόσον αυτό δεν αποτελεί συνήθη πρακτική αλλά έκτακτη ανάγκη. Σε κάθε περίπτωση οι χειρόγραφες συνταγές που συνταγογραφούνται θα καταχωρηθούν ηλεκτρονικά στο σύστημα από το φαρμακείο που θα τις εκτελέσει.

Σε περίπτωση που στο φαρμακείο υπάρξει προσωρινή διακοπή της σύνδεσης στο διαδίκτυο και δεν υπάρχει πρόσβαση στην εφαρμογή δεν μπορεί να εκτελεστεί η εφαρμογή. Εάν η συνταγή του πελάτη δεν λήγει την ίδια ημέρα και τον έχει ταυτοποιήσει, μπορεί, αν το επιθυμεί, να δώσει τα φάρμακα στον πελάτη και αφού ο πελάτης καταβάλλει μόνο τη συμμετοχή του για το Ταμείο του, στη συνέχεια έως την ημερομηνία λήξης της συνταγής μπορεί ο φαρμακοποιός να καταχωρίσει την συνταγή ως εκτελεσμένη στο σύστημα (αφού φυσικά έχει κρατήσει τα κουπόνια των σκευασμάτων που έχει δώσει για τη συγκεκριμένη συνταγή).

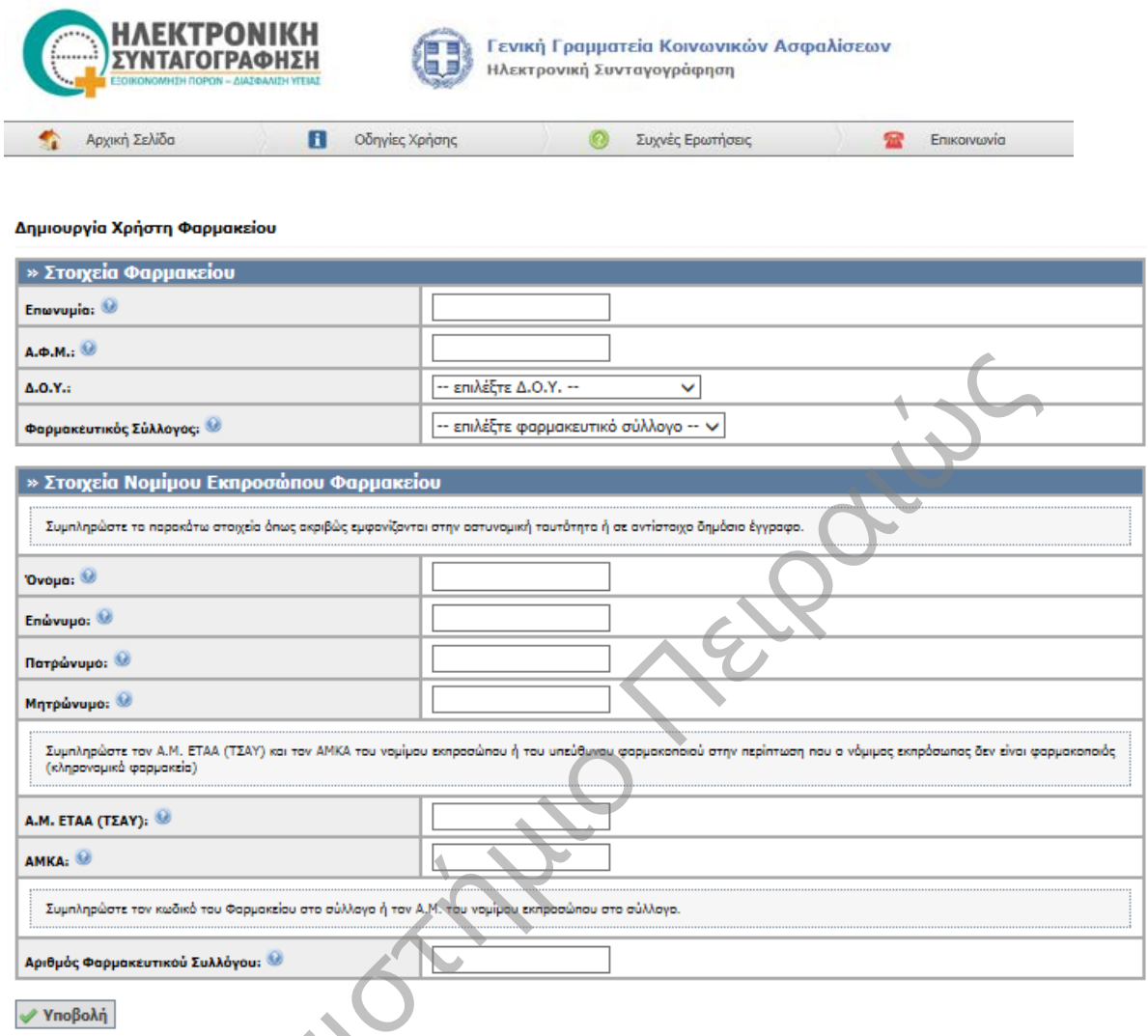
Σε περίπτωση που υπάρξει οποιοδήποτε πρόβλημα με την εφαρμογή (π.χ δεν είναι δυνατή η είσοδος στο σύστημα). Τότε οι χρήστες μπορούν να επικοινωνούν με την τεχνική υποστήριξη του λογισμικού για περαιτέρω οδηγίες και διευκρινήσεις.

Παρακάτω παρουσιάζονται οι οθόνες εγγραφής των χρηστών ιατρού και φαρμακοποιού.

ΙΑΤΡΟΣ

Εικόνα 15: Σελίδα εγγραφής ιατρών

ΦΑΡΜΑΚΟΠΟΙΟΣ



Εικόνα 16: Σελίδα εγγραφής φαρμακοποιών

5.8 Προβλήματα στη λειτουργία του συστήματος

Στις 24 Μαΐου 2012 έχουμε την έναρξη λειτουργίας της Η/Σ στην Η.ΔΙ.Κ.Α Α.Ε Μέσος όρος καταχώρησης και εκτέλεσης: 150.000 συνταγές ημερησίως

- Προβλήματα στην αρχική ρύθμιση λειτουργίας της Η/Σ. Επιλύθηκαν με τοποθέτηση νέων balancers για τη σωστή κατανομή φορτίου στους Application Servers
- Μεγάλη αύξηση συνταγογραφήσεων και εκτελέσεων λόγω των απεργιών των Ιατρών και των Φαρμακοποιών
- Αύξηση του όγκου συνταγογράφησης με την ένταξη των επαγγελματικών ταμείων στον ΕΟΠΥΥ .

Το επίπεδο διαθεσιμότητας της εφαρμογής έφτασε το 99 %.

Το Δεκέμβριο του 2012 έγινε προσθήκη νέου εξοπλισμού (4 Application Servers και 2 Data Base Servers καθώς και 2 νέοι Firewalls) με δυνατότητα εξυπηρέτησης 300.000 συνταγογραφήσεις και 300.000 εκτελέσεις ημερησίως.

Αύξηση του επιπέδου διαθεσιμότητας στο 99,3 %. Τέλος τον Ιανουάριο του 2013 έχουμε την λειτουργία Ενιαίου Συστήματος Συνταγογράφησης Φαρμάκων και Παραπεμπτικών Διαγνωστικών Εξετάσεων e-prescription .

Την 1η εβδομάδα λειτουργίας του e-prescription δημιουργήθηκαν προβλήματα που είχαν να κάνουν με την οργάνωση των παραπεμπτικών εξετάσεων και τα οποία σύντομα λύθηκαν.

Στις 15-22 Φεβρουαρίου υπήρξαν προβλήματα που σχετίζονται με την τάση της ΔΕΗ και την αδιάλειπτη λειτουργία (UPS) με αποτέλεσμα τη διακοπή λειτουργίας του συστήματος της Ηλεκτρονικής Συνταγογράφησης.

Στις 24 Φεβρουαρίου ξεκίνησε η λειτουργία της διάταξης αδιάλειπτης λειτουργίας και προστασίας (UPS). Με αποτέλεσμα το επίπεδο διαθεσιμότηταςτης εφαρμογής να έχει το ποσοστό του 99 %.

Το Μάρτιο του 2013 έγινε προσθήκη νέου εξοπλισμού (3 επιπλέον Application Servers) για την υλοποίηση της διαλειτουργικότητας με το e-dapy για την εκτέλεση των παραπεμπτικών εξετάσεων. Το ποσοστό της διαθεσιμότητα της Η/Σ αυξήθηκε στο 99,8 %.

5.9 Παράδειγμα αντιμετώπισης τεχνικού προβλήματος με προτεινόμενη λύση

5.9.1 Πρωτόκολλο επικοινωνίας με ERPs φακέλους ασθενή

Το λογισμικό ηλεκτρονικής συνταγογράφησης (http://www.e-syntagografisi.gr/) αλλά και αυτών ιατρικών πράξεων του ΟΠΑΔ (http://www.e-diagnosis.gr/medweb/login.aspx) λειτουργούν ως εφαρμογές web με θετικά και αρνητικά σημεία.

Η αδυναμία διασύνδεσης με υπάρχοντα λογισμικά (ERPs) που υπάρχουν σε νοσοκομεία και ιατρεία (ιδιωτικά/δημόσια) και η αδυναμία διασύνδεσης με τοπικά συστήματα ηλεκτρονικού φακέλου ασθενή είναι και το σημαντικότερο πρόβλημα που υφίσταται και απαιτείται σύντομα η εξεύρεση μιας λύσης.

Μια λύση είναι, παράλληλα με την λειτουργία του υπάρχοντος συστήματος, να υπάρχει και η δυνατότητα διασύνδεσης με την χρήση πρωτοκόλλου επικοινωνίας και ανταλλαγής πληροφορίας ενός τοπικού λογισμικού ERP/φακέλου ασθενή που υπάρχει σε μια δημόσια/ιδιωτική μονάδα υγείας/ιατρείο με το κεντρικό σύστημα της ηλεκτρονικής συνταγογράφησης που υπάρχει στο ΗΔΙΚΑ.

Η επικοινωνία μπορεί να γίνεται όπως και σήμερα μέσω Internet με το ίδιο https πρωτόκολλο δικτύου, με την χρήση των ίδιων κωδικών πρόσβασης αλλά στη συγκεκριμένη περίπτωση ο χρήστης χρησιμοποιεί το τοπικό λογισμικό ERP/ηλεκτρονικού φακέλου ασθενή και αυτό το λογισμικό επικοινωνεί μέσω του προτεινόμενου πρωτοκόλλου με το σύστημα ηλεκτρονικής συνταγογράφησης του ΗΔΙΚΑ. Λαμβάνει στο τέλος το ίδιο ακριβώς pdf αρχειο με την συνταγή το οποίο τυπώνεται και είναι πανομοιότυπο με αυτό που τυπώνεται με την υπάρχουσα ιστοσελίδα ηλεκτρονικής συνταγογράφησης του ΗΔΙΚΑ.

Αυτή η υλοποίηση:

Επιτρέπει την ενσωμάτωση της ηλεκτρονικής συνταγογράφησης στα ήδη υπάρχοντα λογισμικά που έχουν νοσοκομεία και ιατρεία και την καλύτερη διαχείριση και παρακολούθηση από τις μονάδες υγείας του έργου που επιτελείται.

Μειώνει τις ανάγκες σε εκπαίδευση των χρηστών που ήδη χρησιμοποιούν κάποια εφαρμογή ηλεκτρονικού φακέλου.

Μειώνει τις ανάγκες σε υπολογιστική ισχύ των συστημάτων και σε παροχή υποστήριξης χρηστών από το ΗΔΙΚΑ.

Επιτρέπει την προσαρμογή της ηλεκτρονικής συνταγογράφησης στις ανάγκες και ιδιαιτερότητες της κάθε μονάδας χωρίς να αλλάζει σε τίποτα το τελικό αποτέλεσμα της συνταγής και της παρακολούθησης της ηλεκτρονικής συνταγογράφησης.

Επιβοηθά την αποδοχή της ηλεκτρονικής συνταντογράφησης από τους χρήστες.

Η Ηλεκτρονική Συνταγογράφηση έχει ιδιαίτερη σημασία, τόσο για τους πολίτες όσο και για την εθνική οικονομία. Η άμεση υλοποίηση της αποτελεί εθνική ανάγκη.

Το υφιστάμενο σύστημα Η/Σ (με έμφαση στον έλεγχο δαπανών) που αναπτύχτηκε (ταχύτατα), λειτουργεί ήδη στην ΗΔΙΚΑ με ικανοποιητικά αποτελέσματα.

Το σύστημα ΗΣ που λειτουργεί ήδη στην ΗΔΙΚΑ είναι το μόνο που μπορεί να καλύψει ικανοποιητικά τις άμεσες εθνικές ανάγκες.

ΚΕΦΑΛΑΙΟ 6

Εφαρμογή Risk Management στο σύστημα e-prescription

Στο κεφάλαιο αυτό θα αναλυθεί η διαδικασία διαχείρισης κινδύνων που αφορά τη λειτουργία του συστήματος e- prescription.

Η διαδικασία διαχείρισης κινδύνων στο συγκεκριμένο σύστημα θα γίνει με βάση τα προβλήματα τα οποία ενδέχεται να προκύψουν κατά τη διάρκεια της λειτουργίας του. Στόχος είναι οι κίνδυνοι αυτοί να προσδιοριστούν, αναλυθούν, αξιολογηθούν και αντιμετωπιστούν τυχόν προβλήματα προβαίνοντας σε κάποιες κατάλληλες διορθωτικές ενέργειες.

6.1 Καθορισμός πλαισίου

Στη φάση αυτή πρέπει να καθοριστούν τα εμπλεκόμενα μέρη του συστήματος, το εσωτερικό και το εξωτερικό πλαίσιο του συστήματος και ο σκοπός ύπαρξης της διαδικασίας διαχείρισης κινδύνων.

Τα εμπλεκόμενα μέρη του συστήματος είναι τα εξής:

- Υπουργείο Υγείας
- Γενική Γραμματεία Κοινωνικών Ασφαλίσεων
- ΕΟΠΥΥ
- ΕΟΦ
- Η.ΔΙ.Κ.Α. Α.Ε
- Ελεγκτικοί Φορείς
- Ασφαλισμένοι
- Ιατρική Κοινότητα
- Φαρμακευτική Κοινότητα
- Αγορά Πληροφορικής
- Επιστημονική Κοινότητα
- Ευρωπαϊκή Επιτροπή
- Εθνική Τράπεζα

Όσον αφορά το εσωτερικό πλαίσιο καθορίζονται τα παρακάτω στοιχεία.

Στόχος συστήματος

- Η βελτίωση των παρεχόμενων υπηρεσιών υγείας στους πολίτες
- Η επίτευξη οικονομιών στον τομέα φροντίδας υγείας.
- Ο καλύτερος συντονισμός και έλεγχος του συστήματος – εξορθολογισμός των σχετικών διαδικασιών.
- Η ανάπτυξη ενός ανοικτού, διαλειτουργικού (nat/int) συστήματος, με ενσωμάτωση των διεθνών βέλτιστων προτύπων και πρακτικών.
- Η παροχή δυνατότητας ανάπτυξης από τρίτους παράλληλων καινοτόμων υπηρεσιών για καλύτερες υπηρεσίες περίθαλψης.

Δομή, λειτουργία, βασικές διαδικασίες

Το e-prescribing ή ηλεκτρονική συνταγογράφηση είναι η χρήση on line, μηχανογραφημένων εργαλείων για τη δημιουργία, υπογραφή και αποστολή των συνταγών από τους ιατρούς και φαρμακοποιούς. Το «λογισμικό του e-prescribing» διευκολύνει και βοηθάει να αντικατασταθούν οι χειρόγραφες συνταγές με ηλεκτρονικές, οι οποίες και αποστέλλονται κατευθείαν από τον ηλεκτρονικό υπολογιστή του ιατρού στα φαρμακεία μέσω διαδικτύου από όπου θα πάει εν συνεχεία ο ασθενής να προμηθευτεί το φάρμακο, και στην συνέχεια το φαρμακείο μετά την εκτέλεση της συνταγής να τη στείλει κατευθείαν στο αντίστοιχο Ταμείο.

Φυσική & τεχνολογική υποδομή

Πρόκειται για Web-based εφαρμογή όπου έχουν πρόσβαση μόνο εξουσιοδοτημένοι χρήστες (ιατροί, φαρμακοποιοί) .

Οι ηλεκτρονικές συνταγές περιλαμβάνουν όλα τα απαραίτητα δεδομένα, όπως:

- ID ιατρού/ασθενούς/φαρμακείου
- Διάγνωση (text & ICD-10)
- Φάρμακα (ποσότητα, δοσολογία,…)
- Ποσοστό συμμετοχής ασθενούς, κτλ

Το σύστημα είναι διαμορφωμένο με τις απαραίτητες τεχνικές και νομικές προδιαγραφές, σε συνεννόηση με την Αρχή Προστασίας Δεδομένων, ώστε να είναι απολύτως ασφαλές.

Για να μπορέσει το σύστημα να προσφέρει τα αναμενόμενα οφέλη και να ελαχιστοποιηθούν όσο τη δυνατόν περισσότερο να προβλήματα που μπορεί να προκύψουν, πρέπει κάποια ομάδα ειδικών να αναλάβει τη διαδικασία διαχείρισης των κινδύνων που μπορεί να παρουσιαστούν. Θα πρέπει να προσδιορίσει τους κινδύνους που μπορεί να προκύψουν, να τους αναλύσει, να τους αξιολογήσει, να δημιουργήσει σχέδια για να τους αντιμετωπίσει, εφ’ όσον κριθεί αναγκαίο, και να τους

παρακολουθεί ώστε να είναι έτοιμη να τους αντιμετωπίσει σε περίπτωση που κάτι αλλάξει σε σχέση με αυτά που αρχικά είχε αποτιμήσει.

6.2 Προσδιορισμός κινδύνων

Στη φάση αυτή πρέπει να εντοπιστούν οι πιθανοί κίνδυνοι χρησιμοποιώντας κάποια/ κάποιες από τις μεθόδους εντοπισμού (συνεντεύξεις, ομαδική παραγωγή ιδεών, ειδικές ομάδες, μέθοδος Delphi, ανάλυση SWOT, διαγραμματικές τεχνικές), να ταξινομηθούν στις διάφορες κατηγορίες και τέλος να φτιαχτεί το μητρώο κινδύνων, ένας συγκεντρωτικός πίνακας με τα παραπάνω στοιχεία.

Μερικοί από τους κινδύνους που μπορεί να προκύψουν είναι οι εξής:

- Ασυμβατότητα λογισμικού με τις απαιτήσεις
- Εξάντληση πόρων του συστήματος
- Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων
- Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών
- Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού
- Έλλειψη διασυνδεσιμότητας των φορέων μέσω του συστήματος
- Λανθασμένος σχεδιασμός υλικού (αρχιτεκτονική συστήματος)
- Λανθασμένος σχεδιασμός λογισμικού (αρχιτεκτονική συστήματος)
- Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών (δικτυακή υποδομή)
- Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού
- Μη αποδεκτή ποιότητα λογισμικού
- Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του λογισμικού του πληροφοριακού συστήματος
- Αδυναμία Σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου
- Ανεπαρκής προστασία κρυπτογραφικών κλειδιών
- Ελλιπής επικύρωση της επεξεργασίας των δεδομένων
- Δυσλειτουργία του υλικού
- Ανεπαρκής έλεγχος του λογισμικού
- Σφάλματα λογισμικού
- Πολυπλοκότητα λογισμικού
- Μη ασφαλής αρχιτεκτονική δικτύου
- Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου

- Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου
- Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος
- Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.
- Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)
- Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος
- Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων
- Ανεπαρκής επίβλεψη των εργαζομένων
- Έλλειψη διαδικασίας για την αφαίρεση των δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης
- Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού
- Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας
- Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού
- Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης
- Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας
- Έλλειψη οικονομικών πόρων
- Προβλήματα με την χρηματοδότηση του έργου
- Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος λόγω κακής χρήσης του
- Κλοπή υλικού από εργαζομένους
- Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα
- Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή
- Καταστροφή εξοπλισμού από υγρά/τρόφιμα
- Διαρροή πληροφοριών
- Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος
- Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους
- Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος
- Μη εξουσιοδοτημένες αλλαγές αρχείων
- Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος
- Έλλειψη κινήτρων για τους εργαζόμενους
- Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας
- Απώλεια συσκευών ταυτοποίησης προσώπου (ταυτότητες)
- Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο

- Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών
- Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου
- Λάθος κατανομή του κεφαλαίου
- Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος
- Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος
- Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού
- Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού
- Λανθασμένη κοστολόγηση του έργου
- Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές
- Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου
- Λανθασμένες αποφάσεις διαχείρισης κινδύνων
- Κίνδυνος σεισμού
- Κίνδυνος Κεραυνού
- Κίνδυνος πλημμύρας
- Κίνδυνος πυρκαγιάς
- Κίνδυνος διαρροής υδάτων
- Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση
- Κατολίσθηση – διάβρωση εδάφους
- Ηλιακές εκλάμψεις
- Σκόνη
- Βλάβη του συστήματος κλιματισμού
- Ηλεκτρομαγνητικές παρεμβολές
- Στατικός ηλεκτρισμός
- Έκρηξη ηφαιστείου
- Πυρηνικό ατύχημα
- Κίνδυνος εκρήξεων
- Έντομα/ τρωκτικά
- Κίνδυνος δονήσεων
- Καπνός / μικροσωματίδια
- Μαγνήτες/ μαγνητικά εργαλεία
- Αγωγές – Μηνύσεις

- Απώλεια καλής φήμης
- Κλοπή πνευματικής ιδιοκτησίας
- Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων
- Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας
- κλοπή υλικού
- Βανδαλισμοί
- Εισβολείς (Hackers) – Υποκλοπή δεδομένων
- Εισβολείς (Hackers) – Καταστροφή δεδομένων
- Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού)
- Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές
- Κατασκοπεία
- Τρομοκρατικές επιθέσεις

Αφού προσδιοριστούν οι διάφοροι κίνδυνοι ταξινομούνται στις διάφορες κατηγορίες όπως φαίνεται στον παρακάτω πίνακα 2.

Κατηγορίες κινδύνων	Κίνδυνοι
Τεχνολογικοί	• Ασυμβατότητα λογισμικού με τις απαιτήσεις • Εξάντληση πόρων του συστήματος • Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων • Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών • Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού • Έλλειψη διασυνδεσιμότητας του φορέων μέσω του συστήματος • Λανθασμένος σχεδιασμός υλικού (αρχιτεκτονική συστήματος) • Λανθασμένος σχεδιασμός λογισμικού (αρχιτεκτονική συστήματος) • Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών (δικτυακή υποδομή) • Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού • Μη αποδεκτή ποιότητα λογισμικού • Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του λογισμικού του πληροφοριακού συστήματος • Αδυναμία Σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου • Ανεπαρκής προστασία κρυπτογραφικών κλειδιών • Ελλιπής επικύρωση της επεξεργασίας των δεδομένων • Δυσλειτουργία του υλικού • Ανεπαρκής έλεγχος του λογισμικού • Σφάλματα λογισμικού • Πολυπλοκότητα λογισμικού • Μη ασφαλής αρχιτεκτονική δικτύου
Λειτουργικοί – Επιχειρησιακοί	• Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου • Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου • Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος • Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου. • Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες) • Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος • Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων • Ανεπαρκής επίβλεψη των εργαζομένων • Έλλειψη διαδικασίας για την αφαίρεση των δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης • Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού • Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας λόγω έλλειψης τεχνικών γνώσεων ή εξαιτίας απλού ανθρώπινου σφάλματος του προσωπικού • Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού • Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης

	• Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας
Χρηματοοικονομικοί	• Έλλειψη οικονομικών πόρων • Προβλήματα με την χρηματοδότηση του έργου
Ανθρώπινοι	• Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος λόγω κακής χρήσης του • Κλοπή υλικού από εργαζομένους • Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα • Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή • Καταστροφή εξοπλισμού από υγρά/τρόφιμα • Διαρροή πληροφοριών • Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος • Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους • Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος • Μη εξουσιοδοτημένες αλλαγές αρχείων • Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος • Έλλειψη κινήτρων για τους εργαζόμενους • Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας • Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο • Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών • Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου • Έλλειψη απαιτούμενης εκπαίδευσης προσωπικού • Εσωτερικοί κίνδυνοι (δόλος)
Στρατηγικοί – Οργανωτικοί	• Λάθος κατανομή του κεφαλαίου • Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος • Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος • Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού • Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού • Λανθασμένη κοστολόγηση του έργου • Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές • Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου • Λανθασμένες αποφάσεις διαχείρισης κινδύνων
Φυσικοί – Περιβαλλοντικοί	• Κίνδυνος σεισμού • Κίνδυνος Κεραυνού • Κίνδυνος πλημμύρας • Κίνδυνος πυρκαγιάς

	• Κίνδυνος διαρροής υδάτων Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση • Κατολίσθηση – διάβρωση εδάφους • Ηλιακές εκλάμψεις • Σκόνη • Βλάβη του συστήματος κλιματισμού • Ηλεκτρομαγνητικές παρεμβολές • Στατικός ηλεκτρισμός • Έκρηξη ηφαιστείου • Πυρηνικό ατύχημα • Κίνδυνος εκρήξεων • Έντομα/ τρωκτικά • Κίνδυνος δονήσεων • Καπνός / μικροσωματίδια • Μαγνήτες/ μαγνητικά εργαλεία
Νομικοί – Κοινωνικοί	• Αγωγές – Μηνύσεις • Απώλεια καλής φήμης • Κλοπή πνευματικής ιδιοκτησίας
Πολιτικοί	• Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων • Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας
Εξωτερικοί	• κλοπή υλικού • Βανδαλισμοί • Εισβολείς (Hackers) – Υποκλοπή δεδομένων • Εισβολείς (Hackers) – Καταστροφή δεδομένων • Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού) • Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές • Κατασκοπεία • Τρομοκρατικές επιθέσεις

Πίνακας 2: Πίνακας κατηγοριοποίησης κινδύνων του συστήματος E-Prescription

Με το πέρας των παραπάνω, δημιουργείται το Μητρώο Κινδύνων (Risk Register), δηλαδή ένα έγγραφο όπου καταγράφονται όλοι οι κίνδυνοι που εντοπίζονται κατά τη φάση του προσδιορισμού και το οποίο γίνεται λεπτομερέστερο όσο προχωρούν τα στάδια της ανάλυσης και της αντιμετώπισης αυτών. Το μητρώο κινδύνων παρακολουθείται και ενημερώνεται σε τακτική βάση με σκοπό να υπάρχουν οργανωμένα και συγκεντρωμένα οι πληροφορίες των κινδύνων, της ανάλυσης, του τρόπου αντιμετώπισης και της κατάστασής τους. Στο μητρώο αυτό στηρίζεται η εφαρμογή της διαδικασίας διαχείρισης κινδύνων. Στη φάση του προσδιορισμού των κινδύνων, όπου το έγγραφο αυτό δημιουργείται, τα βασικά στοιχεία που πρέπει να αναγραφούν για τους κινδύνους φαίνονται στον παρακάτω πίνακα (Πίνακας 3).

Πιο αναλυτικά, στα παραπάνω πεδία συμπληρώνονται τα εξής στοιχεία:

- στο πεδίο «ονομασία» καταγράφεται η αντιπροσωπευτική ονομασία του κινδύνου που προσδιορίστηκε
- στο πεδίο «περιγραφή» καταγράφεται μία σύντομη περιγραφή του κινδύνου και της πιθανής συνέπειάς του
- στο πεδίο «κατηγορία» καταγράφεται η κατηγορία στην οποία ανήκει ο κίνδυνος
- στο πεδίο «ημερομηνία αναγνώρισης» καταγράφεται η ημερομηνία όπου πρωτοαναφέρθηκε ο κίνδυνος
- στο πεδίο «υπεύθυνος» καταγράφεται το όνομα του υπεύθυνου ή της υπεύθυνης ομάδας για τον κίνδυνο

#	Ονομασία	Περιγραφή	Κατηγορία	Ημερομηνία αναγνώρισης	Υπεύθυνος
1	Ασυμβατότητα λογισμικού με τις απαιτήσεις	Το ήδη υπάρχον λογισμικό δεν ανταποκρίνεται στις απαιτήσεις του συστήματος .	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
2	Εξάντληση πόρων του συστήματος	Εξάντληση των πόρων του συστήματος από την αυξημένη κίνηση των χρηστών του.	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
3	Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων	Λάθος ή ελλιπής δημιουργία της βάσης δεδομένων.	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
4	Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών	Έλλειψη μεθόδων προστασίας των προσωπικών δεδομένων - έλλειψη πρωτοκόλλων ασφαλείας με αποτέλεσμα την πιθανή υποκλοπή των προσωπικών δεδομένων των χρηστών.	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
5	Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού	Δημιουργία του κώδικα με μη δομημένο τρόπο με αποτέλεσμα την εμφάνιση δυσκολιών σε μελλοντικές αλλαγές και στην προσθήκη νέων λειτουργιών	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
6	Έλλειψη διασυνδεσιμότητας του φορέων μέσω του συστήματος	Ελλιπής χρήση τεχνολογιών λογισμικού και πρωτοκόλλων για την διασυνδεσιμότητα μεταξύ των συσχετιζόμενων φορέων (π.χ. υπουργείο υγείας, ΓΓΚΑ, ΗΔΙΚΑ, Φ.Κ.Α).	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
7	Λανθασμένος σχεδιασμός υλικού του συστήματος	Ανεπαρκής σχεδιασμός υλικού σε επίπεδο αρχιτεκτονικής συστήματος.	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
8	Λανθασμένος σχεδιασμός λογισμικού του συστήματος	Ανεπαρκής σχεδιασμός λογισμικού σε επίπεδο αρχιτεκτονικής συστήματος.	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
9	Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	Επιλογή τεχνολογίας λογισμικού μη συμβατή με την υπάρχουσα δικτυακή υποδομή των συσχετιζόμενων φορέων.	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
10	Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	Επιλογή λογισμικού τελευταίας τεχνολογίας όπου δεν έχει ελεγχθεί εκτενώς όσον αφορά την ανάπτυξη αντίστοιχων εφαρμογών .	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
11	Μη αποδεκτή ποιότητα λογισμικού	Η ποιότητα της εφαρμογής είναι χαμηλότερη των αποδεκτών ορίων που έχουν τεθεί και προβληματική για τους χρήστες.	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
12	Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του λογισμικού του πληροφοριακού συστήματος	Ελλιπής χρήσης λογισμικού ασφαλείας και αυστηρών μέτρων προστασίας για την αποφυγή κακόβουλων ενεργειών και υποκλοπή προσωπικών δεδομένων.	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
13	Αδυναμία σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	Ανεπαρκής διαδικτυακός εξοπλισμός για την αποτελεσματική εξυπηρέτηση του αριθμού των συνδεδεμένων χρηστών σε περιπτώσεις υψηλού φόρτου.	Τεχνολογικοί	23/10/2013	Κυρίτση Β.

14	Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	Λανθασμένη χρήση τεχνικών κρυπτογραφίας κλειδιών.	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
15	Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	Λανθασμένος κώδικας για τον έλεγχό της επεξεργασίας των δεδομένων εισαγωγής	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
16	Δυσλειτουργία του υλικού	Αστοχία του υλικού που είναι αποθηκευμένο το πληροφοριακό σύστημα.	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
17	Ανεπαρκής έλεγχος λογισμικού	Ανεπαρκείς και ελλιπείς διαδικασίες ποιοτικού ελέγχου.	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
18	Σφάλματα λογισμικού	Εμφάνιση μεγάλου αριθμού λαθών στον κώδικα του πληροφοριακού συστήματος.	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
19	Πολυπλοκότητα λογισμικού	Μη τήρηση συγκεκριμένης μεθοδολογίας για τη συγγραφή κώδικα του πληροφοριακού συστήματος.	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
20	Μη ασφαλής αρχιτεκτονική δικτύου	Ανεπαρκής επιλογή επιπέδων ασφάλειας διαδικτύου.	Τεχνολογικοί	23/10/2013	Κυρίτση Β.
21	Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	Αδυναμία αποτελεσματικής επικοινωνίας με την εταιρεία ανάθεσης με αποτέλεσμα την επιβράδυνση των εργασιών για την κατασκευή του έργου.	Λειτουργικοί - Επιχειρησιακοί	23/10/2013	Κυρίτση Β.
22	Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	Ασάφειες και κενά στους όρους του συμβολαίου οδηγούν στην ανεπαρκή εφαρμογή των συμφωνηθέντων στην περίπτωση εμφάνισης προβλήματος.	Λειτουργικοί - Επιχειρησιακοί	23/10/2013	Κυρίτση Β.
23	Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	Ανεπαρκής αριθμός ατόμων για την υποστήριξη του συστήματος λόγω κόστους σε ανθρώπινο δυναμικό.	Λειτουργικοί - Επιχειρησιακοί	23/10/2013	Κυρίτση Β.
24	Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.	Προβλήματα επικοινωνίας και καταμερισμού εργασιών των ομάδων ανάπτυξης λογισμικού με αποτέλεσμα τη δημιουργία εντάσεων μεταξύ των ατόμων και την διακοπή της ομαλής εξέλιξης του έργου	Λειτουργικοί - Επιχειρησιακοί	23/10/2013	Κυρίτση Β.
25	Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)	Η έλλειψη φύλαξης ενός κτηρίου από άτομο επιπλέον των τεχνικών μέσων μπορεί να έχει ως αποτέλεσμα την μη έγκαιρη αντιμετώπιση οποιασδήποτε πιθανή καταστροφής του κτηρίου όπου στεγάζεται το πληροφοριακό σύστημα.	Λειτουργικοί - Επιχειρησιακοί	23/10/2013	Κυρίτση Β.
26	Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	Δεν έχει δοθεί αρκετό χρονικό διάστημα για την εξοικείωση των χρηστών (ιατροί, φαρμακοποιοί) με το νέο λογισμικό ώστε να υπάρχουν προβλήματα στη σύνταξη των συνταγών (χειρόγραφες, ηλεκτρονικές) με αποτέλεσμα την προβληματική εξυπηρέτηση των πολιτών.	Λειτουργικοί - Επιχειρησιακοί	23/10/2013	Κυρίτση Β.
27	Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων	Ελλιπής ή λανθασμένη επιλογή ατόμων για την υλοποίηση μερών του πληροφοριακού συστήματος.	Λειτουργικοί - Επιχειρησιακοί	23/10/2013	Κυρίτση Β.

28	Ανεπαρκής επίβλεψη εργαζομένων	Ελλιπής επιλογή κατάλληλων ατόμων για επίβλεψη των εργαζομένων με αποτέλεσμα τη μη τήρηση του χρονοδιαγράμματος.	Λειτουργικοί - Επιχειρησιακοί	23/10/2013	Κυρίτση Β.
29	Ελλιπής διαδικασία για την αφαίρεση δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης	Η διαδικασία διακοπής συνεργασίας δεν πληροί όλες τις προϋποθέσεις που χρειάζονται για τη μη πρόσβαση των πρώην εργαζομένων στο πληροφοριακό σύστημα και στους χώρους του πληροφοριακού συστήματος.	Λειτουργικοί - Επιχειρησιακοί	23/10/2013	Κυρίτση Β.
30	Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	Ανεπαρκής διαδικασία τακτικού ελέγχου της λειτουργίας του λογισμικού.	Λειτουργικοί - Επιχειρησιακοί	23/10/2013	Κυρίτση Β.
31	Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας	Εσφαλμένη εγκατάσταση υλικού ή λογισμικού λόγω έλλειψης τεχνικών γνώσεων ή εξαιτίας απλού ανθρώπινου σφάλματος του προσωπικού.	Λειτουργικοί - Επιχειρησιακοί	23/10/2013	Κυρίτση Β.
32	Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	Μη εγκατεστημένο σύστημα ειδοποίησης σε περίπτωση εισβολής στο χώρο του πληροφοριακού συστήματος.	Λειτουργικοί - Επιχειρησιακοί	23/10/2013	Κυρίτση Β.
33	Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	Μη εγκατεστημένο σύστημα ειδοποίησης σε περίπτωση πυρκαγιάς.	Λειτουργικοί - Επιχειρησιακοί	23/10/2013	Κυρίτση Β.
34	Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	Μη εγκατεστημένο σύστημα αναγνώρισης και ελέγχου ταυτότητας για την είσοδο στους χώρους του πληροφοριακού συστήματος.	Λειτουργικοί - Επιχειρησιακοί	23/10/2013	Κυρίτση Β.
35	Έλλειψη οικονομικών πόρων	Ανεπαρκείς οικονομικοί πόροι οδηγούν σε αδυναμία έναρξης ή ολοκλήρωσης του πληροφοριακού συστήματος	Χρηματοοικονομικοί	23/10/2013	Κυρίτση Β.
36	Προβλήματα με την χρηματοδότηση του έργου	Συνεχόμενες διακοπές κατά την υλοποίηση του έργου λόγω προβλημάτων στη χρηματοδότηση με αποτέλεσμα την χρονική καθυστέρηση και την αύξηση του κόστους.	Χρηματοοικονομικοί	23/10/2013	Κυρίτση Β.
37	Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος	Καταστροφή υλικού ή λογισμικού του συστήματος λόγω κακής χρήσης του.	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
38	Κλοπή υλικού από εργαζομένους	Το υλικό ενδέχεται να κλαπεί από τους εργαζόμενους .	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
39	Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	Καθυστέρηση στην υλοποίηση του έργου λόγω απεργιακών κινητοποιήσεων από τους εργαζόμενους.	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
40	Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	Απροθυμία των εργαζομένων του πληροφοριακού συστήματος να προσαρμοστούν στα νέα δεδομένα του εργασιακού τους περιβάλλοντος.	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
41	Καταστροφή εξοπλισμού από υγρά/τρόφιμα	Καταστροφή υλικού του πληροφοριακού συστήματος από επικίνδυνα υλικά που δεν επιτρέπονται κοντά στον εξοπλισμό (π.χ. τρόφιμα, υγρά).	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
42	Διαρροή πληροφοριών	Διάδοση εμπιστευτικών πληροφοριών που αφορούν προσωπικά δεδομένα από εργαζόμενους σε μη εξουσιοδοτημένα άτομα.	Ανθρώπινοι	23/10/2013	Κυρίτση Β.

43	Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	Ικανότητα μη εξουσιοδοτημένων ατόμων να έχουν πρόσβαση στους χώρους όπου βρίσκεται το πληροφοριακό σύστημα με αποτέλεσμα την πρόκληση φθοράς του εξοπλισμού.	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
44	Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους	Ικανότητα μη εξουσιοδοτημένων ατόμων να έχουν πρόσβαση στο πληροφοριακό σύστημα με αποτέλεσμα την πρόκληση καταστροφής του λογισμικού .	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
45	Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	Γνωστοποίηση των κωδικών εισόδου του πληροφοριακού συστήματος σε μη εξουσιοδοτημένα άτομα.	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
46	Μη εξουσιοδοτημένες αλλαγές αρχείων	Ελλιπή μηχανισμός κατανομής δικαιωμάτων διαχείρισης στους εργαζομένους του πληροφοριακού συστήματος με αποτέλεσμα τη δυνατότητα πρόσβαση όλων των εργαζομένων σε όλα τα μέρη του συστήματος .	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
47	Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος	Μη εσκεμμένη αλλαγή των δεδομένων .	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
48	Έλλειψη κινήτρων για τους εργαζόμενους	Μη ύπαρξη διαδικασίας ανταμοιβής για τους εργαζόμενους.	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
49	Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	Ελλιπής εκπαίδευση εργαζομένων σε θέματα ασφαλείας του πληροφοριακού συστήματος.	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
50	Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο	Ο κάθε εργαζόμενος μπορεί να χρησιμοποιήσει δικές του συσκευές για να συνδεθεί στο δίκτυο της εταιρείας με αποτέλεσμα τη διάδοση κακόβουλου λογισμικού	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
51	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	Εγκατάσταση επικίνδυνου για το πληροφοριακό σύστημα λογισμικού και εφαρμογών.	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
52	Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	Μη εσκεμμένη διάδοση προσωπικών δεδομένων μέσω συσκευών αποθήκευσης (π.χ. σκληρός δίσκος.)	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
53	Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	Μη επαρκής επιμόρφωση των εργαζομένων προκειμένου να ανταπεξέλθουν στις νέες απαιτήσεις.	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
54	Εσωτερικοί κίνδυνοι (δόλος)	Κίνδυνος δολιοφθορών του πληροφοριακού συστήματος από δυσαρεστημένα στελέχη ή υπαλλήλους που εργάζονται στον οργανισμό.	Ανθρώπινοι	23/10/2013	Κυρίτση Β.
55	Λάθος κατανομή του κεφαλαίου	Λανθασμένη πρόβλεψη κοστολόγησης τμημάτων του πληροφοριακού συστήματος έτσι ώστε σε μερικά τμήματα του έργου να είναι αναγκαία η ανακοστολόγηση και αυτό να έχει ως αποτέλεσμα την καθυστέρηση του έργου.	Στρατηγικοί - Οργανωτικοί	23/10/2013	Κυρίτση Β.

56	Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	Λανθασμένη βαρύτητα κατά το σχεδιασμό των μερών του πληροφοριακού συστήματος μπορεί να οδηγήσει σε αναθεώρηση ορισμένων από αυτά και επανασχεδιασμού του έργου συνολικά.	Στρατηγικοί - Οργανωτικοί	23/10/2013	Κυρίτση Β.
57	Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	Έλλειψη εφεδρικού σχεδίου σε περίπτωση διακοπής ηλεκτροδότησης ή σε περίπτωση προβλημάτων λειτουργίας των διακομιστών που υποστηρίζουν το πληροφοριακό σύστημα .	Στρατηγικοί - Οργανωτικοί	23/10/2013	Κυρίτση Β.
58	Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	Έλλειψη υλικών πόρων (π.χ. διακομιστές, καλωδίωση κτιρίου κ.τ.λ.)χρήσιμων για την κατασκευή του έργου λόγω λανθασμένης αρχικής πρόβλεψης.	Στρατηγικοί - Οργανωτικοί	23/10/2013	Κυρίτση Β.
59	Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	Επιλογή ακολουθίας εργασιών διάφορη της βέλτιστης που έχει ως αποτέλεσμα την χρονική επιμήκυνση του έργου σε σχέση με τη βέλτιστη επιλογή.	Στρατηγικοί - Οργανωτικοί	23/10/2013	Κυρίτση Β.
60	Λανθασμένη κοστολόγηση του έργου	Το κόστος υλοποίησης του συστήματος αυξήθηκε, θέτοντας σε κίνδυνο την υπόσταση του έργου.	Στρατηγικοί - Οργανωτικοί	23/10/2013	Κυρίτση Β.
61	Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	Πρόσβαση σε εμπιστευτικά δεδομένα από συνεργάτες και προμηθευτές .	Στρατηγικοί - Οργανωτικοί	23/10/2013	Κυρίτση Β.
62	Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	Παρακολούθηση της υλοποίησης του πληροφοριακού συστήματος από άτομα με καθόλου ή λίγη εμπειρία και με ελλιπής γνώσεις τεχνογνωσίας καθώς και ελλιπής γνώσεις τα οποία σε μελλοντικό χρόνο θα κληθούν να λάβουν σημαντικές αποφάσεις κάτω από πιθανές συνθήκες πίεσης ή έλλειψης χρόνου.	Στρατηγικοί - Οργανωτικοί	23/10/2013	Κυρίτση Β.
63	Λανθασμένες αποφάσεις διαχείρισης κινδύνων	Έλλειψη εμπειρίας των ατόμων που λαμβάνουν τις αποφάσεις διαχείρισης κινδύνων του έργου με αποτέλεσμα την ανεπαρκή αντιμετώπιση των κινδύνων.	Στρατηγικοί - οργανωτικοί	23/10/2013	Κυρίτση Β.
64	Κίνδυνος σεισμού	Καταστροφή του κτιρίου που στεγάζεται το πληροφοριακό σύστημα λόγω σεισμού .	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
65	Κίνδυνος Κεραυνού	Καταστροφή στην ηλεκτροδότηση του κτιρίου λόγω κεραυνού που προκλήθηκε από ακραία καιρικά φαινόμενα .	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
66	Κίνδυνος πλημμύρας	Καταστροφή του χώρου που στεγάζεται το σύστημα λόγω ακραίων καιρικών φαινομένων.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
67	Κίνδυνος πυρκαγιάς	Κίνδυνος εκδήλωσης πυρκαγιάς στο χώρο της εγκατάστασης ή σε γειτονικά κτίρια από φυσικά αίτια ή τεχνητά.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
68	Κίνδυνος διαρροής υδάτων	Καταστροφή του χώρου που στεγάζεται το σύστημα από πλημμύρα που οφείλεται σε διαρροή υδάτων λόγω παλαιότητας ή κακής κατασκευής του δικτύου υδροδότησης.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.

69	Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	Αδυναμία ηλεκτροδότησης μέσω της εγκατάστασης του κτιρίου που στεγάζεται το σύστημα λόγω ελλιπούς υποστήριξης σε περιπτώσεις διακοπής της ηλεκτροδότησης.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
70	Κατολίσθηση – διάβρωση εδάφους	Καταστροφή κτιρίου που στεγάζεται το πληροφοριακό σύστημα λόγω κατολίσθησης ή διάβρωσης εδάφους.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
71	Ηλιακές εκλάμψεις	Προβληματική λειτουργία του δικτύου λόγω ηλιακών εκλάμψεων.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
72	Σκόνη	Βλάβες ή δυσλειτουργία υλικού λόγω σκόνης.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
73	Βλάβη του συστήματος κλιματισμού	Καταστροφή από υπερθέρμανση του εξοπλισμού του πληροφοριακού συστήματος λόγω βλάβης του κλιματισμού.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
74	Ηλεκτρομαγνητικές παρεμβολές	Προβληματική λειτουργία του δικτύου λόγω ηλεκτρομαγνητικών παρεμβολών.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
75	Στατικός ηλεκτρισμός	Καταστροφή του εξοπλισμού του πληροφοριακού συστήματος λόγω διαρροής ρεύματος.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
76	Έκρηξη ηφαιστείου	Εγκατάσταση του πληροφοριακού συστήματος ή του διακομιστή του πληροφοριακού συστήματος σε περιοχή που είναι επιρρεπής στις ηφαιστειακές εκρήξεις.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
77	Πυρηνικό ατύχημα	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή όπου βρίσκονται πυρηνικά εργοστάσια.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
78	Κίνδυνος εκρήξεων	Εγκατάσταση του πληροφοριακού συστήματος σε χώρο όπου βρίσκονται εύφλεκτα υλικά .	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
79	Έντομα – τρωκτικά	Εγκατάσταση του πληροφοριακού συστήματος σε κτίριο όπου δεν έχει την κατάλληλη υποδομή και την απαραίτητη προστασία με αποτέλεσμα να εισβάλλουν στο χώρο διάφορα έντομα και τρωκτικά και να προκαλέσουν ζημιά στο υλικό του συστήματος.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
80	Κίνδυνος δονήσεων	Εγκατάσταση πληροφοριακού συστήματος σε περιοχή κοντά σε σιδηροδρομικό σταθμό ή σε εργοτάξιο.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
81	Καπνός - Μικροσωματίδια	Εγκατάσταση πληροφοριακού συστήματος σε σημείο όπου υπάρχουν μεγάλες ποσότητες καπνού και μικροσωματιδίων οι οποίες μπορεί να προκαλέσουν ζημιά στον εξοπλισμό του συστήματος.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
82	Μαγνήτες – μαγνητικά εργαλεία	Χρήση μαγνητών ή μαγνητικών εργαλείων μπορούν να προκαλέσουν βλάβη σε ευαίσθητο εξοπλισμό ή να διαγράψουν δεδομένα.	Φυσικοί - Περιβαλλοντικοί	23/10/2013	Κυρίτση Β.
83	Αγωγές – Μηνύσεις	Παράβλεψη ή καταπάτηση νομοθετικών ρυθμίσεων ή υπάρχουσας νομοθεσίας όσον αφορά τις διαδικασίες μετάδοσης πληροφορίας και τήρησης αρχείων προσωπικών δεδομένων.	Νομικοί - Κοινωνικοί	23/10/2013	Κυρίτση Β.

84	Απώλεια καλής φήμης	Μη αποτελεσματική λειτουργία του συστήματος λόγω λανθασμένου σχεδιασμού με αποτέλεσμα τη δυσαρέσκεια των τελικών χρηστών του συστήματος.	Νομικοί - Κοινωνικοί	23/10/2013	Κυρίτση Β.
85	Κλοπή πνευματικής ιδιοκτησίας	Κλοπή μερών του λογισμικού του πληροφοριακού συστήματος από ανταγωνίστρια εταιρεία το οποίο υπόκειται σε καθεστώς πνευματικής ιδιοκτησίας.	Νομικοί - Κοινωνικοί	23/10/2013	Κυρίτση Β.
86	Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	Αλλαγή πολιτικής ηγεσίας με αποτέλεσμα την αλλαγή ή ματαίωση κατασκευής του συστήματος και την ύπαρξη χρονικής καθυστέρησης ή κόστους.	Πολιτικοί	23/10/2013	Κυρίτση Β.
87	Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή με πολιτικές αναταραχές / πολέμους.	Πολιτικοί	23/10/2013	Κυρίτση Β.
88	Κλοπή υλικού	Εισβολή αγνώστων ατόμων στο κτίριο που στεγάζεται το πληροφοριακό σύστημα με αποτέλεσμα την κλοπή υλικού απαραίτητου για τη σωστή λειτουργία του.	Εξωτερικοί	23/10/2013	Κυρίτση Β.
89	Βανδαλισμοί	Καταστροφή του εξοπλισμού από βανδαλισμούς αγνώστων ατόμων.	Εξωτερικοί	23/10/2013	Κυρίτση Β.
90	Εισβολείς (Hackers) – Υποκλοπή δεδομένων	Προσβολή του συστήματος από την επιδρομή hackers με αποτέλεσμα την ύπαρξη κινδύνου υποκλοπής μεταδιδόμενων πληροφοριών.	Εξωτερικοί	23/10/2013	Κυρίτση Β.
91	Εισβολείς (Hackers) – Καταστροφή δεδομένων	Προσβολή του συστήματος από την επιδρομή hackers με αποτέλεσμα την ύπαρξη κινδύνου καταστροφής δεδομένων.	Εξωτερικοί	23/10/2013	Κυρίτση Β.
92	Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού)	Προσβολή του συστήματος από ηλεκτρονικούς εγκληματίες με αποτέλεσμα την αλλοίωση ή καταστροφή των αποθηκευμένων δεδομένων του συστήματος.	Εξωτερικοί	23/10/2013	Κυρίτση Β.
93	Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	Αντιγραφή μερών ή ολόκληρου του σχεδιασμού του πληροφοριακού συστήματος από πρώην εργαζόμενους	Εξωτερικοί	23/10/2013	Κυρίτση Β.
94	Κατασκοπεία	Υποκλοπή ευαίσθητων προσωπικών δεδομένων του πληθυσμού από εχθρικά κράτη.	Εξωτερικοί	23/10/2013	Κυρίτση Β.
95	Τρομοκρατικές ενέργειες	Καταστροφή των εγκαταστάσεων που στεγάζεται το πληροφοριακό σύστημα λόγω τρομοκρατικών επιθέσεων σε διπλανό κτίριο ή και στο ίδιο κτίριο.	Εξωτερικοί	23/10/2013	Κυρίτση Β.

Πίνακας 3: Μητρώο κινδύνων - Προσδιορισμός κινδύνων συστήματος E- Prescription

6.3 Ανάλυση κινδύνων

Στη φάση αυτή πρέπει να γίνει ποιοτική ανάλυση των κίνδυνων επομένως πρέπει να ομαδοποιηθούν οι κίνδυνοι με βάση τη σημαντικότητά τους και να αναπαρασταθούν σε έναν πίνακα κινδύνων.

Έστω ότι ο πίνακας κινδύνων της ποιοτικής ανάλυσης του συστήματος ηλεκτρονικής συνταγογράφησης ορίζεται ως εξής:

Επίπεδο κινδύνου / Πιθανότητα	Πολύ χαμηλό (1)	Χαμηλό (2)	Μέτριο (3)	Υψηλό (4)	Πολύ Υψηλό (5)
Πολύ χαμηλή (0.1)	0.10	0.20	0.30	0.40	0.50
Χαμηλή (0.3)	0.30	0.60	0.90	1.20	1.50
Μέση (0.5)	0.50	1.00	1.50	2.00	2.50
Υψηλή (0.7)	0.70	1.40	2.10	2.80	3.50
Πολύ Υψηλή (0.9)	0.90	1.80	2.70	3.60	4.50

Πίνακας 4: Risk matrix ποιοτικής ανάλυσης του συστήματος E- Prescription

Y(2.50-4.50) : Υψηλός κίνδυνος, δηλαδή μη αποδεκτός ο οποίος χρειάζεται άμεση αντίδραση
M(0.90-2.10) : Μέσος κίνδυνος, δηλαδή μπορεί να χρειάζεται αντίδραση
X(0.10-0.70): Χαμηλός κίνδυνος, δηλαδή δε χρειάζεται αντίδραση αλλά απλή παρακολούθηση

Επίπεδο κινδύνου / Πιθανότητα	Πολύ χαμηλό (1)	Χαμηλό (2)	Μέτριο (3)	Υψηλό (4)	Πολύ Υψηλό (5)
Πολύ χαμηλή (0.1)	X_7	X_6	X_5	X_4	X_3
Χαμηλή (0.3)	X_5	X_2	M_8	M_6	M_4
Μέση (0.5)	X_3	M_7	M_4	M_2	Y_6
Υψηλή (0.7)	X_1	M_5	M_1	Y_4	Y_3
Πολύ Υψηλή (0.9)	M_8	M_3	Y_5	Y_2	Y_1

Πίνακας 4.1: Risk matrix ποιοτικής ανάλυσης του συστήματος E- Prescription

X_1: 0.70 , X_2:0.60 , X_3:0.50, X_4:0.40, X_5:0.30, X_6:0.20, X_7:0.10
M_1:2.10 , M_2: 2.00, M_3: 1.80, M_4:1.50, M_5:1.40, M_6:1.20, M_7:1.00, M_8:0.90
Y_1: 4.50, Y_2: 360, Y_3: 3.50 , Y_4:2.80, Y_5:2.70, Y_6:2.50

Στον παραπάνω πίνακα 4.1 οι κίνδυνοι έχουν ομαδοποιηθεί σε υποκατηγορίες των υψηλών, μέσων και χαμηλών κινδύνων, ώστε να γίνεται περισσότερο αντιληπτός ο διαχωρισμός της επικινδυνότητας αυτών. Πιο συγκεκριμένα, ο κίνδυνος που ανήκει στην κατηγορία Υ1 είναι περισσότερο επικίνδυνος από τον κίνδυνο που ανήκει στην κατηγορία Υ2 και αυτός με τη σειρά του είναι περισσότερο επικίνδυνος από τον κίνδυνο που ανήκει στην κατηγορία Υ3 και ούτω καθεξής. Το ίδιο ισχύει και για τους μέσους και τους χαμηλούς κινδύνους. Έτσι ο βαθμός επικινδυνότητας των κινδύνων από τον πιο μεγάλο στον πιο μικρό, δηλαδή από τον πιο σοβαρό κίνδυνο στον πιο ακίνδυνο, ορίζεται ως εξής:

$Y_1 \rightarrow Y_2 \rightarrow Y_3 \rightarrow Y_4 \rightarrow Y_5 \rightarrow Y_6 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow M_4 \rightarrow M_5 \rightarrow M_6 \rightarrow M_7 \rightarrow M_8 \rightarrow X_1 \rightarrow X_2 \rightarrow X_3 \rightarrow X_4 \rightarrow X_5 \rightarrow X_6 \rightarrow X_7$

Στον παρακάτω πίνακα (Πίνακας 5) ορίζονται η πιθανότητα και το επίπεδο κινδύνου του κάθε κινδύνου που έχει προσδιοριστεί και με βάση τον πίνακα κινδύνων βρίσκεται η έκθεση του κάθε κινδύνου, ώστε να γίνει η ποιοτική ανάλυση.

Κίνδυνοι	Πιθανότητα	Επίπεδο	Έκθεση
Ασυμβατότητα λογισμικού με τις απαιτήσεις	0.1	5	X_3
Εξάντληση πόρων του συστήματος	0.5	5	Y_6
Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων	0.1	5	X_3
Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών	0.9	5	Y_1
Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού	0.3	4	M_6
Έλλειψη διασυνδεσιμότητας του φορέων μέσω του συστήματος	0.5	3	M_4
Λανθασμένος σχεδιασμός υλικού του συστήματος	0.1	5	X_3
Λανθασμένος σχεδιασμός λογισμικού του συστήματος	0.1	5	X_3
Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	0.3	5	M_4
Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	0.5	3	M_4
Μη αποδεκτή ποιότητα λογισμικού	0.5	3	X_3
Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του πληροφοριακού συστήματος	0.1	5	M_2
Αδυναμία σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	0.5	4	M_1
Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	0.3	4	M_6
Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	0.3	4	M_6
Δυσλειτουργία του υλικού	0.5	4	M_2
Ανεπαρκής έλεγχος λογισμικού	0.5	4	M_2
Σφάλματα λογισμικού	0.5	5	Y_6
Πολυπλοκότητα λογισμικού	0.5	3	M_4
Μη ασφαλής αρχιτεκτονική δικτύου	0.5	4	M_2
Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	0.5	2	M_7
Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	0.5	2	M_7
Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	0.5	4	M_2
Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου	0.5	3	M_4
Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)	0.3	5	M_4
Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	0.7	2	M_5
Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων	0.7	3	M_1
Ανεπαρκής επίβλεψη εργαζομένων	0.5	4	M_2
Ελλιπής διαδικασία για την αφαίρεση δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης	0.3	4	M_6
Ελλιπής σχεδιασμό τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	0.7	3	M_1
Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας	0.5	5	Y_6
Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	0.7	4	Y_4
Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	0.7	4	Y_4
Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	0.7	4	Y_4
Έλλειψη οικονομικών πόρων	0.5	3	M_4
Προβλήματα με την χρηματοδότηση του έργου	0.7	2	M_5

Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος	0.7	4	Y_4
Κλοπή υλικού από εργαζομένους	0.7	4	Y_4
Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	0.5	4	M_2
Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	0.7	4	Y_4
Καταστροφή εξοπλισμού από υγρά/τρόφιμα	0.5	4	M_2
Διαρροή πληροφοριών	0.7	4	Y_4
Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	0.7	4	Y_4
Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους	0.7	5	Y_3
Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	0.7	5	Y_3
Μη εξουσιοδοτημένες αλλαγές αρχείων	0.3	5	M_4
Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος	0.3	5	M_4
Έλλειψη κινήτρων για τους εργαζόμενους	0.5	4	M_2
Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	0.7	4	Y_4
Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο	0.7	4	Y_4
Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	0.3	5	M_4
Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	0.5	4	M_2
Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	0.7	1	X_1
Εσωτερικοί κίνδυνοι (δόλος)	0.3	3	M_8
Λάθος κατανομή του κεφαλαίου	0.3	3	M_8
Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	0.3	4	M_6
Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	0.5	4	M_2
Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	0.5	3	M_4
Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	0.5	2	M_7
Λανθασμένη κοστολόγηση του έργου	0.5	3	M_4
Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	0.3	3	M_8
Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	0.3	4	M_6
Λανθασμένες αποφάσεις διαχείρισης κινδύνων	0.1	4	X_4
Κίνδυνος σεισμού	0.5	3	M_4
Κίνδυνος Κεραυνού	0.3	4	M_6
Κίνδυνος πλημμύρας	0.3	4	M_6
Κίνδυνος πυρκαγιάς	0.7	4	Y_4
Κίνδυνος διαρροής υδάτων	0.1	4	X_4
Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	0.3	4	M_6
Κατολίσθηση – διάβρωση εδάφους	0.1	5	X_3
Ηλιακές εκλάμψεις	0.1	3	X_5
Σκόνη	0.5	2	M_7
Βλάβη του συστήματος κλιματισμού	0.3	4	M_6

Ηλεκτρομαγνητικές παρεμβολές	0.3	3	M_8
Στατικός ηλεκτρισμός	0.1	4	X_4
Έκρηξη ηφαιστείου	0.1	5	X_3
Πυρηνικό ατύχημα	0.1	5	X_3
Κίνδυνος εκρήξεων	0.3	5	M_4
Έντομα /τρωκτικά	0.5	4	M_2
Κίνδυνος δονήσεων	0.3	4	M_6
Καπνός / μικροσωματίδια	0.3	4	M_6
Μαγνήτες /μαγνητικά εργαλεία	0.5	5	Y_6
Αγωγές/ Μηνύσεις	0.1	2	X_6
Απώλεια καλής φήμης	0.1	3	X_5
Κλοπή πνευματικής ιδιοκτησίας	0.3	2	X_2
Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	0.1	3	X_5
Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	0.1	5	X_3
Κλοπή υλικού	0.3	4	M_6
Βανδαλισμοί	0.3	4	M_6
Εισβολείς (Hackers) – Υποκλοπή δεδομένων	0.7	5	Y_3
Εισβολείς (Hackers) – Καταστροφή δεδομένων	0.7	5	Y_3
Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού)	0.9	5	Y_1
Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	0.5	3	M_4
Κατασκοπεία	0.3	4	M_6
Τρομοκρατικές ενέργειες	0.3	4	M_6

Πίνακας 5: Εκθέσεις κινδύνων συστήματος E-Prescription

6.4 Αξιολόγηση κινδύνων

Στη φάση αυτή οι κίνδυνοι που έχουν προσδιοριστεί και αναλυθεί ταξινομούνται ανάλογα με την έκθεση κινδύνου που βρέθηκε προηγουμένως και ενημερώνεται το μητρώο κινδύνων.

Στον παρακάτω πίνακα φαίνεται η ταξινόμηση των κινδύνων σύμφωνα με την έκθεσή τους, με σειρά προτεραιότητας από τον σημαντικότερο στον πιο ασήμαντο.

Κίνδυνοι	Πιθανότητα	Επίπεδο	Έκθεση
Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών	0.9	5	Y_1
Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού)	0.9	5	Y_1
Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους	0.7	5	Y_3
Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	0.7	5	Y_3
Εισβολείς (Hackers) – Υποκλοπή δεδομένων	0.7	5	Y_3
Εισβολείς (Hackers) – Καταστροφή δεδομένων	0.7	5	Y_3
Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	0.7	4	Y_4
Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	0.7	4	Y_4
Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	0.7	4	Y_4
Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος	0.7	4	Y_4
Κλοπή υλικού από εργαζομένους	0.7	4	Y_4
Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	0.7	4	Y_4
Διαρροή πληροφοριών	0.7	4	Y_4
Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	0.7	4	Y_4
Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	0.7	4	Y_4
Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο	0.7	4	Y_4
Κίνδυνος πυρκαγιάς	0.7	4	Y_4
Εξάντληση πόρων του συστήματος	0.5	5	Y_6
Σφάλματα λογισμικού	0.5	5	Y_6
Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας	0.5	5	Y_6
Μαγνήτες / μαγνητικά εργαλεία	0.5	5	Y_6
Ανεπαρκής ή λανθασμένος διαχωρισμός καθηκόντων	0.7	3	M_1
Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	0.7	3	M_1
Αδυναμία Σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	0.5	4	M_2
Δυσλειτουργία του υλικού	0.5	4	M_2
Ανεπαρκής έλεγχος του λογισμικού	0.5	4	M_2
Μη ασφαλής αρχιτεκτονική δικτύου	0.5	4	M_2
Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	0.5	4	M_2
Ανεπαρκής επίβλεψη των εργαζομένων	0.5	4	M_2
Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	0.5	4	M_2
Καταστροφή εξοπλισμού από υγρά/τρόφιμα	0.5	4	M_2
Έλλειψη κινήτρων για τους εργαζόμενους	0.5	4	M_2
Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	0.5	4	M_2
Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	0.5	4	M_2
Έντομα / τρωκτικά	0.5	4	M_2
Έλλειψη διασυνδεσιμότητας των φορέων μέσω του συστήματος	0.5	3	M_4

Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	0.5	3	M_4
Μη αποδεκτή ποιότητα λογισμικού	0.5	3	M_4
Πολυπλοκότητα λογισμικού	0.5	3	M_4
Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου	0.5	3	M_4
Έλλειψη οικονομικών πόρων	0.5	3	M_4
Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	0.5	3	M_4
Λανθασμένη κοστολόγηση του έργου	0.5	3	M_4
Κίνδυνος σεισμού	0.5	3	M_4
Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	0.5	3	M_4
Ασυμβατότητα τις τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	0.3	5	M_4
Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα (φύλακες)	0.3	5	M_4
Μη εξουσιοδοτημένες αλλαγές αρχείων	0.3	5	M_4
Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος	0.3	5	M_4
Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	0.3	5	M_4
Κίνδυνος εκρήξεων	0.3	5	M_4
Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	0.7	2	M_5
Προβλήματα με την χρηματοδότηση του έργου	0.7	2	M_5
Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού	0.3	4	M_6
Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	0.3	4	M_6
Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	0.3	4	M_6
Ελλιπής διαδικασία για την αφαίρεση των δικαιωμάτων πρόσβασης κατά τη λήξη της απασχόλησης	0.3	4	M_6
Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	0.3	4	M_6
Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου.	0.3	4	M_6
Κίνδυνος Κεραυνού	0.3	4	M_6
Κίνδυνος πλημμύρας	0.3	4	M_6
Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	0.3	4	M_6
Βλάβη του συστήματος κλιματισμού	0.3	4	M_6
Κίνδυνος δονήσεων	0.3	4	M_6
Καπνός - Μικροσωματίδια	0.3	4	M_6
Κλοπή υλικού	0.3	4	M_6
Βανδαλισμοί	0.3	4	M_6
Κατασκοπεία	0.3	4	M_6
Τρομοκρατικές επιθέσεις	0.3	4	M_6
Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	0.5	2	M_7
Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	0.5	2	M_7
Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	0.5	2	M_7
Σκόνη	0.5	2	M_7

Εσωτερικοί κίνδυνοι (δόλος)	0.3	3	M_8
Λάθος κατανομή του κεφαλαίου	0.3	3	M_8
Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	0.3	3	M_8
Ηλεκτρομαγνητικές παρεμβολές	0.3	3	M_8
Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	0.7	1	X_1
Κλοπή πνευματικής ιδιοκτησίας	0.3	2	X_2
Ασυμβατότητα λογισμικού με τις απαιτήσεις	0.1	5	X_3
Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων	0.1	5	X_3
Λανθασμένος σχεδιασμός υλικού (αρχιτεκτονική συστήματος)	0.1	5	X_3
Λανθασμένος σχεδιασμός λογισμικού(αρχιτεκτονική συστήματος)	0.1	5	X_3
Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του λογισμικού του πληροφοριακού συστήματος	0.1	5	X_3
Κατολίσθηση – διάβρωση εδάφους	0.1	5	X_3
Έκρηξη ηφαιστείου	0.1	5	X_3
Πυρηνικό ατύχημα	0.1	5	X_3
Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	0.1	5	X_3
Λανθασμένες αποφάσεις διαχείρισης κινδύνων	0.1	4	X_4
Κίνδυνος διαρροής υδάτων	0.1	4	X_4
Στατικός ηλεκτρισμός	0.1	4	X_4
Ηλιακές εκλάμψεις	0.1	3	X_5
Απώλεια καλής φήμης	0.1	3	X_5
Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	0.1	3	X_5
Αγωγές – Μηνύσεις	0.1	2	X_6

Πίνακας 6: Σειρά κατάταξης κινδύνων συστήματος E-Prescription

Στη συνέχεια ενημερώνεται το μητρώο κινδύνων

	Ονομασία	Πιθανότητα	Επίπεδο	Έκθεση	Προτεραιότητα	Ημ. Ενημέρωσης
1	Ασυμβατότητα λογισμικού με τις απαιτήσεις	0.1	5	X_3	80	26/10/2013
2	Εξάντληση πόρων του συστήματος	0.5	5	Y_6	18	26/10/2013
3	Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων	0.1	5	X_3	81	26/10/2013
4	Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών	0.9	5	Y_1	1	26/10/2013
5	Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού	0.3	4	M_6	54	26/10/2013
6	Έλλειψη διασυνδεσιμότητας του φορέων μέσω του συστήματος	0.5	3	M_4	36	26/10/2013
7	Λανθασμένος σχεδιασμός υλικού του συστήματος	0.1	5	X_3	82	26/10/2013
8	Λανθασμένος σχεδιασμός λογισμικού του συστήματος	0.1	5	X_3	83	26/10/2013
9	Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	0.3	5	M_4	46	26/10/2013
10	Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	0.5	3	M_4	37	26/10/2013
11	Μη αποδεκτή ποιότητα λογισμικού	0.5	3	M_4	38	26/10/2013
12	Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του πληροφοριακού συστήματος	0.1	5	X_3	84	26/10/2013
13	Αδυναμία σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	0.5	4	M_2	24	26/10/2013
14	Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	0.3	4	M_6	55	26/10/2013
15	Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	0.3	4	M_6	56	26/10/2013
16	Δυσλειτουργία του υλικού	0.5	4	M_2	25	26/10/2013
17	Ανεπαρκής έλεγχος λογισμικού	0.5	4	M_2	26	26/10/2013
18	Σφάλματα λογισμικού	0.5	5	Y_6	19	26/10/2013
19	Πολυπλοκότητα λογισμικού	0.5	3	M_4	39	26/10/2013
20	Μη ασφαλής αρχιτεκτονική δικτύου	0.5	4	M_2	27	26/10/2013
21	Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	0.5	2	M_7	70	26/10/2013
22	Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	0.5	2	M_7	71	26/10/2013
23	Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	0.5	4	M_2	28	26/10/2013
24	Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.	0.5	3	M_4	40	26/10/2013
25	Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)	0.3	5	M_4	47	26/10/2013
26	Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	0.7	2	M_5	52	26/10/2013
27	Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων	0.7	3	M_1	22	26/10/2013
28	Ανεπαρκής επίβλεψη εργαζομένων	0.5	4	M_2	29	26/10/2013
29	Ελλιπής διαδικασία για την αφαίρεση δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης	0.3	4	M_6	57	26/10/2013
30	Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	0.7	3	M_1	23	26/10/2013
31	Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας	0.5	5	Y_6	20	26/10/2013

32	Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	0.7	4	Y_4	7	26/10/2013
33	Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	0.7	4	Y_4	8	26/10/2013
34	Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	0.7	4	Y_4	9	26/10/2013
35	Έλλειψη οικονομικών πόρων	0.5	3	M_4	41	26/10/2013
36	Προβλήματα με την χρηματοδότηση του έργου	0.7	2	M_5	53	26/10/2013
37	Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος	0.7	4	Y_4	10	26/10/2013
38	Κλοπή υλικού από εργαζομένους	0.7	4	Y_4	11	26/10/2013
39	Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	0.5	4	M_2	30	26/10/2013
40	Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	0.7	4	Y_4	12	26/10/2013
41	Καταστροφή εξοπλισμού από υγρά/τρόφιμα	0.5	4	M_2	31	26/10/2013
42	Διαρροή πληροφοριών	0.7	4	Y_4	13	26/10/2013
43	Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	0.7	4	Y_4	14	26/10/2013
44	Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους	0.7	5	Y_3	3	26/10/2013
45	Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	0.7	5	Y_3	4	26/10/2013
46	Μη εξουσιοδοτημένες αλλαγές αρχείων	0.3	5	M_4	48	26/10/2013
47	Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος	0.3	5	M_4	49	26/10/2013
48	Έλλειψη κινήτρων για τους εργαζόμενους	0.5	4	M_2	32	26/10/2013
49	Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	0.7	4	Y_4	15	26/10/2013
50	Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο	0.7	4	Y_4	16	26/10/2013
51	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	0.3	5	M_4	50	26/10/2013
52	Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	0.5	4	M_2	33	26/10/2013
53	Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	0.7	1	X_1	78	26/10/2013
54	Εσωτερικοί κίνδυνοι (δόλος)	0.3	3	M_8	74	26/10/2013
55	Λάθος κατανομή του κεφαλαίου	0.3	3	M_8	75	26/10/2013
56	Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	0.3	4	M_6	58	26/10/2013
57	Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	0.5	4	M_2	34	26/10/2013
58	Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	0.5	3	M_4	42	26/10/2013
59	Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	0.5	2	M_7	72	26/10/2013
60	Λανθασμένη κοστολόγηση του έργου	0.5	3	M_4	43	26/10/2013
61	Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	0.3	3	M_8	76	26/10/2013
62	Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	0.3	4	M_6	59	26/10/2013
63	Λανθασμένες αποφάσεις διαχείρισης κινδύνων	0.1	4	X_4	89	26/10/2013
64	Κίνδυνος σεισμού	0.5	3	M_4	44	26/10/2013

65	Κίνδυνος Κεραυνού	0.3	4	M_6	60	26/10/2013
66	Κίνδυνος πλημμύρας	0.3	4	M_6	61	26/10/2013
67	Κίνδυνος πυρκαγιάς	0.7	4	Y_4	17	26/10/2013
68	Κίνδυνος διαρροής υδάτων	0.1	4	X_4	90	26/10/2013
69	Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	0.3	4	M_6	62	26/10/2013
70	Κατολίσθηση – διάβρωση εδάφους	0.1	5	X_3	85	26/10/2013
71	Ηλιακές εκλάμψεις	0.1	3	X_5	92	26/10/2013
72	Σκόνη	0.5	2	M_7	73	26/10/2013
73	Βλάβη του συστήματος κλιματισμού	0.3	4	M_6	63	26/10/2013
74	Ηλεκτρομαγνητικές παρεμβολές	0.3	3	M_8	77	26/10/2013
75	Στατικός ηλεκτρισμός	0.1	4	X_4	91	26/10/2013
76	Έκρηξη ηφαιστείου	0.1	5	X_3	86	26/10/2013
77	Πυρηνικό ατύχημα	0.1	5	X_3	87	26/10/2013
78	Κίνδυνος εκρήξεων	0.3	5	M_4	51	26/10/2013
79	Έντομα – τρωκτικά	0.5	4	M_2	35	26/10/2013
80	Κίνδυνος δονήσεων	0.3	4	M_6	64	26/10/2013
81	Καπνός - Μικροσωματίδια	0.3	4	M_6	65	26/10/2013
82	Μαγνήτες – μαγνητικά εργαλεία	0.5	5	Y_6	21	26/10/2013
83	Αγωγές – Μηνύσεις	0.1	2	X_6	95	26/10/2013
84	Απώλεια καλής φήμης	0.1	3	X_5	93	26/10/2013
85	Κλοπή πνευματικής ιδιοκτησίας	0.3	2	X_2	79	26/10/2013
86	Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	0.1	3	X_5	94	26/10/2013
87	Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	0.1	5	X_3	88	26/10/2013
88	Κλοπή υλικού	0.3	4	M_6	66	26/10/2013
89	Βανδαλισμοί	0.3	4	M_6	67	26/10/2013
90	Εισβολείς (Hackers) – Υποκλοπή δεδομένων	0.7	5	Y_3	5	26/10/2013
91	Εισβολείς (Hackers) – Καταστροφή δεδομένων	0.7	5	Y_3	6	26/10/2013
92	Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού)	0.9	5	Y_1	2	26/10/2013
93	Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	0.5	3	M_4	45	26/10/2013
94	Κατασκοπεία	0.3	4	M_6	68	26/10/2013
95	Τρομοκρατικές ενέργειες	0.3	4	M_6	69	26/10/2013

Πίνακας 7: Μητρώο κινδύνων–Ανάλυση/Αξιολόγηση κινδύνων συστήματος E-Prescription

6.5 Σχέδια αντιμετώπισης κινδύνων

Στη φάση αυτή η ομάδα που ασχολείται με τη διαδικασία διαχείρισης των κινδύνων, έχει το μητρώο κινδύνων με τους κινδύνους που έχουν προσδιοριστεί, ιεραρχημένους ανάλογα με τη σοβαρότητά τους από την ανάλυση και την αξιολόγηση που έχει γίνει. Στη συνέχεια πρέπει να βρει την κατάλληλη μέθοδο αντιμετώπισης του κάθε κινδύνου. Οι μέθοδοι αντιμετώπισης των απειλών είναι η αποφυγή (avoidance), η μεταφορά (transfer), ο μετριασμός (mitigation) και η αποδοχή (acceptance). Στον παρακάτω πίνακα θα αναφερθούν οι κίνδυνοι και η μέθοδος αντιμετώπισης του καθενός.

Κίνδυνος	Μέθοδοι Αντιμετώπισης
Ασυμβατότητα λογισμικού με τις απαιτήσεις	Μεταφορά
Εξάντληση πόρων του συστήματος	Αποφυγή
Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων	Μεταφορά
Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών	Μεταφορά
Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού	Μεταφορά
Έλλειψη διασυνδεσιμότητας των φορέων μέσω του συστήματος	Μεταφορά
Λανθασμένος σχεδιασμός του υλικού (αρχιτεκτονική συστήματος)	Μεταφορά
Λανθασμένος σχεδιασμός του λογισμικού (αρχιτεκτονική συστήματος)	Μεταφορά
Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	Μεταφορά
Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	Μεταφορά
Μη αποδεκτή ποιότητα λογισμικού	Μεταφορά
Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του πληροφοριακού συστήματος	Μεταφορά
Αδυναμία Σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	Αποφυγή
Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	Μεταφορά
Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	Μεταφορά
Δυσλειτουργία του υλικού	Αποδοχή
Ανεπαρκής έλεγχος του λογισμικού	Μεταφορά
Σφάλματα λογισμικού	Μεταφορά
Πολυπλοκότητα λογισμικού	Μεταφορά
Μη ασφαλής αρχιτεκτονική δικτύου	Μεταφορά
Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	Μετριασμός
Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	Αποφυγή
Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	Μεταφορά
Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.	Μετριασμός
Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)	Μετριασμός
Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	Αποδοχή
Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων	Μεταφορά
Ανεπαρκής επίβλεψη των εργαζομένων	Μεταφορά
Ελλιπής διαδικασία για την αφαίρεση των δικαιωμάτων πρόσβασης κατά τη λήξη της απασχόλησης	Αποφυγή
Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	Μεταφορά
Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας	Μεταφορά
Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	Μετριασμός
Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	Μετριασμός
Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	Μετριασμός
Έλλειψη οικονομικών πόρων	Αποφυγή

Προβλήματα με την χρηματοδότηση του έργου	Αποφυγή
Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος	Μετριασμός
Κλοπή υλικού από εργαζομένους	Αποφυγή
Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	Μετριασμός
Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	Μετριασμός
Καταστροφή εξοπλισμού από υγρά/τρόφιμα	Αποφυγή
Διαρροή πληροφοριών	Μετριασμός
Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	Μετριασμός
Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους	Μεταφορά
Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	Μετριασμός
Μη εξουσιοδοτημένες αλλαγές αρχείων	Μεταφορά
Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος	Αποδοχή
Έλλειψη κινήτρων για τους εργαζόμενους	Μετριασμός
Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	Μετριασμός
Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο	Αποδοχή
Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	Μετριασμός
Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	Μετριασμός
Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	Μετριασμός
Εσωτερικοί κίνδυνοι (δόλος)	Μετριασμός
Λάθος κατανομή του κεφαλαίου	Μεταφορά
Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	Μεταφορά
Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	Μεταφορά
Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	Αποφυγή
Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	Μεταφορά
Λανθασμένη κοστολόγηση του έργου	Μεταφορά
Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	Μεταφορά
Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	Μετριασμός
Λανθασμένες αποφάσεις διαχείρισης κινδύνων	Μετριασμός
Κίνδυνος σεισμού	Μετριασμός
Κίνδυνος Κεραυνού	Αποφυγή
Κίνδυνος πλημμύρας	Μετριασμός
Κίνδυνος πυρκαγιάς	Μετριασμός
Κίνδυνος διαρροής υδάτων	Μετριασμός
Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	Μετριασμός
Κατολίσθηση – διάβρωση εδάφους	Αποδοχή
Ηλιακές εκλάμψεις	Αποδοχή
Σκόνη	Μετριασμός
Βλάβη του συστήματος κλιματισμού	Μετριασμός

Ηλεκτρομαγνητικές παρεμβολές	Αποδοχή
Στατικός ηλεκτρισμός	Μετριασμός
Έκρηξη ηφαιστείου	Αποφυγή
Πυρηνικό ατύχημα	Αποφυγή
Κίνδυνος εκρήξεων	Μετριασμός
Έντομα/τρωκτικά	Μετριασμός
Κίνδυνος δονήσεων	Μετριασμός
Καπνός/μικροσωματίδια	Μετριασμός
Μαγνήτες/μαγνητικά εργαλεία	Μετριασμός
Αγωγές – Μηνύσεις	Μεταφορά
Απώλεια καλής φήμης	Μεταφορά
Κλοπή πνευματικής ιδιοκτησίας	Μεταφορά
Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	Αποδοχή
Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	Αποδοχή
Κλοπή υλικού	Μετριασμός
Βανδαλισμοί	Μετριασμός
Εισβολείς (Hackers) – Υποκλοπή δεδομένων	Μεταφορά
Εισβολείς (Hackers) – Καταστροφή δεδομένων	Μεταφορά
Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού)	Μεταφορά
Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	Αποδοχή
Κατασκοπεία	Μεταφορά
Τρομοκρατικές επιθέσεις	Μετριασμός

Πίνακας 8: Σχέδια αντιμετώπισης κινδύνων συστήματος E-Prescription

Οι κίνδυνοι οι οποίοι είναι αποδεκτοί, πρέπει να παρακολουθούνται ώστε να ελέγχεται η κατάστασή τους κατά τη διάρκεια της υλοποίησης του συστήματος. Οι κίνδυνοι οι οποίοι πρέπει να μεταφερθούν σε κάποιο εμπλεκόμενο μέρος πρέπει να καλύπτονται από τις ρήτρες του συμβολαίου μεταξύ του εργολάβου και του ανάδοχου του έργου.

Στους κινδύνους τους οποίους πρέπει να μειωθεί είτε η πιθανότητα εμφάνισής τους είτε η συνέπεια που μπορεί να επιφέρουν, πρέπει να βρεθούν κάποια εναλλακτικά σχέδια που θα τεθούν σε εφαρμογή είτε πριν την εμφάνισή τους είτε μετά από αυτή. Τέλος, οι κίνδυνοι που πρέπει να αποφευχθούν είναι αυτοί που μπορούν να έχουν το μεγαλύτερο αντίκτυπο στην υλοποίηση και λειτουργία του συστήματος και πρέπει να βρεθούν εναλλακτικοί τρόποι ώστε να εκλείψουν.

Στη συνέχεια ενημερώνεται το μητρώο κινδύνων με τη μέθοδο (στρατηγική) αντιμετώπισης, το δείκτη παρακολούθησης και τον προπομπό του κάθε κινδύνου (Πίνακας 9).

Πιο αναλυτικά, στα παρακάτω πεδία συμπληρώνονται τα εξής στοιχεία:

- στο πεδίο «δείκτης παρακολούθησης» καταγράφονται οι παράμετροι ή τα γεγονότα τα οποία χαρακτηρίζουν τον κίνδυνο και τα οποία θα παρακολουθεί η ομάδα διαχείρισης.
- στο πεδίο «προπομπός κινδύνου» (risk trigger), καταγράφεται το γεγονός που μπορεί να υποδηλώσει την έναρξη υλοποίησης του κάθε κινδύνου, ώστε η ομάδα διαχείρισης να ενεργήσει έγκαιρα και σωστά για την αντιμετώπισή του.
- στο πεδίο «στρατηγική αντιμετώπισης» καταγράφεται η μέθοδος με την οποία θα αντιμετωπιστεί ο κάθε κίνδυνος.
- στο πεδίο «ημερομηνία ενημέρωσης» καταγράφεται η ημερομηνία όπου έγινε το σχέδιο αντιμετώπισης του κάθε κινδύνου.

#	Κίνδυνοι	Δείκτης παρακολούθησης	Προπομπός Κινδύνου	Στρατηγική Αντιμετώπισης	Ημερομηνία ενημέρωσης
1	Ασυμβατότητα λογισμικού με τις απαιτήσεις	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του συστήματος	Κάποια έκδοση δεν λειτουργεί σωστά	Μεταφορά	27/10/2013
2	Εξάντληση πόρων του συστήματος	Στατιστικά χρήσης του συστήματος	Η χρήση του συστήματος έχει ανέλθει στο ανώτατο κατώφλι ασφαλείας που έχει τεθεί από τον εργολάβο (π.χ. το 80% των πόρων του συστήματος)	Αποφυγή	27/10/2013
3	Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του συστήματος	Σε κάποια έκδοση η βάση δεδομένων δε λειτουργεί σωστά	Μεταφορά	27/10/2013
4	Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών	Έλεγχος στις εκδόσεις των λογισμικών ασφαλείας	Υπάρχει ενδεχόμενο υποκλοπής κάποιων στοιχείων	Μεταφορά	27/10/2013
5	Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού	Παρακολούθηση του σχεδιασμού και των τεχνικών προδιαγραφών υλοποίησης του συστήματος	Εμφάνιση αυξημένης πολυπλοκότητας στην αρχιτεκτονική σχεδιασμού και δυσκολία εισαγωγής νέων χαρακτηριστικών	Μεταφορά	27/10/2013
6	Έλλειψη διασυνδεσιμότητας των φορέων μέσω του συστήματος	Πρωτόκολλα επικοινωνίας	Αδυναμία διασύνδεσης με τα συστήματα των άλλων φορέων	Μεταφορά	27/10/2013
7	Λανθασμένος σχεδιασμός υλικού (αρχιτεκτονική συστήματος)	Παρακολούθηση των απαιτήσεων σχεδιασμού	Λανθασμένη υλοποίηση των απαιτήσεων σχεδιασμού	Μεταφορά	27/10/2013
8	Λανθασμένος σχεδιασμός λογισμικού (αρχιτεκτονική συστήματος)	Παρακολούθηση των απαιτήσεων σχεδιασμού	Λανθασμένη υλοποίηση των απαιτήσεων σχεδιασμού	Μεταφορά	27/10/2013

9	Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	Παρακολούθηση τεχνολογίας ανάπτυξης λογισμικού	Αδυναμία αξιοποίησης στο μέγιστο των υποδομών ροής πληροφοριών	Μεταφορά	27/10/2013
10	Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	Παρακολούθηση τεχνολογίας ανάπτυξης λογισμικού	Αδυναμία κάλυψης των λειτουργικών απαιτήσεων του συστήματος	Μεταφορά	27/10/2013
11	Μη αποδεκτή ποιότητα λογισμικού	Παρακολούθηση των ποιοτικών χαρακτηριστικών του συστήματος	Απόκλιση από τα αποδεκτά όρια ποιότητας	Μεταφορά	27/10/2013
12	Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του λογισμικού του πληροφοριακού συστήματος	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του λογισμικού ασφαλείας	Κάποια έκδοση του λογισμικού ασφαλείας δεν λειτουργεί σωστά με αποτέλεσμα την μετάδοση κακόβουλου λογισμικού	Μεταφορά	27/10/2013
13	Αδυναμία Σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	Παρακολούθηση χαρακτηριστικών του τηλεπικοινωνιακού δικτύου	Συνεχής υπερφόρτωση του δικτύου	Αποφυγή	27/10/2013
14	Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	Παρακολούθηση των απαιτήσεων ασφάλειας στο σχεδιασμό του λογισμικού	Λανθασμένη υλοποίηση των απαιτήσεων ασφάλειας	Μεταφορά	27/10/2013
15	Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	Παρακολούθηση του τρόπου επεξεργασίας των δεδομένων	Λανθασμένη επεξεργασία των δεδομένων	Μεταφορά	27/10/2013
16	Δυσλειτουργία του υλικού	Παρακολούθηση του τρόπου λειτουργίας του υλικού	Συνεχής υπερθέρμανση του συστήματος/ έντονος ήχος κατά τη λειτουργία του	Αποδοχή	27/10/2013
17	Ανεπαρκής έλεγχός του λογισμικού	Παρακολούθηση των απαιτήσεων ελέγχου του λογισμικού	Λανθασμένη υλοποίηση των απαιτήσεων ελέγχου	Μεταφορά	27/10/2013
18	Σφάλματα λογισμικού	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του λογισμικού	Κάποια έκδοση του λογισμικού δεν παράγει τα αναμενόμενα αποτελέσματα	Μεταφορά	27/10/2013

19	Πολυπλοκότητα λογισμικού	Έλεγχος στον σχεδιασμό του λογισμικού	Δυσκολία στην αναβάθμιση του λογισμικού	Μεταφορά	27/10/2013
20	Μη ασφαλής αρχιτεκτονική δικτύου	Παρακολούθηση των απαιτήσεων ασφάλειας για το σχεδιασμό του δικτύου	Λανθασμένη υλοποίηση των απαιτήσεων ασφάλειας	Μεταφορά	27/10/2013
21	Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	Έλεγχος της επικοινωνίας με την εταιρεία ανάθεσης έργου	Έλλειψη επικοινωνίας με την εταιρεία ανάθεσης έργου	Μετριασμός	27/10/2013
22	Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	Παρακολούθηση της διαδικασίας καθορισμού των όρων του συμβολαίου	Ύπαρξη ασαφειών μεταξύ των όρων του συμβολαίου	Αποφυγή	27/10/2013
23	Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	Παρακολούθηση ανταπόκρισης της ομάδα υποστήριξης του συστήματος σε περίπτωση ανάγκης	Προβληματική υποστήριξη του συστήματος	Μεταφορά	27/10/2013
24	Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.	Παρακολούθηση της επικοινωνίας μεταξύ των ομάδων	Προβληματική συνεργασία μεταξύ των ομάδων	Μετριασμός	27/10/2013
25	Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)	Παρακολούθηση της ασφάλειας του κτιρίου	Εμφάνιση φαινομένων εισβολής	Μετριασμός	27/10/2013
26	Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	Έλεγχος του χρόνου προσαρμογής των χρηστών	Απόκλιση από τον προβλεπόμενο χρόνο προσαρμογής	Αποδοχή	27/10/2013
27	Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων	Έλεγχος και αξιολόγηση των εργαζομένων του συστήματος σύμφωνα με τα προσόντα και τις γνώσεις τους	Λανθασμένη υλοποίηση του συστήματος και μη σωστή λειτουργία των ομάδων που συνεργάζονται για την υλοποίηση του συστήματος	Μεταφορά	27/10/2013
28	Ανεπαρκής επίβλεψη των εργαζομένων	Μη ύπαρξη προσωπικού για την επίβλεψη εργαζομένων	Καθυστέρηση στην υλοποίηση του έργου /Υπαρξη λαθών κατά την υλοποίηση του	Μεταφορά	27/10/2013

29	Ελλιπής διαδικασία για την αφαίρεση των δικαιωμάτων πρόσβασης κατά τη λήξη της απασχόλησης	Έλεγχος των ατόμων που συνδέονται καθημερινά στο σύστημα	Ανίχνευση πρόσβασης στο σύστημα από πρώην εργαζόμενο στην εταιρεία	Αποφυγή	27/10/2013
30	Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	Έλεγχος της λειτουργίας του λογισμικού	Μη αναμενόμενη συμπεριφορά του λογισμικού	Μεταφορά	27/10/2013
31	Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου	Μεταφορά	27/10/2013
32	Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό	Μη αναμενόμενη συμπεριφορά του υλικού, μη τακτική συντήρηση του υλικού	Μετριασμός	27/10/2013
33	Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό	Μη αναμενόμενη συμπεριφορά του υλικού, ύπαρξη εύφλεκτων υλικών στο χώρο, μη τακτική συντήρηση του υλικού	Μετριασμός	27/10/2013
34	Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό	Μη αναμενόμενη συμπεριφορά του υλικού, μη τακτική συντήρηση του υλικού	Μετριασμός	27/10/2013
35	Έλλειψη οικονομικών πόρων	Οικονομικοί δείκτες ρευστότητας και χρηματοδότησης του έργου	Περικοπή κάποιου προϋπολογισμού	Αποφυγή	27/10/2013
36	Προβλήματα με την χρηματοδότηση του έργου	Ανακοινώσεις της κυβέρνησης σχετικά με τη χρηματοδότηση του έργου	Ύπαρξη γενικότερων οικονομικών προβλημάτων και έλλειψη ρευστότητας του κράτους	Αποφυγή	27/10/2013

37	Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό.	Μη αναμενόμενη συμπεριφορά του υλικού, μη τακτική συντήρηση του υλικού	Μετριασμός	27/10/2013
38	Κλοπή υλικού από εργαζομένους	Έλεγχος του εξοπλισμού σε τακτά χρονικά διαστήματα	Μη ταύτιση καταγεγραμμένου και υπάρχοντος εξοπλισμού	Αποφυγή	27/10/2013
39	Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	Παρακολούθηση της συμπεριφοράς των εργαζομένων ως προς τα εργασιακά ζητήματα	Εμφάνιση αντιδράσεων σε εργασιακές αλλαγές	Μετριασμός	27/10/2013
40	Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	Παρακολούθηση των στατιστικών χρήσης του συστήματος	Τα στατιστικά χρήσης του συστήματος είναι στο κατώτατο όριο από αυτό που έχει οριστεί από την εταιρεία ανάθεσης του έργου	Μετριασμός	27/10/2013
41	Καταστροφή εξοπλισμού από υγρά/τρόφιμα	Έλεγχος αν υπάρχει σήμανση για την απαγόρευση των τροφίμων και των ποτών στου χώρους που βρίσκεται το πληροφοριακό σύστημα	Εργαζόμενοι που εισέρχονται με τρόφιμα και ποτά στους χώρους του πληροφοριακού συστήματος	Αποφυγή	27/10/2013
42	Διαρροή πληροφοριών	Έλεγχος για την ύπαρξη ειδικού λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος	Μη ύπαρξη του λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος	Μετριασμός	27/10/2013
43	Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	Έλεγχος για την ύπαρξη συσκευών αναγνώρισης των ειδικών καρτών των εργαζομένων	Μη ύπαρξη των συσκευών αναγνώρισης στις εισόδους του κτιρίου που στεγάζεται το σύστημα	Μετριασμός	27/10/2013

44	Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου	Μεταφορά	27/10/2013
45	Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	Έλεγχος για την ύπαρξη ειδικού λογισμικού που να καταγράφει την ηλεκτρονική διεύθυνση που αντιστοιχεί σε κάθε εργαζόμενο	Μη ύπαρξη του ειδικού λογισμικού	Μετριασμός	27/10/2013
46	Μη εξουσιοδοτημένες αλλαγές αρχείων	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου	Μεταφορά	27/10/2013
47	Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος	Περιοδική ταυτοποίηση ενός δείγματος δεδομένων και έλεγχος των αποτελεσμάτων	Εμφάνιση σφαλμάτων κατά την ταυτοποίηση	Αποδοχή	27/10/2013
48	Έλλειψη κινήτρων για τους εργαζόμενους	Παρακολούθηση δεικτών παραγωγικότητας	Μείωση παραγωγικότητας των εργαζομένων	Μετριασμός	27/10/2013
49	Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	Παρακολούθηση της τήρησης των κανόνων ασφαλείας	Εμφάνισης συχνής παραβατικότητας	Μετριασμός	27/10/2013
50	Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο	Τακτικός έλεγχος του δικτύου μέσω λογισμικού ασφαλείας (Antivirus)	Εμφάνιση και διόρθωση ιού κατά τη διαδικασία του τακτικού ελέγχου	Αποδοχή	27/10/2013
51	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	Τακτικός έλεγχος για την αυθεντικότητα του λογισμικού και των εφαρμογών	Εμφάνιση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	Μετριασμός	27/10/2013
52	Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	Έλεγχος για την ύπαρξη ειδικού λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος	Μη ύπαρξη του λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος	Μετριασμός	27/10/2013
53	Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	Παρακολούθηση του αρχείου εκπαίδευσης των υπαλλήλων	Ύπαρξη προβλημάτων κατά τη χρήση του συστήματος	Μετριασμός	27/10/2013

54	Εσωτερικοί κίνδυνοι (δόλος)	Παρακολούθηση συμπεριφοράς εργαζομένων	Ύποπτες κινήσεις εργαζομένων	Μετριασμός	27/10/2013
55	Λάθος κατανομή του κεφαλαίου	Παρακολούθηση της προσυμφωνημένης κατανομής του κεφαλαίου	Ανομοιόμορφη κατανομή του κεφαλαίου	Μεταφορά	27/10/2013
56	Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	Έλεγχος στις εκδόσεις του συστήματος	Το σύστημα δεν καλύπτει κάποια σημαντικά σημεία που έπρεπε να έχουν ληφθεί πολύ σοβαρά υπ' όψιν	Μεταφορά	27/10/2013
57	Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	Παρακολούθηση του σχεδιασμού του έργου	Ανεπαρκής ή ελλιπής ύπαρξη εφεδρικού σχεδίου κατά το στάδιο ολοκλήρωσης του έργου	Αποφυγή	27/10/2013
58	Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	Έλεγχος του προγραμματισμού των απαιτούμενων πόρων υλικού	Απόκλιση από τον αρχικό προγραμματισμό των απαιτούμενων πόρων	Αποφυγή	27/10/2013
59	Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	Παρακολούθηση και σύγκριση του πραγματικού χρονοδιαγράμματος με το εκτιμώμενο	Παρατήρηση καθυστερήσεων κατά τα επιμέρους στάδια ολοκλήρωσης του έργου	Μεταφορά	27/10/2013
60	Λανθασμένη κοστολόγηση του έργου	Παρακολούθηση οικονομικών δεικτών	Τα πρώτα στάδια της υλοποίησης του έργου βγαίνουν εκτός του αρχικού προϋπολογισμού	Μεταφορά	27/10/2013
61	Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου	Μεταφορά	27/10/2013

62	Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	Ελλιπής έλεγχος των απαραίτητων διαδικασιών για την διεξαγωγή του έργου	Εμφάνιση πολλών λαθών κατά τη διάρκεια του προγραμματισμού και της διαχείρισης του έργου	Μετριασμός	27/10/2013
63	Λανθασμένες αποφάσεις διαχείρισης κινδύνων	Τακτική παρακολούθηση του σχεδιασμού διαχείρισης κινδύνου	Απόκλιση αποφάσεων από τον αρχικό σχεδιασμό διαχείρισης κινδύνου	Μετριασμός	27/10/2013
64	Κίνδυνος σεισμού	Έλεγχος στατικότητας του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα	Ενδείξεις προβληματικής στατικότητας του κτιρίου	Μετριασμός	27/10/2013
65	Κίνδυνος Κεραυνού	Έλεγχος των καιρικών φαινομένων	Έντονες βροχοπτώσεις	Αποφυγή	27/10/2013
66	Κίνδυνος πλημμύρας	Έλεγχος των καιρικών φαινομένων	Παρατήρηση πλημμυρικών φαινομένων σε ορισμένα τμήματα του κτιρίου	Μετριασμός	27/10/2013
67	Κίνδυνος πυρκαγιάς	Έλεγχος του χώρου εγκατάστασης ως προς τα μέτρα πυρασφάλειας	Ελλιπής ή ανύπαρκτη συντήρηση του εξοπλισμού πυρασφάλειας	Μετριασμός	27/10/2013
68	Κίνδυνος διαρροής υδάτων	Έλεγχος του δικτύου υδροδότησης του κτιρίου	Ελλιπής ή ανύπαρκτη συντήρηση του δικτύου υδροδότησης	Μετριασμός	27/10/2013
69	Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	Έλεγχος του δικτύου ηλεκτροδότησης του κτιρίου	Ελλιπής ή ανύπαρκτη συντήρηση του δικτύου ηλεκτροδότησης	Μετριασμός	27/10/2013
70	Κατολίσθηση/ διάβρωση εδάφους	Περιοδικοί έλεγχοι του εδάφους περιμετρικά του κτιρίου όπου βρίσκεται το πληροφοριακό σύστημα	Εμφάνιση φαινομένων διάβρωσης	Αποδοχή	27/10/2013

71	Ηλιακές εκλάμψεις	Περιοδικός έλεγχος της σωστής λειτουργίας του δικτύου από ηλεκτρομαγνητικές παρεμβολές	Μη σωστή λειτουργία του δικτύου λόγω ηλεκτρομαγνητικών παρεμβολών	Αποδοχή	27/10/2013
72	Σκόνη	Τακτικός έλεγχος της κατάστασης του εξοπλισμού	Παρατήρηση δυσλειτουργιών λόγω σκόνης	Μετριασμός	27/10/2013
73	Βλάβη του συστήματος κλιματισμού	Τακτική παρακολούθηση του συστήματος κλιματισμού	Παρατήρηση δυσλειτουργιών του συστήματος λόγω υπερθέρμανσης	Μετριασμός	27/10/2013
74	Ηλεκτρομαγνητικές παρεμβολές	Περιοδικός έλεγχος της σωστής λειτουργίας του δικτύου από ηλεκτρομαγνητικές παρεμβολές	Μη σωστή λειτουργία του δικτύου λόγω ηλεκτρομαγνητικών παρεμβολών	Αποδοχή	27/10/2013
75	Στατικός ηλεκτρισμός	Περιοδικός έλεγχος του κτιρίου που στεγάζεται το πληροφοριακό σύστημα για διαρροή ρεύματος	Εμφάνιση σημείων του κτιρίου όπου μπορεί να προκληθεί διαρροή ρεύματος - βραχυκύκλωμα	Μετριασμός	27/10/2013
76	Έκρηξη ηφαιστείου	Παρακολούθηση των μετρήσεων που γίνονται από το ηφαιστειολογικό παρατηρητήριο της περιοχής όπου στεγάζεται το πληροφοριακό σύστημα	Όταν οι μετρήσεις αποκλίνουν από τα επιτρεπτά όρια που έχουν ορισθεί	Αποφυγή	27/10/2013
77	Πυρηνικό ατύχημα	Παρακολούθηση των μετρήσεων που γίνονται από τα πυρηνικά εργοστάσια της περιοχής όπου στεγάζεται το πληροφοριακό σύστημα	Όταν οι μετρήσεις αποκλίνουν από τα επιτρεπτά όρια που έχουν ορισθεί	Αποφυγή	27/10/2013
78	Κίνδυνος εκρήξεων	Έλεγχος για την ύπαρξη εύφλεκτων υλικών στο χώρο όπου στεγάζεται το πληροφοριακό σύστημα	Εμφάνιση αποθηκευμένων υλικών που μπορεί να προκαλέσουν εκρήξεις	Μετριασμός	27/10/2013

79	Έντομα/τρωκτικά	Τακτικός έλεγχος του κτιρίου για εμφάνιση τρωκτικών	Εμφάνιση καταστροφών στο υλικό του συστήματος από τρωκτικά	Μετριασμός	27/10/2013
80	Κίνδυνος δονήσεων	Έλεγχος του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα για την ύπαρξη ιδιοτήτων αντικραδασμικής λειτουργίας	Μη ύπαρξη ιδιοτήτων αντικραδασμικής λειτουργίας	Μετριασμός	27/10/2013
81	Καπνός/ μικροσωματίδια	Έλεγχος της καθαρότητας του αέρα	Εμφάνιση καπνού στο χώρο του πληροφοριακού συστήματος	Μετριασμός	27/10/2013
82	Μαγνήτες/μαγνητικά εργαλεία	Τακτικός έλεγχος της βάσης δεδομένων και καταμέτρηση των αποθηκευμένων δεδομένων στη βάση	Απώλεια δεδομένων/μη σωστή αποθήκευση των δεδομένων	Μετριασμός	27/10/2013
83	Αγωγές – Μηνύσεις	Παρακολούθηση ορθής λειτουργίας του συστήματος και αποδοχής του από τα εμπλεκόμενα μέρη	Ύπαρξη σοβαρών αντιδράσεων	Μεταφορά	27/10/2013
84	Απώλεια καλής φήμης	Έλεγχος της αποδοχής και της χρήσης του συστήματος από τα εμπλεκόμενα μέλη	Μη χρήση της εφαρμογής από τους χρήστες λόγω ύπαρξης λαθών / μη εύχρηστη εφαρμογή για τους τελικούς χρήστες του συστήματος	Μεταφορά	27/10/2013
85	Κλοπή πνευματικής ιδιοκτησίας	Παρακολούθηση των εφαρμογών που χρησιμοποιούν ανταγωνίστριες εταιρείες	Χρήση εφαρμογής από ανταγωνίστρια εταιρεία με ίδια χαρακτηριστικά	Μεταφορά	27/10/2013
86	Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	Παρακολούθηση των πολιτικών αποφάσεων και δραστηριοτήτων της κυβέρνησης	Αποφάσεις μείωσης λειτουργικότητας και περιορισμού χρήσης του πληροφοριακού στο σύστημα υγείας	Αποδοχή	27/10/2013

87	Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	Παρακολούθηση των πολιτικών αποφάσεων και δραστηριοτήτων της κυβέρνησης	Πολεμικές αναταραχές	Αποδοχή	27/10/2013
88	Κλοπή υλικού	Έλεγχος του εξοπλισμού και επιθεώρηση του χώρου όπου βρίσκεται ο εξοπλισμός σε τακτά χρονικά διαστήματα	Μη ταύτιση καταγεγραμμένου και υπάρχοντος εξοπλισμού	Μετριασμός	27/10/2013
89	Βανδαλισμοί	Έλεγχος των κτιριακών εγκαταστάσεων όπου στεγάζεται το πληροφοριακό σύστημα καθώς και του εξοπλισμού του πληροφοριακού συστήματος	Καταστροφή του κτιρίου και του εξοπλισμού	Μετριασμός	27/10/2013
90	Εισβολείς (Hackers)- Υποκλοπή δεδομένων	Έλεγχος του λογισμικού ασφαλείας	Υποκλοπή μεταδιδόμενων πληροφοριών	Μεταφορά	27/10/2013
91	Εισβολείς (Hackers)- Καταστροφή δεδομένων	Έλεγχος του λογισμικού ασφαλείας	Καταστροφή/ διαγραφή δεδομένων	Μεταφορά	27/10/2013
92	Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού)	Έλεγχος του λογισμικού ασφαλείας	Μετάδοση κακόβουλου λογισμικού	Μεταφορά	27/10/2013
93	Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	Παρακολούθηση των εφαρμογών που χρησιμοποιούν ανταγωνίστριες εταιρείες	Χρήση εφαρμογής από ανταγωνίστρια εταιρεία με ίδια χαρακτηριστικά	Αποδοχή	27/10/2013
94	Κατασκοπεία	Έλεγχος του λογισμικού ασφαλείας	Υποκλοπή ευαίσθητων προσωπικών δεδομένων	Μεταφορά	27/10/2013
95	Τρομοκρατικές ενέργειες	Έλεγχος του χώρου εγκατάστασης του πληροφοριακού συστήματος και της συμπεριφοράς των εργαζομένων	Ύποπτες ενέργειες των εργαζομένων/ εύρεση ύποπτου εξοπλισμού στο χώρο	Μετριασμός	27/10/2013

Πίνακας 9: Μητρώο κινδύνων–Σχέδια αντιμετώπισης κινδύνων συστήματος E-Prescription

Έπειτα, αν η μέθοδος αντιμετώπισης είναι ο μετριασμός αναγράφονται σε αυτό τα προληπτικά ή και διορθωτικά σχέδια αντιμετώπισης του κάθε κινδύνου, το εναλλακτικό σχέδιο ή και το σχέδιο μετάπτωσης (Πίνακας 10) και στις άλλες στρατηγικές τα σχέδια αποφυγής, μεταφοράς, ή αποδοχής (Πίνακας 11).

Πιο αναλυτικά, στα παρακάτω πεδία συμπληρώνονται τα εξής στοιχεία:

- στο πεδίο «προληπτικά μέτρα» καταγράφονται οι ενέργειες που πρέπει να γίνουν και αφορούν την αλλαγή της πιθανότητας εμφάνισης του κάθε κινδύνου και τα οποία θα παρθούν πριν εμφανιστεί ο κίνδυνος
- στο πεδίο «διορθωτικά μέτρα» καταγράφονται οι ενέργειες που πρέπει να γίνουν και αφορούν τη συνέπεια που μπορεί να έχει η εμφάνιση του κάθε κινδύνου και τα οποία θα παρθούν πριν εμφανιστεί ο κίνδυνος
- στο πεδίο «εναλλακτικό σχέδιο» καταγράφονται οι ενέργειες που πρέπει να γίνουν και αφορούν τη συνέπεια που μπορεί να έχει η εμφάνιση του κάθε κινδύνου και τα οποία θα παρθούν αφού εμφανιστεί ο κίνδυνος
- στο πεδίο «σχέδιο μετάπτωσης» καταγράφονται οι ενέργειες που πρέπει να γίνουν σε περίπτωση που αποτύχει το εναλλακτικό σχέδιο

#	Κίνδυνοι	Προληπτικά μέτρα	Διορθωτικά μέτρα	Εναλλακτικό σχέδιο	Σχέδιο μετάπτωσης
21	Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	Συναντήσεις με την εταιρεία ανάθεσης έργου για επίτευξη καλύτερης επικοινωνίας	Ύπαρξη έγγραφων αναφορών για την αποφυγή παρερμηνεύσεων	Εφαρμογή των κυρώσεων που αναγράφονται στο συμβόλαιο	Ακύρωση του συμβολαίου με την εταιρεία ανάθεσης έργου και ανάθεση του έργου στον επόμενο μειοδότη
24	Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.	Συνεχής επικοινωνία μεταξύ των ομάδων κατασκευής του έργου		Συγκέντρωση των ομάδων κατασκευής στον ίδιο χώρο	
25	Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)	Πρόσληψη προσωπικού για τη φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα	Πρόσληψη ειδικά εκπαιδευμένου προσωπικού	Χρήση ειδικού εξοπλισμού παρακολούθησης του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα (κάμερες ασφαλείας)	
32	Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	Εγκατάσταση συστήματος συναγερμού			
33	Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	Εγκατάσταση συστήματος πυρανίχνευσης			
34	Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	Εγκατάσταση μηχανημάτων ελέγχου ταυτότητας στις εσωτερικές εισόδους που οδηγούν σε κάθε όροφο			
37	Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος	Εκπαίδευση των εργαζομένων σχετικά με τον τρόπο χρήσης του εξοπλισμού		Επίπληξη εργαζομένου που δεν συμβαδίζει με τους κανονισμούς ασφαλής χρήσης του εξοπλισμού	Επιβολή ποινών σε όποιον δεν ακολουθεί τους κανονισμούς ασφαλής χρήσης του εξοπλισμού
39	Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	Επικοινωνία με τους εργαζόμενους για την κατανόηση των αναγκών τους και συζήτηση μαζί τους για την εύρεση της βέλτιστης λύσης	Ύπαρξη εγγράφων που να γίνεται η καταγραφή των αναγκών των εργαζομένων με στόχο την κάλυψη τους	Αλλαγή αρμοδιοτήτων	

40	Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	Μελέτη των αναγκών των χρηστών για την κατανόηση των αναγκών τους όσον αφορά τη χρήση της εφαρμογής	Καταγραφή των αναγκών των χρηστών και υλοποίηση τυχόν αλλαγές στην εφαρμογής για να είναι πιο φιλικοί προς τους χρήστες		
42	Διαρροή πληροφοριών	Εγκατάσταση ειδικού λογισμικού το οποίο ελέγχει τις ενέργειες των εργαζομένων	Ενημέρωση των εργαζομένων σχετικά με τους κανονισμούς της εταιρείας όσον αφορά την ασφάλεια των πληροφοριών και των δεδομένων	Επιπληξη εργαζομένου που δεν συμβαδίζει με του κανονισμούς της εταιρείας	Επιβολή ποινών σε όποιον δεν ακολουθεί τους κανονισμούς της εταιρείας
43	Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	Συνεχής έλεγχος των εγκαταστάσεων όπου βρίσκεται ο εξοπλισμός	Χρήση ειδικού εξοπλισμού όπου απαγορεύει την πρόσβαση μη εξουσιοδοτημένου προσωπικού στους χώρους εγκατάστασης του εξοπλισμού		
45	Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	Ενημέρωση των εργαζομένων για τη διαφύλαξη των κωδικών που έχουν για τη χρήση του πληροφοριακού συστήματος	Δυνατότητα αλλαγής των κωδικών περιοδικά		
48	Έλλειψη κινήτρων για τους εργαζόμενους	Επικοινωνία με τους εργαζόμενους για την κατανόηση των αναγκών τους και συζήτηση μαζί τους για την εύρεση της βέλτιστης λύσης	Δημιουργία περισσότερων κινήτρων για τους εργαζόμενους με βάση τις ανάγκες που έχουν		
49	Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	Εκπαίδευση των εργαζομένων σε θέματα ασφάλειας του εξοπλισμού και του λογισμικού	Καταγραφή και ενημέρωση των εργαζομένων με τους κανόνες που πρέπει να ακολουθούν για την ασφάλεια του πληροφοριακού συστήματος	Επίπληξη εργαζομένου που δεν συμβαδίζει με του κανονισμούς της ασφάλειας του πληροφοριακού συστήματος	Επιβολή ποινών σε όποιον δεν ακολουθεί τους κανονισμούς της ασφάλειας του πληροφοριακού συστήματος

51	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών	Ύπαρξη ειδικού λογισμικού ασφαλείας όπου ανιχνεύει την εγκατάσταση μη εξουσιοδοτημένου λογισμικού στο σύστημα	Τακτικός έλεγχος του λογισμικού και των εφαρμογών που χρησιμοποιούνται		
52	Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	Μη δυνατή αποθήκευση των προσωπικών δεδομένων σε αποθηκευτικά μέσα καθώς μη ύπαρξη δυνατότητας μεταφορά δεδομένων μέσω διαδικτύου			
53	Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	Εκπαίδευση του προσωπικού για την ανταπόκρισή του στις απαιτήσεις του συστήματος		Αλλαγή αρμοδιοτήτων	
54	Εσωτερικοί κίνδυνοι (δόλος)	Χρήση κωδικών ασφαλείας έτσι ώστε ο κάθε χρήστης να έχει δικαιώματα στο σύστημα ανάλογα με την ιδιότητά του	Χρήση εξειδικευμένου λογισμικού έτσι ώστε να ελέγχονται όλες οι ενέργειες των χρηστών		
62	Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	Έλεγχος των εργαζομένων που προσλαμβάνονται για να αναλάβουν την παρακολούθηση του έργου σύμφωνα με την εμπειρία τους και τις γνώσεις που έχουν για τη συγκεκριμένη θέση με τη βοήθεια συνεντεύξεων και γραπτού διαγωνισμού όπου οι υποψήφιοι θα εξετάζονται σε θέματα που αφορούν τη διαχείριση ενός έργου	Ύπαρξη συνεχών ενημερώσεων από τα πρόσωπα που έχουν αναλάβει την παρακολούθηση του έργου καθώς και καταγραφή των δραστηριοτήτων τους και των ελέγχων που έχουν πραγματοποιήσει καθ' όλη τη διάρκεια έργου	Συνεχής κατάρτιση των εργαζομένων σε θέματα διαχείρισης έργου και νέων τεχνολογιών με διεξαγωγή σεμιναρίων.	Αλλαγή αρμοδιοτήτων

63	Λανθασμένες αποφάσεις διαχείρισης κινδύνων	Τακτικός έλεγχος των εργαζομένων που έχουν αναλάβει τις αποφάσεις διαχείρισης κινδύνων		Συνεχής κατάρτιση των εργαζομένων σε θέματα διαχείρισης κινδύνων με διεξαγωγή σεμιναρίων.	Αλλαγή αρμοδιοτήτων
64	Κίνδυνος σεισμού	Συνεχής έλεγχος των κτιριακών εγκαταστάσεων	Μετεγκατάσταση του εξοπλισμού σε πιο σύγχρονες κτιριακές εγκαταστάσεις	Εγκατάσταση του εξοπλισμού σε χώρο αντισεισμικών προδιαγραφών	
66	Κίνδυνος πλημμύρας	Δημιουργία αντιπλημμυρικών έργων στο χώρο εγκατάστασης του εξοπλισμού	Τοποθέτηση του συστήματος σε σημείο υψηλότερο της επιφάνειας του εδάφους		
67	Κίνδυνος πυρκαγιάς	Ύπαρξη και συνεχής έλεγχος λειτουργικών πυροσβεστήρων σε όλους τους ορόφους του κτιρίου	Χρήση εξοπλισμού πυρανίχνευσης		
68	Κίνδυνος διαρροής υδάτων	Συνεχής έλεγχος και συντήρηση του δικτύου υδροδότησης	Μετεγκατάσταση του εξοπλισμού σε πιο σύγχρονες κτιριακές εγκαταστάσεις		
69	Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	Συνεχής έλεγχος και συντήρηση του συστήματος ηλεκτροδότησης	Χρήση γεννητριών	Μετεγκατάσταση του εξοπλισμού σε πιο σύγχρονες κτιριακές εγκαταστάσεις	
72	Σκόνη	Τακτικός καθαρισμός του χώρου όπου βρίσκεται ο εξοπλισμό του συστήματος	Τοποθέτηση του εξοπλισμού σε ειδικό χώρο		
73	Βλάβη του συστήματος κλιματισμού	Τακτικός έλεγχος και συντήρηση του συστήματος κλιματισμού	Ύπαρξη εφεδρικού συστήματος κλιματισμού στους χώρους όπου βρίσκεται ο εξοπλισμός του συστήματος	Αλλαγή του συστήματος κλιματισμού	

75	Στατικός ηλεκτρισμός	Τακτικός έλεγχος του δικτύου ηλεκτροδότησης όπου στεγάζεται το πληροφοριακό σύστημα	Ύπαρξη πινάκων ασφαλείας όπου θα διακόπτουν την παροχή ρεύματος σε περίπτωση διαρροής ρεύματος και θα γίνεται η ρευματοδότηση του συστήματος από γεννήτριες		
78	Κίνδυνος εκρήξεων	Έλεγχος των κτιριακών εγκαταστάσεων και του περιβάλλοντα χώρου για τυχόν εύφλεκτα υλικά όπου μπορεί να προκαλέσουν εκρήξεις και απομάκρυνση αυτών από το χώρο	Αποθήκευση των δεδομένων του συστήματος και σε άλλους servers σε άλλες περιοχές.	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις	
79	Έντομα/τρωκτικά	Τακτικός έλεγχος των κτιριακών εγκαταστάσεων και συχνή απολύμανση του χώρου όπου στεγάζεται το πληροφοριακό για τυχόν έντομα και τρωκτικά	Εγκατάσταση ειδικού εξοπλισμού όπου αποτρέπει τα έντομα και τρωκτικά να εισχωρήσουν στο χώρο	Ύπαρξη εφεδρικού εξοπλισμού σε περίπτωση φθοράς του υπάρχοντος	
80	Κίνδυνος δονήσεων	Εγκατάσταση του πληροφοριακού συστήματος σε κτίριο όπου έχει αντικραδασμική λειτουργία		Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις όπου βρίσκονται σε περιοχή με μειωμένη κραδασμική δραστηριότητα	
81	Καπνός/μικροσωματίδια	Τακτικός έλεγχος και συντήρηση του συστήματος εξαερισμού καθώς και τοποθέτηση του εξοπλισμού σε ειδικό χώρο		Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις όπου βρίσκονται σε περιοχή με λιγότερο καπνό και ρύπους	

82	Μαγνήτες/μαγνητικά εργαλεία	Τοποθέτηση πινακίδας απαγόρευσης όπου δεν θα επιτρέπει την είσοδο μαγνητών και μαγνητικών εργαλείων στο χώρο όπου βρίσκονται οι servers του συστήματος	Τοποθέτηση αισθητήρων ανίχνευσης μαγνητικών εργαλείων στην είσοδο του χώρου όπου βρίσκονται οι servers του συστήματος	Επιβολή ποινών σε όποιον δεν συμμορφώνεται με τους κανονισμούς	
88	Κλοπή υλικού	Εγκατάσταση καμερών στους χώρους όπου βρίσκεται ο εξοπλισμός	Συνεχής παρακολούθηση του χώρου όλο το 24ώρο	Ύπαρξη εφεδρικού εξοπλισμού	
89	Βανδαλισμοί	Εγκατάσταση καμερών και συνεχή παρακολούθηση των εισόδων του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα	Έλεγχος των ατόμων που εισέρχονται στο κτίριο επιδεικνύοντας κάποιο αποδεικτικό στοιχείο (π.χ. ΑΔΤ)	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις	
95	Τρομοκρατικές ενέργειες	Συνεχής έλεγχος των εγκαταστάσεων όπου βρίσκεται ο εξοπλισμός για τυχόν εύρεση ύποπτων αντικειμένων εντός και εκτός του χώρου καθώς και ύποπτων συμπεριφορών των εργαζομένων	Χρήση ειδικού εξοπλισμού ανίχνευσης μετάλλων στην είσοδο του κτιρίου	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις	

Πίνακας 10: Μητρώο κινδύνων–Μείωση/Μετριασμός κινδύνων συστήματος E-Prescription

Πιο αναλυτικά, στα παραπάνω πεδία συμπληρώνονται τα εξής στοιχεία:

- στο πεδίο «σχέδιο αποφυγής» καταγράφονται οι ενέργειες που πρέπει να γίνουν εφ' όσον ο η στρατηγική του κινδύνου είναι η αποφυγή
- στο πεδίο «σχέδιο μεταφοράς» καταγράφονται οι ενέργειες που πρέπει να γίνουν εφ' όσον ο η στρατηγική του κινδύνου είναι η μεταφορά
- στο πεδίο «σχέδιο αποδοχής» καταγράφονται οι ενέργειες που πρέπει να γίνουν εφ' όσον ο η στρατηγική του κινδύνου είναι η αποδοχή

#	Κίνδυνοι	Σχέδιο αποφυγής	Σχέδιο μεταφοράς	Σχέδιο αποδοχής
1	Ασυμβατότητα λογισμικού με τις απαιτήσεις		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
2	Εξάντληση πόρων του συστήματος	Συνεχής έλεγχος για έγκαιρη διάγνωση του κινδύνου, άμεσες κινήσεις για την αύξηση των πόρων του συστήματος		
3	Λανθασμένη βάση δεδομένων		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
4	Ελλιπής ασφάλεια προσωπικών δεδομένων των πολιτών		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
5	Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
6	Έλλειψη διασυνδεσιμότητας των φορέων μέσω του συστήματος		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
7	Λανθασμένος σχεδιασμός υλικού (αρχιτεκτονική συστήματος)		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
8	Λανθασμένος σχεδιασμός λογισμικού (αρχιτεκτονική συστήματος)		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
9	Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
10	Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
11	Μη αποδεκτή ποιότητα λογισμικού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
12	Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του λογισμικού και του πληροφοριακού συστήματος		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
13	Αδυναμία Σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	Αποθήκευσης των δεδομένων και των προγραμμάτων του πληροφοριακού συστήματος σε περιβάλλον cloud		
14	Ανεπαρκής προστασία κρυπτογραφικών κλειδιών		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
15	Ελλιπής επικύρωση της επεξεργασίας των δεδομένων		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	

16	Δυσλειτουργία του υλικού			Τακτικός έλεγχος και συντήρηση του υλικού καθώς και ύπαρξη εφεδρικού υλικού ώστε να αποφευχθεί ο κίνδυνος
17	Ανεπαρκής έλεγχος του λογισμικού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
18	Σφάλματα λογισμικού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
19	Πολυπλοκότητα λογισμικού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
20	Μη ασφαλής αρχιτεκτονική δικτύου		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
22	Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	Σύνταξη του συμβολαίου από έμπειρα στελέχη		
23	Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
26	Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος			Έλεγχος της απόδοσης των χρηστών και συνεχής εκπαίδευση σε νέες τεχνολογίες
27	Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
28	Ανεπαρκής επίβλεψη των εργαζομένων		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
29	Ελλιπής διαδικασία για την αφαίρεση των δικαιωμάτων πρόσβασης κατά τη λήξη της απασχόλησης	Έλεγχος των ατόμων που συνδέονται καθημερινά στο σύστημα και είναι εν ενεργεία		
30	Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
31	Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
35	Έλλειψη οικονομικών πόρων	Δέσμευση κεφαλαίων για την κατασκευή του έργου		

36	Προβλήματα με την χρηματοδότηση του έργου	Δέσμευση κεφαλαίων για την κατασκευή του έργου		
38	Κλοπή υλικού από εργαζόμενους	Τακτικός έλεγχος του καταγεγραμμένου υλικού για τυχόν απώλειες		
41	Καταστροφή εξοπλισμού από υγρά/τρόφιμα	Ενημέρωση όλων των εργαζομένων για την απαγόρευση ποτών και τροφίμων στους χώρους όπου βρίσκεται ο εξοπλισμός		
44	Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
46	Μη εξουσιοδοτημένες αλλαγές αρχείων		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
47	Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος			Περιοδική ταυτοποίηση ενός δείγματος δεδομένων και έλεγχος των αποτελεσμάτων
50	Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο			Ενημέρωση των εργαζομένων να ελέγχουν πρώτα κάθε συσκευή που πρόκειται να συνδέσουν στο εταιρικό δίκτυο για τυχόν κακόβουλο λογισμικό
51	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
55	Λάθος κατανομή του κεφαλαίου		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
56	Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
57	Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος		Προκήρυξη διαγωνισμού για την ανάθεση του εφεδρικού σχεδίου με τη μέθοδο outsourcing σε εξειδικευμένες εταιρίες	

58	Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	Συνεχής έλεγχος του σχεδιασμού του συστήματος για έγκαιρη διάγνωση του κινδύνου, άμεσες κινήσεις για την αύξηση των πόρων υλικού		
59	Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
60	Λανθασμένη κοστολόγηση του έργου		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
61	Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
65	Κίνδυνος κεραυνού	Χρήση ειδικού εξοπλισμού για την αποφυγή κεραυνών (αλεξικέραυνο)		
70	Κατολίσθηση/ Διάβρωση εδάφους			Εύρεση νέων κτιριακών εγκαταστάσεων για τη στέγαση του πληροφοριακού συστήματος
71	Ηλιακές εκλάμψεις			Αποθήκευσης των δεδομένων και των προγραμμάτων του πληροφοριακού συστήματος σε περιβάλλον cloud
74	Ηλεκτρομαγνητικές παρεμβολές			Αποθήκευσης των δεδομένων και των προγραμμάτων του πληροφοριακού συστήματος σε περιβάλλον cloud
76	Έκρηξη ηφαιστείου	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή που δεν είναι ηφαιστειογενής		
77	Πυρηνικό ατύχημα	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή όπου δεν υπάρχουν πυρηνικά εργοστάσια		
83	Αγωγές – Μηνύσεις		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	

84	Απώλεια καλής φήμης		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
85	Κλοπή πνευματικής ιδιοκτησίας		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
86	Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων			Συμμετοχή των πολιτικών δυνάμεων στην απόφαση κατασκευής του συστήματος
87	Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας			Συμμετοχή των πολιτικών δυνάμεων στην απόφαση να μην επηρεαστεί το έργο
90	Εισβολείς (Hackers)-Υποκλοπή δεδομένων		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
91	Εισβολείς (Hackers) – Καταστροφή δεδομένων		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
92	Ηλεκτρονικοί εγκληματίες (Μετάδοση κακόβουλου λογισμικού)		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	
93	Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές			Όρος στο συμβόλαιο με τον εργαζόμενο για τη μη γνωστοποίηση σε τρίτους των εφαρμογών που κατασκευάζονται στην εταιρεία
94	Κατασκοπεία		Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου	

Πίνακας 11: Μητρώο κινδύνων–Αποφυγή, Μεταφορά, Αποδοχή κινδύνων συστήματος E-Prescription

6.6 Έλεγχος και παρακολούθηση κινδύνων

Στη φάση αυτή η ομάδα διαχείρισης κινδύνων πρέπει να παρακολουθεί τους κινδύνους που έχει προσδιορίσει, αναλύσει και αξιολογήσει ώστε να δει αν κάποιος κίνδυνος έχει αλλάξει μορφή και πρέπει να αλλάξει τη στρατηγική αντιμετώπισης που είχε ορίσει αρχικά. Επίσης, πρέπει να ελέγχει και να επαναλαμβάνει τη διαδικασία διαχείρισης των κινδύνων ώστε να είναι σε θέσει να εντοπίσει πιθανούς νέους κινδύνους που μπορεί να έχουν προκύψει.

Τέλος, ενημερώνει το μητρώο κινδύνων με τη συχνότητα που πρέπει να παρακολουθείται ο κάθε κίνδυνος, με την κατάσταση στην οποία βρίσκεται αυτός και με την ημερομηνία κλεισίματος, εφ' όσον κάποιος κίνδυνος θεωρείται ότι είτε έχει επέλθει και έχει περάσει είτε ότι δεν πρόκειται να συμβεί.

Πιο αναλυτικά, στα παραπάνω πεδία συμπληρώνονται τα εξής στοιχεία:

- στο πεδίο «παρακολούθηση» καταγράφεται η συχνότητα με την οποία πρέπει να παρακολουθείται ο κάθε κίνδυνος
- στο πεδίο «κατάσταση» καταγράφεται η κατάσταση του κινδύνου, αν δηλαδή είναι ανοιχτή (δεν έχει ακόμα συμβεί ο κίνδυνος), αν είναι κλειστή (έχει συμβεί ο κίνδυνος) ή αν είναι τελειωμένη (έχει ξεπεραστεί ο κίνδυνος).
- στο πεδίο «ημερομηνία κλεισίματος» καταγράφεται η ημερομηνία που έκλεισε ο κίνδυνος, εφ' όσον η κατάστασή του είναι κλειστή
- στο πεδίο «ημερομηνία ελέγχου» καταγράφεται η ημερομηνία που έγινε ο έλεγχος και η παρακολούθηση του κάθε κινδύνου

#	Κίνδυνοι	Παρακολούθηση	Κατάσταση	Ημερομηνία κλεισίματος	Ημερομηνία ελέγχου
1	Ασυμβατότητα λογισμικού με τις απαιτήσεις	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		31/10/2013
2	Εξάντληση πόρων του συστήματος	Μηνιαία	Ανοιχτή		31/10/2013
3	Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		31/10/2013
4	Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών	Κάθε μέρα	Ανοιχτή		31/10/2013
5	Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού	Εφόσον προκύψει	Ανοιχτή		31/10/2013
6	Έλλειψη διασυνδεσιμότητας των φορέων μέσω του συστήματος	Κάθε μέρα	Ανοιχτή		31/10/2013
7	Λανθασμένος σχεδιασμός υλικού (αρχιτεκτονική συστήματος)	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		31/10/2013
8	Λανθασμένος σχεδιασμός λογισμικού (αρχιτεκτονική συστήματος)	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		31/10/2013
9	Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	Εφόσον προκύψει	Κλειστή	2012	31/10/2013
10	Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		31/10/2013
11	Μη αποδεκτή ποιότητα λογισμικού	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		31/10/2013
12	Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του πληροφοριακού συστήματος	Μηνιαία	Ανοιχτή		31/10/2013
13	Αδυναμία Σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	Κάθε μέρα	Ανοιχτή		31/10/2013
14	Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	Μηνιαία	Ανοιχτή		31/10/2013
15	Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		31/10/2013
16	Δυσλειτουργία του υλικού	Κάθε 2 μήνες έλεγχος και συντήρηση του υλικού	Κλειστή	2012	31/10/2013
17	Ανεπαρκής έλεγχος του λογισμικού	Εφόσον προκύψει	Κλειστή	2012	31/10/2013
18	Σφάλματα λογισμικού	Εφόσον προκύψουν	Κλειστή	2012	31/10/2013
19	Πολυπλοκότητα λογισμικού	Εφόσον προκύψει	Κλειστή	2012	31/10/2013
20	Μη ασφαλής αρχιτεκτονική δικτύου	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		31/10/2013
21	Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	Εφόσον προκύψουν	Κλειστή	2012	31/10/2013
22	Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	1 φορά στην αρχική σύναψη του συμβολαίου	Τελειωμένη		31/10/2013
23	Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	1 φορά στην αρχική σύναψη του συμβολαίου	Τελειωμένη		31/10/2013
24	Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.	Έλεγχος κάθε μήνα για τη συνεργασία που υπάρχει μεταξύ των ομάδων	Κλειστή	2012	31/10/2013
25	Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)	Κάθε μέρα	Ανοιχτή		31/10/2013
26	Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	Εφόσον προκύψει	Κλειστή	2012	31/10/2013

27	Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων	Εξαμηνιαίος έλεγχος στις αναφορές που θα υπάρχουν από κάθε εργαζόμενο για το έργο που έχει υλοποιήσει	Κλειστή	2012	31/10/2013
28	Ανεπαρκής επίβλεψη των εργαζομένων	Μηνιαίος έλεγχος για το αν έχουν υλοποιηθεί οι στόχοι του προηγούμενου μήνα	Ανοιχτή		31/10/2013
29	Ελλιπής διαδικασία για την αφαίρεση των δικαιωμάτων πρόσβασης κατά τη λήξη της απασχόλησης	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		31/10/2013
30	Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		31/10/2013
31	Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		31/10/2013
32	Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	Κάθε μέρα	Ανοιχτή		31/10/2013
33	Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	Μηνιαία	Ανοιχτή		31/10/2013
34	Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	Κάθε μέρα	Ανοιχτή		31/10/2013
35	Έλλειψη οικονομικών πόρων	Εφόσον προκύψει	Ανοιχτή		31/10/2013
36	Προβλήματα με την χρηματοδότηση του έργου	Εφόσον προκύψει	Ανοιχτή		31/10/2013
37	Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος λόγω κακής χρήσης του	Κάθε μέρα	Ανοιχτή		31/10/2013
38	Κλοπή υλικού από εργαζομένους	Κάθε μέρα	Ανοιχτή		31/10/2013
39	Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	Εφόσον προκύψει	Κλειστή	2012	31/10/2013
40	Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	Εφόσον προκύψει	Κλειστή	2012	31/10/2013
41	Καταστροφή εξοπλισμού από υγρά/τρόφιμα	Κάθε μέρα	Ανοιχτή		31/10/2013
42	Διαρροή πληροφοριών	Κάθε μέρα	Ανοιχτή		31/10/2013
43	Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	Κάθε μέρα	Ανοιχτή		31/10/2013
44	Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους	Κάθε μέρα	Ανοιχτή		31/10/2013
45	Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	Κάθε μέρα	Ανοιχτή		31/10/2013
46	Μη εξουσιοδοτημένες αλλαγές αρχείων	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		31/10/2013
47	Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος	Μηνιαία	Ανοιχτή		31/10/2013
48	Έλλειψη κινήτρων για τους εργαζόμενους	Εφόσον προκύψει	Ανοιχτή		31/10/2013
49	Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	Εφόσον προκύψει	Ανοιχτή		31/10/2013
50	Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο	Κάθε μέρα	Ανοιχτή		31/10/2013
51	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού κι εφαρμογών	1 φορά στον αρχικό σχεδιασμό	Τελειωμένη		31/10/2013
52	Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	Κάθε μέρα	Ανοιχτή		31/10/2013
53	Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	Ετήσια	Ανοιχτή		31/10/2013

54	Εσωτερικοί κίνδυνοι (δόλος)	Κάθε μέρα	Ανοιχτή		31/10/2013
55	Λάθος κατανομή του κεφαλαίου	1 φορά πριν την έναρξη του έργου	Τελειωμένη		31/10/2013
56	Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	1 φορά πριν την έναρξη του έργου	Τελειωμένη		31/10/2013
57	Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	1 φορά πριν την έναρξη του έργου	Τελειωμένη		31/10/2013
58	Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	1 φορά πριν την έναρξη του έργου	Τελειωμένη		31/10/2013
59	Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	Μηνιαία μέχρι την ολοκλήρωση του έργου	Ανοιχτή		31/10/2013
60	Λανθασμένη κοστολόγηση του έργου	Μηνιαία μέχρι την ολοκλήρωση του έργου	Ανοιχτή		31/10/2013
61	Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	1 φορά στην αρχική σύναψη του συμβολαίου	Ανοιχτή		31/10/2013
62	Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	Εφόσον προκύψει	Ανοιχτή		31/10/2013
63	Λανθασμένες αποφάσεις διαχείρισης κινδύνων	Εφόσον προκύψει	Ανοιχτή		31/10/2013
64	Κίνδυνος σεισμού	Εφόσον προκύψει	Ανοιχτή		31/10/2013
65	Κίνδυνος Κεραυνού	Εφόσον προκύψει	Ανοιχτή		31/10/2013
66	Κίνδυνος πλημμύρας	Εφόσον προκύψει	Ανοιχτή		31/10/2013
67	Κίνδυνος πυρκαγιάς	Εφόσον προκύψει	Ανοιχτή		31/10/2013
68	Κίνδυνος διαρροής υδάτων	Εφόσον προκύψει	Ανοιχτή		31/10/2013
69	Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	Μηνιαία	Ανοιχτή		31/10/2013
70	Κατολίσθηση/ διάβρωση εδάφους	Εφόσον προκύψει	Ανοιχτή		31/10/2013
71	Ηλιακές εκλάμψεις	Εφόσον προκύψει	Ανοιχτή		31/10/2013
72	Σκόνη	Εβδομαδιαία	Ανοιχτή		31/10/2013
73	Βλάβη του συστήματος κλιματισμού	Μηνιαία	Ανοιχτή		31/10/2013
74	Ηλεκτρομαγνητικές παρεμβολές	Εφόσον προκύψει	Ανοιχτή		31/10/2013
75	Στατικός ηλεκτρισμός	Μηνιαία	Ανοιχτή		31/10/2013
76	Έκρηξη ηφαιστείου	Εφόσον προκύψει	Ανοιχτή		31/10/2013
77	Πυρηνικό ατύχημα	Εφόσον προκύψει	Ανοιχτή		31/10/2013
78	Κίνδυνος εκρήξεων	Εφόσον προκύψει	Ανοιχτή		31/10/2013
79	Έντομα/τρωκτικά	Εξαμηνιαία	Ανοιχτή		31/10/2013
80	Κίνδυνος δονήσεων	Εφόσον προκύψει	Ανοιχτή		31/10/2013
81	Καπνός/ μικροσωματίδια	Εφόσον προκύψει	Ανοιχτή		31/10/2013
82	Μαγνήτες/μαγνητικά εργαλεία	Εφόσον προκύψει	Ανοιχτή		31/10/2013
83	Αγωγές – Μηνύσεις	Εφόσον προκύψει	Ανοιχτή		31/10/2013

84	Απώλεια καλής φήμης	Εφόσον προκύψει	Ανοιχτή		31/10/2013
85	Κλοπή πνευματικής ιδιοκτησίας	Εφόσον προκύψει	Ανοιχτή		31/10/2013
86	Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	Εφόσον προκύψει	Ανοιχτή		31/10/2013
87	Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	Εφόσον προκύψει	Ανοιχτή		31/10/2013
88	Κλοπή υλικού	Κάθε 2 μήνες	Ανοιχτή		31/10/2013
89	Βανδαλισμοί	Κάθε μέρα	Ανοιχτή		31/10/2013
90	Εισβολείς (Hackers)- Υποκλοπή δεδομένων	Κάθε μέρα	Ανοιχτή		31/10/2013
91	Εισβολείς (Hackers)- Καταστροφή δεδομένων	Κάθε μέρα	Ανοιχτή		31/10/2013
92	Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού)	Κάθε μέρα	Ανοιχτή		31/10/2013
93	Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	Εφόσον προκύψει	Ανοιχτή		31/10/2013
94	Κατασκοπεία	Κάθε μέρα	Ανοιχτή		31/10/2013
95	Τρομοκρατικές ενέργειες	Κάθε μέρα	Ανοιχτή		31/10/2013

Πίνακας 12: Μητρώο κινδύνων–Παρακολούθηση κινδύνων συστήματος e- Prescription

Κατά τη φάση του εντοπισμού των κινδύνων δημιουργούνται τα φύλλα κινδύνων (risk sheet). Το φύλλο κινδύνου είναι ουσιαστικά η ταυτότητα του κάθε κινδύνου, δημιουργείται κατά τον εντοπισμό του και αρχειοθετείται όταν ο κίνδυνος έχει παρέλθει ή εκλείψει. Το φύλλο κινδύνου περιέχει στοιχεία από όλες τις φάσεις διαχείρισης κινδύνων.

Στη συνέχεια παρουσιάζονται τα φύλλα των κινδύνων (Πίνακες 13- 107)

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #1				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ασυμβατότητα λογισμικού με τις απαιτήσεις			
Σύντομη Περιγραφή:	Το ήδη υπάρχον λογισμικό δεν ανταποκρίνεται στις απαιτήσεις του συστήματος			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	5	X_3	80	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του συστήματος			
Προπομπός Κινδύνου:	Κάποια έκδοση δεν λειτουργεί σωστά			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 13: Φύλλο κινδύνου #1 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #2				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Εξάντληση πόρων του συστήματος			
Σύντομη Περιγραφή:	Εξάντληση των πόρων του συστήματος από την αυξημένη κίνηση των χρηστών του			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	5	Υ6	18	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Στατιστικά χρήσης του συστήματος			
Προπομπός Κινδύνου:	Η χρήση του συστήματος έχει ανέλθει στο ανώτατο κατώφλι ασφαλείας που έχει τεθεί από τον εργολάβο (π.χ. το 80% των πόρων του συστήματος)			
Στρατηγική αντιμετώπισης:	Αποφυγή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Συνεχής έλεγχος για έγκαιρη διάγνωση του κινδύνου, άμεσες κινήσεις για την αύξηση των πόρων του συστήματος			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 14: Φύλλο κινδύνου #2 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #3				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων			
Σύντομη Περιγραφή:	Λάθος ή ελλιπής δημιουργία της βάσης δεδομένων			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	5	X_3	81	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του συστήματος			
Προπομπός Κινδύνου:	Σε κάποια έκδοση η βάση δεδομένων δε λειτουργεί σωστά			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 15: Φύλλο κινδύνου #3 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #4				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλιπής ασφάλεια προσωπικών δεδομένων των πολιτών			
Σύντομη Περιγραφή:	Έλλειψη μεθόδων προστασίας των προσωπικών δεδομένων - έλλειψη πρωτοκόλλων ασφαλείας με αποτέλεσμα την πιθανή υποκλοπή των προσωπικών δεδομένων των χρηστών			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.9	5	Y_1	1	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος στις εκδόσεις των λογισμικών ασφαλείας			
Προπομπός Κινδύνου:	Υπάρχει ενδεχόμενο υποκλοπής κάποιων στοιχείων			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 16: Φύλλο κινδύνου #4 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #5				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού			
Σύντομη Περιγραφή:	Δημιουργία του κώδικα με μη δομημένο τρόπο με αποτέλεσμα την εμφάνιση δυσκολιών σε μελλοντικές αλλαγές και στην προσθήκη νέων λειτουργιών			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	54	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση του σχεδιασμού και των τεχνικών προδιαγραφών υλοποίησης του συστήματος			
Προπομπός Κινδύνου:	Εμφάνιση αυξημένης πολυπλοκότητας στην αρχιτεκτονική σχεδιασμού και δυσκολία εισαγωγής νέων χαρακτηριστικών			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 17: Φύλλο κινδύνου #5 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #6				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη διασυνδεσιμότητας των φορέων μέσω του συστήματος			
Σύντομη Περιγραφή:	Ελλιπής χρήση τεχνολογιών λογισμικού και πρωτοκόλλων για την διασυνδεσιμότητα μεταξύ των συσχετιζόμενων φορέων (π.χ. υπουργείο υγείας, ΓΓΚΑ, ΗΔΙΚΑ, Φ.Κ.Α)			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	3	M_4	36	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Πρωτόκολλα επικοινωνίας			
Προπομπός Κινδύνου:	Αδυναμία διασύνδεσης με τα συστήματα των άλλων φορέων			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 18: Φύλλο κινδύνου #6 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #7				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λανθασμένος σχεδιασμός υλικού (αρχιτεκτονική συστήματος)			
Σύντομη Περιγραφή:	Ανεπαρκής σχεδιασμός υλικού σε επίπεδο αρχιτεκτονικής συστήματος			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	5	X_3	82	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των απαιτήσεων σχεδιασμού			
Προπομπός Κινδύνου:	Λανθασμένη υλοποίηση των απαιτήσεων σχεδιασμού			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 19: Φύλλο κινδύνου #7 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #8				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λανθασμένος σχεδιασμός λογισμικού (αρχιτεκτονική συστήματος)			
Σύντομη Περιγραφή:	Ανεπαρκής σχεδιασμός λογισμικού σε επίπεδο αρχιτεκτονικής συστήματος			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	5	X_3	83	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των απαιτήσεων σχεδιασμού			
Προπομπός Κινδύνου:	Λανθασμένη υλοποίηση των απαιτήσεων σχεδιασμού			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 20: Φύλλο κινδύνου #8 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #9				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών			
Σύντομη Περιγραφή:	Επιλογή τεχνολογίας λογισμικού μη συμβατή με την υπάρχουσα δικτυακή υποδομή των συσχετιζόμενων φορέων			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	5	M_4	46	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση τεχνολογίας ανάπτυξης λογισμικού			
Προπομπός Κινδύνου:	Αδυναμία αξιοποίησης στο μέγιστο των υποδομών ροής πληροφοριών			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2012			
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 21: Φύλλο κινδύνου #9 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #10				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού			
Σύντομη Περιγραφή:	Επιλογή λογισμικού τελευταίας τεχνολογίας όπου δεν έχει ελεγχθεί εκτενώς όσον αφορά την ανάπτυξη αντίστοιχων εφαρμογών			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	3	M_4	37	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση τεχνολογίας ανάπτυξης λογισμικού			
Προπομπός Κινδύνου:	Αδυναμία κάλυψης των λειτουργικών απαιτήσεων του συστήματος			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 22: Φύλλο κινδύνου #10 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #11				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μη αποδεκτή ποιότητα λογισμικού			
Σύντομη Περιγραφή:	Η ποιότητα της εφαρμογής είναι χαμηλότερη των αποδεκτών ορίων που έχουν τεθεί και προβληματική για τους χρήστες			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	3	M_4	38	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των ποιοτικών χαρακτηριστικών του συστήματος			
Προπομπός Κινδύνου:	Απόκλιση από τα αποδεκτά όρια			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 23: Φύλλο κινδύνου #11 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #12				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του λογισμικού του πληροφοριακού συστήματος			
Σύντομη Περιγραφή:	Ελλιπής χρήσης λογισμικού ασφαλείας και αυστηρών μέτρων προστασίας για την αποφυγή κακόβουλων ενεργειών και υποκλοπή προσωπικών δεδομένων			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	5	X_3	84	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του λογισμικού ασφαλείας			
Προπομπός Κινδύνου:	Κάποια έκδοση του λογισμικού ασφαλείας δεν λειτουργεί σωστά με αποτέλεσμα την μετάδοση κακόβουλου λογισμικού			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 24: Φύλλο κινδύνου #12 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #13				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Αδυναμία Σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου			
Σύντομη Περιγραφή:	Ανεπαρκής διαδικτυακός εξοπλισμός για την αποτελεσματική εξυπηρέτηση του αριθμού των συνδεδεμένων χρηστών σε περιπτώσεις υψηλού φόρτου			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	4	M_2	24	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση χαρακτηριστικών του τηλεπικοινωνιακού δικτύου			
Προπομπός Κινδύνου:	Συνεχής υπερφόρτωση του δικτύου			
Στρατηγική αντιμετώπισης:	Αποφυγή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Αποθήκευσης των δεδομένων και των προγραμμάτων του πληροφοριακού συστήματος σε περιβάλλον cloud			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 25: Φύλλο κινδύνου #13 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #14				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ανεπαρκής προστασία κρυπτογραφικών κλειδιών			
Σύντομη Περιγραφή:	Λανθασμένη χρήση τεχνικών κρυπτογραφίας κλειδιών			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	55	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των απαιτήσεων ασφάλειας στο σχεδιασμό του λογισμικού			
Προπομπός Κινδύνου:	Λανθασμένη υλοποίηση των απαιτήσεων ασφάλειας			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 26: Φύλλο κινδύνου #14 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #15				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλιπής επικύρωση της επεξεργασίας των δεδομένων			
Σύντομη Περιγραφή:	Λανθασμένος κώδικας για τον έλεγχό της επεξεργασίας των δεδομένων εισαγωγής			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	56	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση του τρόπου επεξεργασίας των δεδομένων			
Προπομπός Κινδύνου:	Λανθασμένη επεξεργασία των δεδομένων			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 27: Φύλλο κινδύνου #15 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #16				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Δυσλειτουργία του υλικού			
Σύντομη Περιγραφή:	Αστοχία του υλικού που είναι αποθηκευμένο το πληροφοριακό σύστημα			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	4	M_2	25	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση του τρόπου λειτουργίας του υλικού			
Προπομπός Κινδύνου:	Συνεχής υπερθέρμανση του συστήματος/ έντονος ήχος κατά τη λειτουργία του			
Στρατηγική αντιμετώπισης:	Αποδοχή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Τακτικός έλεγχος και συντήρηση του υλικού καθώς και ύπαρξη εφεδρικού υλικού ώστε να αποφευχθεί ο κίνδυνος			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε 2 μήνες έλεγχος και συντήρηση του υλικού			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2012			
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 28: Φύλλο κινδύνου #16 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #17				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ανεπαρκής έλεγχος λογισμικού			
Σύντομη Περιγραφή:	Ανεπαρκείς και ελλιπείς διαδικασίες ποιοτικού ελέγχου			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	4	M_2	26	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των απαιτήσεων ελέγχου του λογισμικού			
Προπομπός Κινδύνου:	Λανθασμένη υλοποίηση των απαιτήσεων ελέγχου			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2012			
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 29: Φύλλο κινδύνου #17 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #18				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Σφάλματα λογισμικού			
Σύντομη Περιγραφή:	Εμφάνιση μεγάλου αριθμού λαθών στον κώδικα του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	5	Y_6	19	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του τρόπου λειτουργίας των εκδόσεων του λογισμικού			
Προπομπός Κινδύνου:	Κάποια έκδοση του λογισμικού δεν παράγει τα αναμενόμενα αποτελέσματα			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψουν			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2012			
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 30: Φύλλο κινδύνου #18 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #19				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Πολυπλοκότητα λογισμικού			
Σύντομη Περιγραφή:	Μη τήρηση συγκεκριμένης μεθοδολογίας για τη συγγραφή κώδικα του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	3	M_4	39	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος στον σχεδιασμό του λογισμικού			
Προπομπός Κινδύνου:	Δυσκολία στην αναβάθμιση του λογισμικού			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2012			
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 31: Φύλλο κινδύνου #19 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #20				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μη ασφαλής αρχιτεκτονική δικτύου			
Σύντομη Περιγραφή:	Ανεπαρκής επιλογή επιπέδων ασφάλειας διαδικτύου			
Κατηγορία Κινδύνου:	Τεχνολογικός			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	4	M_2	27	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των απαιτήσεων ασφάλειας για το σχεδιασμό του δικτύου			
Προπομπός Κινδύνου:	Λανθασμένη υλοποίηση των απαιτήσεων ασφάλειας			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:				

Πίνακας 32: Φύλλο κινδύνου #20 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #21				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου			
Σύντομη Περιγραφή:	Αδυναμία αποτελεσματικής επικοινωνίας με την εταιρεία ανάθεσης με αποτέλεσμα την επιβράδυνση των εργασιών για την κατασκευή του έργου			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	2	M_7	70	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος της επικοινωνίας με την εταιρεία ανάθεσης έργου			
Προπομπός Κινδύνου:	Έλλειψη επικοινωνίας με την εταιρεία ανάθεσης έργου			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Συναντήσεις με την εταιρεία ανάθεσης έργου για επίτευξη καλύτερης επικοινωνίας			
Διορθωτικά μέτρα:	Υπαρξη έγγραφων αναφορών για την αποφυγή παρερμηνεύσεων			
Εναλλακτικό σχέδιο:	Εφαρμογή των κυρώσεων που αναγράφονται στο συμβόλαιο			
Σχέδιο μετάπτωσης:	Ακύρωση του συμβολαίου με την εταιρεία ανάθεσης έργου και ανάθεση του έργου στον επόμενο μειοδότη			
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψουν			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2012			
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 33: Φύλλο κινδύνου #21 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #22				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου			
Σύντομη Περιγραφή:	Ασάφειες και κενά στους όρους του συμβολαίου οδηγούν στην ανεπαρκή εφαρμογή των συμφωνηθέντων στην περίπτωση εμφάνισης προβλήματος			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	2	M_7	71	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση της διαδικασίας καθορισμού των όρων του συμβολαίου			
Προπομπός Κινδύνου:	Ύπαρξη ασαφειών μεταξύ των όρων του συμβολαίου			
Στρατηγική αντιμετώπισης:	Αποφυγή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Σύνταξη του συμβολαίου από έμπειρα στελέχη			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στην αρχική σύναψη του συμβολαίου			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 34: Φύλλο κινδύνου #22 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #23				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος			
Σύντομη Περιγραφή:	Ανεπαρκής αριθμός ατόμων για την υποστήριξη του συστήματος λόγω κόστους σε ανθρώπινο δυναμικό			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	4	M_2	28	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση ανταπόκρισης της ομάδα υποστήριξης του συστήματος σε περίπτωση ανάγκης			
Προπομπός Κινδύνου:	Προβληματική υποστήριξη του συστήματος			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στην αρχική σύναψη του συμβολαίου			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 35 : Φύλλο κινδύνου #23 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #24				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.			
Σύντομη Περιγραφή:	Προβλήματα επικοινωνίας και καταμερισμού εργασιών των ομάδων ανάπτυξης λογισμικού με αποτέλεσμα τη δημιουργία εντάσεων μεταξύ των ατόμων και την διακοπή της ομαλής εξέλιξης του έργου			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	3	M_4	40	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση της επικοινωνίας μεταξύ των ομάδων			
Προπομπός Κινδύνου:	Προβληματική συνεργασία μεταξύ των ομάδων			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Συνεχής επικοινωνία μεταξύ των ομάδων κατασκευής του έργου			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:	Συγκέντρωση των ομάδων κατασκευής στον ίδιο χώρο			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Έλεγχος κάθε μήνα για τη συνεργασία που υπάρχει μεταξύ των ομάδων			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2012			
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 36: Φύλλο κινδύνου #24 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #25				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)			
Σύντομη Περιγραφή:	Η έλλειψη φύλαξης ενός κτηρίου από άτομο επιπλέον των τεχνικών μέσων μπορεί να έχει ως αποτέλεσμα την μη έγκαιρη αντιμετώπιση οποιασδήποτε πιθανή καταστροφής του κτηρίου όπου στεγάζεται το πληροφοριακό σύστημα			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	5	M_4	47	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση της ασφάλειας του κτιρίου			
Προπομπός Κινδύνου:	Εμφάνιση φαινομένων εισβολής			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Πρόσληψη προσωπικού για τη φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα			
Διορθωτικά μέτρα:	Πρόσληψη ειδικά εκπαιδευμένου προσωπικού			
Εναλλακτικό σχέδιο:	Χρήση ειδικού εξοπλισμού παρακολούθησης του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα (κάμερες ασφαλείας)			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 37: Φύλλο κινδύνου #25 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #26				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος			
Σύντομη Περιγραφή:	Δεν έχει δοθεί αρκετό χρονικό διάστημα για την εξοικείωση των χρηστών (ιατροί, φαρμακοποιοί) με το νέο λογισμικό ώστε να υπάρχουν προβλήματα στη σύνταξη των συνταγών (χειρόγραφες, ηλεκτρονικές) με αποτέλεσμα την προβληματική εξυπηρέτηση των πολιτών			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	2	M_5	52	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του χρόνου προσαρμογής των χρηστών			
Προπομπός Κινδύνου:	Απόκλιση από τον προβλεπόμενο χρόνο προσαρμογής			
Στρατηγική αντιμετώπισης:	Αποδοχή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Έλεγχος της απόδοσης των χρηστών και συνεχής εκπαίδευση σε νέες τεχνολογίες			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2012			
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 38: Φύλλο κινδύνου #26 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #27				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων			
Σύντομη Περιγραφή:	Ελλιπής ή λανθασμένη επιλογή ατόμων για την υλοποίηση μερών του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	3	M_1	22	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος και αξιολόγηση των εργαζομένων του συστήματος σύμφωνα με τα προσόντα και τις γνώσεις τους			
Προπομπός Κινδύνου:	Λανθασμένη υλοποίηση του συστήματος και μη σωστή λειτουργία των ομάδων που συνεργάζονται για την υλοποίηση του συστήματος			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εξαμηνιαίος έλεγχος στις αναφορές που θα υπάρχουν από κάθε εργαζόμενο για το έργο που έχει υλοποιήσει			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2012			
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 39: Φύλλο κινδύνου #27 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #28				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ανεπαρκής επίβλεψη εργαζομένων			
Σύντομη Περιγραφή:	Ελλιπής επιλογή κατάλληλων ατόμων για επίβλεψη των εργαζομένων με αποτέλεσμα τη μη τήρηση του χρονοδιαγράμματος			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	4	M_2	29	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Μη ύπαρξη προσωπικού για την επίβλεψη εργαζομένων			
Προπομπός Κινδύνου:	Καθυστέρηση στην υλοποίηση του έργου/Υπαρξη λαθών κατά την υλοποίηση του έργου			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαίος έλεγχος για το αν έχουν υλοποιηθεί οι στόχοι του προηγούμενου μήνα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 40: Φύλλο κινδύνου #28 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #29				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλιπής διαδικασία για την αφαίρεση δικαιωμάτων πρόσβασης κατά την λήξη της απασχόλησης			
Σύντομη Περιγραφή:	Η διαδικασία διακοπής συνεργασίας δεν πληροί όλες τις προϋποθέσεις που χρειάζονται για τη μη πρόσβαση των πρώην εργαζομένων στο πληροφοριακό σύστημα και στους χώρους του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	57	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των ατόμων που συνδέονται καθημερινά στο σύστημα			
Προπομπός Κινδύνου:	Ανίχνευση πρόσβασης στο σύστημα από πρώην εργαζόμενο στην εταιρεία			
Στρατηγική αντιμετώπισης:	Αποφυγή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Έλεγχος των ατόμων που συνδέονται καθημερινά στο σύστημα και είναι εν ενεργεία			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 41: Φύλλο κινδύνου #29 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #30				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού			
Σύντομη Περιγραφή:	Ανεπαρκής διαδικασία τακτικού ελέγχου της λειτουργίας του λογισμικού			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	3	M_1	23	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος της λειτουργίας του λογισμικού			
Προπομπός Κινδύνου:	Μη αναμενόμενη συμπεριφορά του λογισμικού			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 42: Φύλλο κινδύνου #30 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #31				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας			
Σύντομη Περιγραφή:	Εσφαλμένη εγκατάσταση υλικού ή λογισμικού λόγω έλλειψης τεχνικών γνώσεων ή εξαιτίας απλού ανθρώπινου σφάλματος του προσωπικού			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	5	Y_6	20	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου			
Προπομπός Κινδύνου:	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 43: Φύλλο κινδύνου #31 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #32				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού			
Σύντομη Περιγραφή:	Μη εγκατεστημένο σύστημα ειδοποίησης σε περίπτωση εισβολής στο χώρο του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	4	Y_4	7	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό			
Προπομπός Κινδύνου:	Μη αναμενόμενη συμπεριφορά του υλικού, μη τακτική συντήρηση του υλικού			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εγκατάσταση συστήματος συναγερμού			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 44: Φύλλο κινδύνου #32 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #33				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης			
Σύντομη Περιγραφή:	Μη εγκατεστημένο σύστημα ειδοποίησης σε περίπτωση πυρκαγιάς			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	4	Y_4	8	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό			
Προπομπός Κινδύνου:	Μη αναμενόμενη συμπεριφορά του υλικού, ύπαρξη εύφλεκτων υλικών στο χώρο, μη τακτική συντήρηση του υλικού			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εγκατάσταση συστήματος πυρανίχνευσης			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 45: Φύλλο κινδύνου #33 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #34				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας			
Σύντομη Περιγραφή:	Μη εγκατεστημένο σύστημα αναγνώρισης και ελέγχου ταυτότητας για την είσοδο στους χώρους του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Λειτουργικοί – Επιχειρησιακοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	4	Y_4	9	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό			
Προπομπός Κινδύνου:	Μη αναμενόμενη συμπεριφορά του υλικού, μη τακτική συντήρηση του υλικού			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εγκατάσταση μηχανημάτων ελέγχου ταυτότητας στις εσωτερικές εισόδους που οδηγούν σε κάθε όροφο			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 46: Φύλλο κινδύνου #34 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #35				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη οικονομικών πόρων			
Σύντομη Περιγραφή:	Ανεπαρκείς οικονομικοί πόροι οδηγούν σε αδυναμία έναρξης ανάπτυξης του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Χρηματοοικονομικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	3	M_4	41	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Οικονομικοί δείκτες ρευστότητας και χρηματοδότησης του έργου			
Προπομπός Κινδύνου:	Περικοπή κάποιου προϋπολογισμού			
Στρατηγική αντιμετώπισης:	Αποφυγή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Δέσμευση κεφαλαίων για την κατασκευή του έργου			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 47: Φύλλο κινδύνου #35 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #36				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Προβλήματα με την χρηματοδότηση του έργου			
Σύντομη Περιγραφή:	Συνεχόμενες διακοπές κατά την υλοποίηση του έργου λόγω προβλημάτων στη χρηματοδότηση με αποτέλεσμα την χρονική καθυστέρηση και την αύξηση του κόστους.			
Κατηγορία Κινδύνου:	Χρηματοοικονομικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	2	M_5	53	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Ανακοινώσεις της κυβέρνησης σχετικά με τη χρηματοδότηση του έργου			
Προπομπός Κινδύνου:	Ύπαρξη γενικότερων οικονομικών προβλημάτων και έλλειψη ρευστότητας του κράτους			
Στρατηγική αντιμετώπισης:	Αποφυγή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Δέσμευση κεφαλαίων για την κατασκευή του έργου			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 48: Φύλλο κινδύνου #36 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #37				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος			
Σύντομη Περιγραφή:	Καταστροφή υλικού ή λογισμικού του συστήματος λόγω κακής χρήσης του			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	4	Y_4	10	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Επιθεώρηση του υλικού και του χώρου στον οποίο βρίσκεται αυτό.			
Προπομπός Κινδύνου:	Μη αναμενόμενη συμπεριφορά του υλικού, μη τακτική συντήρηση του υλικού			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εκπαίδευση των εργαζομένων σχετικά με τον τρόπο χρήσης του εξοπλισμού			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:	Επίπληξη εργαζομένου που δεν συμβαδίζει με τους κανονισμούς ασφαλής χρήσης του εξοπλισμού			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 49: Φύλλο κινδύνου #37 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #38				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κλοπή υλικού από εργαζομένους			
Σύντομη Περιγραφή:	Το υλικό ενδέχεται να κλαπεί από τους εργαζόμενους			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	4	Y_4	11	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του εξοπλισμού σε τακτά χρονικά διαστήματα			
Προπομπός Κινδύνου:	Μη ταύτιση καταγεγραμμένου και υπάρχοντος εξοπλισμού			
Στρατηγική αντιμετώπισης:	Αποφυγή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Τακτικός έλεγχος του καταγεγραμμένου υλικού για τυχόν απώλειες			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 50: Φύλλο κινδύνου #38 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #39				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα			
Σύντομη Περιγραφή:	Καθυστέρηση στην υλοποίηση του έργου λόγω απεργιακών κινητοποιήσεων από τους εργαζόμενους.			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	4	M_2	30	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση της συμπεριφοράς των εργαζομένων ως προς τα εργασιακά ζητήματα			
Προπομπός Κινδύνου:	Εμφάνιση αντιδράσεων σε εργασιακές αλλαγές			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Επικοινωνία με τους εργαζόμενους για την κατανόηση των αναγκών τους και συζήτηση μαζί τους για την εύρεση της βέλτιστης λύσης			
Διορθωτικά μέτρα:	Ύπαρξη εγγράφων που να γίνεται η καταγραφή των αναγκών των εργαζομένων με στόχο την κάλυψη των περισσότερων αναγκών			
Εναλλακτικό σχέδιο:	Αλλαγή αρμοδιοτήτων			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2012			
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 51: Φύλλο κινδύνου #39 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #40				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή			
Σύντομη Περιγραφή:	Απροθυμία των εργαζομένων του πληροφοριακού συστήματος να προσαρμοστούν στα νέα δεδομένα του εργασιακού τους περιβάλλοντος			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	4	Y_4	12	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των στατιστικών χρήσης του συστήματος			
Προπομπός Κινδύνου:	Τα στατιστικά χρήσης του συστήματος είναι στο κατώτατο όριο από αυτό που έχει οριστεί από την εταιρεία ανάθεσης του έργου			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Μελέτη των αναγκών των χρηστών για την κατανόηση των αναγκών τους όσον αφορά τη χρήση της εφαρμογής			
Διορθωτικά μέτρα:	Καταγραφή των αναγκών των χρηστών και υλοποίηση τυχόν αλλαγές στην εφαρμογής για να είναι πιο φιλικοί προς τους χρήστες			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Κλειστή			
Ημερομηνία Κλεισίματος:	2012			
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 52: Φύλλο κινδύνου #40 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #41				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Καταστροφή εξοπλισμού από υγρά/τρόφιμα			
Σύντομη Περιγραφή:	Καταστροφή υλικού του πληροφοριακού συστήματος από επικίνδυνα υλικά που δεν επιτρέπονται κοντά στον εξοπλισμό (π.χ. τρόφιμα, υγρά)			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	4	M_2	31	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος αν υπάρχει σήμανση για την απαγόρευση των τροφίμων και των ποτών στου χώρους που βρίσκεται το πληροφοριακό σύστημα			
Προπομπός Κινδύνου:	Εργαζόμενοι που εισέρχονται με τρόφιμα και ποτά στους χώρους του πληροφοριακού συστήματος			
Στρατηγική αντιμετώπισης:	Αποφυγή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Ενημέρωση όλων των εργαζομένων για την απαγόρευση ποτών και τροφίμων στους χώρους όπου βρίσκεται ο εξοπλισμός			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 53: Φύλλο κινδύνου #41 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #42				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Διαρροή πληροφοριών			
Σύντομη Περιγραφή:	Διάδοση εμπιστευτικών πληροφοριών που αφορούν προσωπικά δεδομένα από εργαζόμενους σε μη εξουσιοδοτημένα άτομα.			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	4	Y_4	13	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος για την ύπαρξη ειδικού λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος			
Προπομπός Κινδύνου:	Μη ύπαρξη του λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εγκατάσταση ειδικού λογισμικού το οποίο ελέγχει τις ενέργειες των εργαζομένων			
Διορθωτικά μέτρα:	Ενημέρωση των εργαζομένων σχετικά με τους κανονισμούς της εταιρείας όσον αφορά την ασφάλεια των πληροφοριών και των δεδομένων			
Εναλλακτικό σχέδιο:	Επίπληξη εργαζομένου που δεν συμβαδίζει με του κανονισμούς της εταιρείας			
Σχέδιο μετάπτωσης:	Επιβολή ποινών σε όποιον δεν ακολουθεί τους κανονισμούς της εταιρείας			
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 54: Φύλλο κινδύνου #42 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #43				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος			
Σύντομη Περιγραφή:	Ικανότητα μη εξουσιοδοτημένων ατόμων να έχουν πρόσβαση στους χώρους όπου βρίσκεται το πληροφοριακό σύστημα με αποτέλεσμα την πρόκληση φθοράς του εξοπλισμού			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
4	4	Y_3	17	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος για την ύπαρξη συσκευών αναγνώρισης των ειδικών καρτών των εργαζομένων			
Προπομπός Κινδύνου:	Μη ύπαρξη των συσκευών αναγνώρισης στις εισόδους του κτιρίου που στεγάζεται το σύστημα			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Συνεχής έλεγχος των εγκαταστάσεων όπου βρίσκεται ο εξοπλισμός			
Διορθωτικά μέτρα:	Χρήση ειδικού εξοπλισμού όπου απαγορεύει την πρόσβαση μη εξουσιοδοτημένου προσωπικού στους χώρους εγκατάστασης του εξοπλισμού			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 55: Φύλλο κινδύνου #43 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #44				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους			
Σύντομη Περιγραφή:	Ικανότητα μη εξουσιοδοτημένων ατόμων να έχουν πρόσβαση στο πληροφοριακό σύστημα με αποτέλεσμα την πρόκληση καταστροφής του λογισμικού			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	5	Y_3	3	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου			
Προπομπός Κινδύνου:	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 56: Φύλλο κινδύνου #44 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #45				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος			
Σύντομη Περιγραφή:	Γνωστοποίηση των κωδικών εισόδου του πληροφοριακού συστήματος σε μη εξουσιοδοτημένα άτομα.			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	5	Y_3	4	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος για την ύπαρξη ειδικού λογισμικού που να καταγράφει την ηλεκτρονική διεύθυνση που αντιστοιχεί σε κάθε εργαζόμενο			
Προπομπός Κινδύνου:	Μη ύπαρξη του ειδικού λογισμικού			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Ενημέρωση των εργαζομένων για τη διαφύλαξη των κωδικών που έχουν για τη χρήση του πληροφοριακού συστήματος			
Διορθωτικά μέτρα:	Δυνατότητα αλλαγής των κωδικών περιοδικά			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 57: Φύλλο κινδύνου #45 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #46				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μη εξουσιοδοτημένες αλλαγές αρχείων			
Σύντομη Περιγραφή:	Ελλιπή μηχανισμός κατανομής δικαιωμάτων διαχείρισης στους εργαζομένους του πληροφοριακού συστήματος με αποτέλεσμα τη δυνατότητα πρόσβαση όλων των εργαζομένων σε όλα τα μέρη του συστήματος			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	5	M_4	48	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου			
Προπομπός Κινδύνου:	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 58 : Φύλλο κινδύνου #46 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #47				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος			
Σύντομη Περιγραφή:	Μη εσκεμμένη αλλαγή των δεδομένων			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	5	M_4	49	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Περιοδική ταυτοποίηση ενός δείγματος δεδομένων και έλεγχος των αποτελεσμάτων			
Προπομπός Κινδύνου:	Εμφάνιση σφαλμάτων κατά την ταυτοποίηση			
Στρατηγική αντιμετώπισης:	Αποδοχή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Περιοδική ταυτοποίηση ενός δείγματος δεδομένων και έλεγχος των αποτελεσμάτων			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 59: Φύλλο κινδύνου #47 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #48				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη κινήτρων για τους εργαζόμενους			
Σύντομη Περιγραφή:	Μη ύπαρξη διαδικασίας ανταμοιβής για τους εργαζόμενους			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	4	M_2	32	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση δεικτών παραγωγικότητας			
Προπομπός Κινδύνου:	Μείωση παραγωγικότητας των εργαζομένων			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Επικοινωνία με τους εργαζόμενους για την κατανόηση των αναγκών τους και συζήτηση μαζί τους για την εύρεση της βέλτιστης λύσης			
Διορθωτικά μέτρα:	Δημιουργία περισσότερων κινήτρων για τους εργαζόμενους με βάση τις ανάγκες που έχουν			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 60: Φύλλο κινδύνου #48 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #49				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας			
Σύντομη Περιγραφή:	Ελλιπής εκπαίδευση εργαζομένων σε θέματα ασφαλείας του πληροφοριακού συστήματος			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	4	Y_4	15	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση της τήρησης των κανόνων ασφαλείας			
Προπομπός Κινδύνου:	Εμφάνισης συχνής παραβατικότητας			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εκπαίδευση των εργαζομένων σε θέματα ασφάλειας του εξοπλισμού και του λογισμικού			
Διορθωτικά μέτρα:	Καταγραφή και ενημέρωση των εργαζομένων με του κανόνες που πρέπει να ακολουθούν για την ασφάλεια του πληροφοριακού συστήματος			
Εναλλακτικό σχέδιο:	Επίπληξη εργαζομένου που δεν συμβαδίζει με του κανονισμούς της ασφάλειας του πληροφοριακού συστήματος			
Σχέδιο μετάπτωσης:	Επιβολή ποινών σε όποιον δεν ακολουθεί τους κανονισμούς της ασφάλειας του πληροφοριακού συστήματος			
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 61: Φύλλο κινδύνου #49 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #50				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο			
Σύντομη Περιγραφή:	Ο κάθε εργαζόμενος μπορεί να χρησιμοποιήσει δικές του συσκευές για να συνδεθεί στο δίκτυο της εταιρείας με αποτέλεσμα τη διάδοση κακόβουλου λογισμικού			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	4	Y_4	16	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Τακτικός έλεγχος του δικτύου μέσω λογισμικού ασφαλείας (Antivirus)			
Προπομπός Κινδύνου:	Εμφάνιση και διόρθωση ιού κατά τη διαδικασία του τακτικού ελέγχου			
Στρατηγική αντιμετώπισης:	Αποδοχή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Ενημέρωση των εργαζομένων να ελέγχουν πρώτα κάθε συσκευή που πρόκειται να συνδέσουν στο εταιρικό δίκτυο για τυχόν κακόβουλο λογισμικό			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 62: Φύλλο κινδύνου #50 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #51				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού και εφαρμογών			
Σύντομη Περιγραφή:	Εγκατάσταση επικίνδυνου για το πληροφοριακό σύστημα λογισμικού και εφαρμογών			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	5	M_4	50	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Τακτικός έλεγχος για την αυθεντικότητα του λογισμικού και των εφαρμογών			
Προπομπός Κινδύνου:	Εμφάνιση μη εξουσιοδοτημένου λογισμικού και εφαρμογών			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Ύπαρξη ειδικού λογισμικού ασφαλείας όπου ανιχνεύει την εγκατάσταση μη εξουσιοδοτημένου λογισμικού στο σύστημα			
Διορθωτικά μέτρα:	Τακτικός έλεγχος του λογισμικού και των εφαρμογών που χρησιμοποιούνται			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στον αρχικό σχεδιασμό			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 63: Φύλλο κινδύνου #51 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #52				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου			
Σύντομη Περιγραφή:	Μη εσκεμμένη διάδοση προσωπικών δεδομένων μέσω συσκευών αποθήκευσης (π.χ. σκληρός δίσκος.)			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	4	M_2	33	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος για την ύπαρξη ειδικού λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος			
Προπομπός Κινδύνου:	Μη ύπαρξη του λογισμικού που να καταγράφει τις κινήσεις του κάθε εργαζομένου κατά τη διάρκεια της χρήσης του πληροφοριακού συστήματος			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Μη δυνατή αποθήκευση των προσωπικών δεδομένων σε αποθηκευτικά μέσα καθώς μη ύπαρξη δυνατότητας μεταφορά δεδομένων μέσω διαδικτύου			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 64: Φύλλο κινδύνου #52 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #53				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού			
Σύντομη Περιγραφή:	Μη επαρκής επιμόρφωση των εργαζομένων προκειμένου να ανταπεξέλθουν στις νέες απαιτήσεις			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	1	X_1	78	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση του αρχείου εκπαίδευσης των υπαλλήλων			
Προπομπός Κινδύνου:	Ύπαρξη προβλημάτων κατά τη χρήση του συστήματος			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εκπαίδευση του προσωπικού για την ανταπόκρισή του στις απαιτήσεις του συστήματος			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:	Αλλαγή αρμοδιοτήτων			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Ετήσια			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 65: Φύλλο κινδύνου #53 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #54				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Εσωτερικοί κίνδυνοι (δόλος)			
Σύντομη Περιγραφή:	Κίνδυνος δολιοφθορών του πληροφοριακού συστήματος από δυσαρεστημένα στελέχη ή υπαλλήλους που εργάζονται στον οργανισμό			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	3	M_3	74	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση συμπεριφοράς εργαζομένων			
Προπομπός Κινδύνου:	Ύποπτες κινήσεις εργαζομένων			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Χρήση κωδικών ασφαλείας έτσι ώστε ο κάθε χρήστης να έχει δικαιώματα στο σύστημα ανάλογα με την ιδιότητά του			
Διορθωτικά μέτρα:	Χρήση εξειδικευμένου λογισμικού έτσι ώστε να ελέγχονται όλες οι ενέργειες των χρηστών			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 66: Φύλλο κινδύνου #54 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #55				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λάθος κατανομή του κεφαλαίου			
Σύντομη Περιγραφή:	Λανθασμένη πρόβλεψη κοστολόγησης τμημάτων του πληροφοριακού συστήματος έτσι ώστε σε μερικά τμήματα του έργου να είναι αναγκαία η ανακοστολόγηση και αυτό να έχει ως αποτέλεσμα την καθυστέρηση του έργου			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	3	M_8	75	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση της προσυμφωνημένης κατανομής του κεφαλαίου			
Προπομπός Κινδύνου:	Ανομοιόμορφη κατανομή του κεφαλαίου			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά πριν την έναρξη του έργου			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 67: Φύλλο κινδύνου #55 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #56				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος			
Σύντομη Περιγραφή:	Λανθασμένη βαρύτητα κατά το σχεδιασμό των μερών του πληροφοριακού συστήματος μπορεί να οδηγήσει σε αναθεώρηση ορισμένων από αυτά και επανασχεδιασμού του έργου συνολικά			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	58	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος στις εκδόσεις του συστήματος			
Προπομπός Κινδύνου:	Το σύστημα δεν καλύπτει κάποια σημαντικά σημεία που έπρεπε να έχουν ληφθεί πολύ σοβαρά υπ' όψιν			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά πριν την έναρξη του έργου			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 68: Φύλλο κινδύνου #56 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #57				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος			
Σύντομη Περιγραφή:	Έλλειψη εφεδρικού σχεδίου σε περίπτωση διακοπής ηλεκτροδότησης ή σε περίπτωση προβλημάτων λειτουργίας των διακομιστών που υποστηρίζουν το πληροφοριακό σύστημα			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	4	M_2	34	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση του σχεδιασμού του έργου			
Προπομπός Κινδύνου:	Ανεπαρκής ή ελλιπής ύπαρξη εφεδρικού σχεδίου κατά το στάδιο ολοκλήρωσης του έργου			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Προκήρυξη διαγωνισμού για την ανάθεση του εφεδρικού σχεδίου με τη μέθοδο outsourcing σε εξειδικευμένες εταιρίες			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά πριν την έναρξη του έργου			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 69: Φύλλο κινδύνου #57 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #58				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού			
Σύντομη Περιγραφή:	Έλλειψη υλικών πόρων (π.χ. διακομιστές, καλωδίωση κτιρίου κ.τ.λ.)χρήσιμων για την κατασκευή του έργου λόγω λανθασμένης αρχικής πρόβλεψης.			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	3	M_4	42	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του προγραμματισμού των απαιτούμενων πόρων υλικού			
Προπομπός Κινδύνου:	Απόκλιση από τον αρχικό προγραμματισμό των απαιτούμενων πόρων			
Στρατηγική αντιμετώπισης:	Αποφυγή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Συνεχής έλεγχος του σχεδιασμού του συστήματος για έγκαιρη διάγνωση του κινδύνου, άμεσες κινήσεις για την αύξηση των πόρων υλικού			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά πριν την έναρξη του έργου			
Κατάσταση:	Τελειωμένη			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 70: Φύλλο κινδύνου #58 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #59				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού			
Σύντομη Περιγραφή:	Επιλογή ακολουθίας εργασιών διάφορη της βέλτιστης που έχει ως αποτέλεσμα την χρονική επιμήκυνση του έργου σε σχέση με τη βέλτιστη επιλογή			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	2	M_7	72	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση και σύγκριση του πραγματικού χρονοδιαγράμματος με το εκτιμώμενο			
Προπομπός Κινδύνου:	Παρατήρηση καθυστερήσεων κατά τα επιμέρους στάδια ολοκλήρωσης του έργου			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία μέχρι την ολοκλήρωση του έργου			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 71: Φύλλο κινδύνου #59 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #60				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λανθασμένη κοστολόγηση του έργου			
Σύντομη Περιγραφή:	Το κόστος υλοποίησης του συστήματος αυξήθηκε, θέτοντας σε κίνδυνο την υπόσταση του έργου			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	3	M_4	43	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση οικονομικών δεικτών			
Προπομπός Κινδύνου:	Τα πρώτα στάδια της υλοποίησης του έργου βγαίνουν εκτός του αρχικού προϋπολογισμού			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία μέχρι την ολοκλήρωση του έργου			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 72: Φύλλο κινδύνου #60 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #61				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές			
Σύντομη Περιγραφή:	Πρόσβαση σε εμπιστευτικά δεδομένα από συνεργάτες και προμηθευτές			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	3	M_8	76	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των όρων που υπάρχουν στο συμβόλαιο με την εταιρεία ανάθεσης έργου			
Προπομπός Κινδύνου:	Μη ύπαρξη του όρου για την αποφυγή του κινδύνου			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	1 φορά στην αρχική σύναψη του συμβολαίου			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 73: Φύλλο κινδύνου #61 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #62				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου			
Σύντομη Περιγραφή:	Παρακολούθηση της υλοποίησης του πληροφοριακού συστήματος από άτομα με καθόλου ή λίγη εμπειρία και με ελλιπής γνώσεις τεχνογνωσίας καθώς και ελλιπής γνώσεις τα οποία σε μελλοντικό χρόνο θα κληθούν να λάβουν σημαντικές αποφάσεις κάτω από πιθανές συνθήκες πίεσης ή έλλειψης χρόνου			
Κατηγορία Κινδύνου:	Στρατηγικοί - Οργανωτικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	59	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Ελλιπής έλεγχος των απαραίτητων διαδικασιών για την διεξαγωγή του έργου			
Προπομπός Κινδύνου:	Εμφάνιση πολλών λαθών κατά τη διάρκεια του προγραμματισμού και της διαχείρισης του έργου			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Έλεγχος των εργαζομένων που προσλαμβάνονται για να αναλάβουν την παρακολούθηση του έργου σύμφωνα με την εμπειρία τους και τις γνώσεις που έχουν για τη συγκεκριμένη θέση με τη βοήθεια συνεντεύξεων και γραπτού διαγωνισμού όπου οι υποψήφιοι θα εξετάζονται σε θέματα που αφορούν τη διαχείριση ενός έργου			
Διορθωτικά μέτρα:	Ύπαρξη συνεχών ενημερώσεων από τα πρόσωπα που έχουν αναλάβει την παρακολούθηση του έργου καθώς και καταγραφή των δραστηριοτήτων τους και των ελέγχων που έχουν πραγματοποιήσει καθ' όλη τη διάρκεια έργου			
Εναλλακτικό σχέδιο:	Συνεχής κατάρτιση των εργαζομένων σε θέματα διαχείρισης έργου και νέων τεχνολογιών με διεξαγωγή σεμιναρίων			
Σχέδιο μετάπτωσης:	Αλλαγή αρμοδιοτήτων			
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 74: Φύλλο κινδύνου #62 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #63				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Λανθασμένες αποφάσεις διαχείρισης κινδύνων			
Σύντομη Περιγραφή:	Έλλειψη εμπειρίας των ατόμων που λαμβάνουν τις αποφάσεις διαχείρισης κινδύνων του έργου με αποτέλεσμα την ανεπαρκή αντιμετώπιση των κινδύνων			
Κατηγορία Κινδύνου:	Ανθρώπινοι			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	4	X_4	89	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Τακτική παρακολούθηση του σχεδιασμού διαχείρισης κινδύνου			
Προπομπός Κινδύνου:	Απόκλιση αποφάσεων από τον αρχικό σχεδιασμό διαχείρισης κινδύνου			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τακτικός έλεγχος των εργαζομένων που έχουν αναλάβει τις αποφάσεις διαχείρισης κινδύνων			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:	Συνεχής κατάρτιση των εργαζομένων σε θέματα διαχείρισης κινδύνων με διεξαγωγή σεμιναρίων.			
Σχέδιο μετάπτωσης:	Αλλαγή αρμοδιοτήτων			
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 75: Φύλλο κινδύνου #63 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #64				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος σεισμού			
Σύντομη Περιγραφή:	Καταστροφή του κτιρίου που στεγάζεται το πληροφοριακό σύστημα λόγω σεισμού			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	3	M_4	44	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος στατικότητας του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα			
Προπομπός Κινδύνου:	Ενδείξεις προβληματικής στατικότητας του κτιρίου			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Συνεχής έλεγχος των κτιριακών εγκαταστάσεων			
Διορθωτικά μέτρα:	Μετεγκατάσταση του εξοπλισμού σε πιο σύγχρονες κτιριακές εγκαταστάσεις			
Εναλλακτικό σχέδιο:	Εγκατάσταση του εξοπλισμού σε χώρο αντισεισμικών προδιαγραφών			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 76: Φύλλο κινδύνου #64 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #65				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Κεραυνού			
Σύντομη Περιγραφή:	Καταστροφή στην ηλεκτροδότηση του κτιρίου λόγω κεραυνού που προκλήθηκε από ακραία καιρικά φαινόμενα			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	60	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των καιρικών φαινομένων			
Προπομπός Κινδύνου:	Έντονες βροχοπτώσεις			
Στρατηγική αντιμετώπισης:	Αποφυγή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Χρήση ειδικού εξοπλισμού για την αποφυγή κεραυνών (αλεξικέραυνο)			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 77: Φύλλο κινδύνου #65 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #66				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος πλημμύρας			
Σύντομη Περιγραφή:	Καταστροφή του χώρου που στεγάζεται το σύστημα λόγω ακραίων καιρικών φαινομένων			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	61	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των καιρικών φαινομένων			
Προπομπός Κινδύνου:	Παρατήρηση πλημμυρικών φαινομένων σε ορισμένα τμήματα του κτιρίου			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Δημιουργία αντιπλημμυρικών έργων στο χώρο εγκατάστασης του εξοπλισμού			
Διορθωτικά μέτρα:	Τοποθέτηση του συστήματος σε σημείο υψηλότερο της επιφάνειας του εδάφους			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 78 : Φύλλο κινδύνου #66 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #67				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος πυρκαγιάς			
Σύντομη Περιγραφή:	Κίνδυνος εκδήλωσης πυρκαγιάς στο χώρο της εγκατάστασης ή σε γειτονικά κτίρια από φυσικά αίτια ή τεχνητά			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	4	Y_4	17	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του χώρου εγκατάστασης ως προς τα μέτρα πυρασφάλειας			
Προπομπός Κινδύνου:	Ελλιπής ή ανύπαρκτη συντήρηση του εξοπλισμού πυρασφάλειας			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Ύπαρξη και συνεχής έλεγχος λειτουργικών πυροσβεστήρων σε όλους τους ορόφους του κτιρίου			
Διορθωτικά μέτρα:	Χρήση εξοπλισμού πυρανίχνευσης			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 79: Φύλλο κινδύνου #67 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #68				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος διαρροής υδάτων			
Σύντομη Περιγραφή:	Καταστροφή του χώρου που στεγάζεται το σύστημα από πλημμύρα που οφείλεται σε διαρροή υδάτων λόγω παλαιότητας ή κακής κατασκευής του δικτύου υδροδότησης			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	4	X_4	90	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του δικτύου υδροδότησης του κτιρίου			
Προπομπός Κινδύνου:	Ελλιπής ή ανύπαρκτη συντήρηση του δικτύου υδροδότησης			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Συνεχής έλεγχος και συντήρηση του δικτύου υδροδότησης			
Διορθωτικά μέτρα:	Μετεγκατάσταση του εξοπλισμού σε πιο σύγχρονες κτιριακές εγκαταστάσεις			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 80: Φύλλο κινδύνου #68 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #69				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση			
Σύντομη Περιγραφή:	Αδυναμία ηλεκτροδότησης μέσω της εγκατάστασης του κτιρίου που στεγάζεται το σύστημα λόγω ελλιπούς υποστήριξης σε περιπτώσεις διακοπής της ηλεκτροδότησης			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	62	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του δικτύου ηλεκτροδότησης του κτιρίου			
Προπομπός Κινδύνου:	Ελλιπής ή ανύπαρκτη συντήρηση του δικτύου ηλεκτροδότησης			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Συνεχής έλεγχος και συντήρηση του συστήματος ηλεκτροδότησης			
Διορθωτικά μέτρα:	Χρήση γεννητριών			
Εναλλακτικό σχέδιο:	Μετεγκατάσταση του εξοπλισμού σε πιο σύγχρονες κτιριακές εγκαταστάσεις			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 81: Φύλλο κινδύνου #69 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #70				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κατολίσθηση – διάβρωση εδάφους			
Σύντομη Περιγραφή:	Καταστροφή κτιρίου που στεγάζεται το πληροφοριακό σύστημα λόγω κατολίσθησης ή διάβρωσης εδάφους.			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	5	X_3	85	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Περιοδικοί έλεγχοι του εδάφους περιμετρικά του κτιρίου όπου βρίσκεται το πληροφοριακό σύστημα			
Προπομπός Κινδύνου:	Εμφάνιση φαινομένων διάβρωσης			
Στρατηγική αντιμετώπισης:	Αποδοχή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Εύρεση νέων κτιριακών εγκαταστάσεων για τη στέγαση του πληροφοριακού συστήματος			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 82: Φύλλο κινδύνου #70 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #71				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ηλιακές εκλάμψεις			
Σύντομη Περιγραφή:	Προβληματική λειτουργία του δικτύου λόγω ηλιακών εκλάμψεων			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	3	X_5	92	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Περιοδικός έλεγχος της σωστής λειτουργίας του δικτύου από ηλεκτρομαγνητικές παρεμβολές			
Προπομπός Κινδύνου:	Μη σωστή λειτουργία του δικτύου λόγω ηλεκτρομαγνητικών παρεμβολών			
Στρατηγική αντιμετώπισης:	Αποδοχή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Αποθήκευσης των δεδομένων και των προγραμμάτων του πληροφοριακού συστήματος σε περιβάλλον cloud			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 83: Φύλλο κινδύνου #71 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #72				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Σκόνη			
Σύντομη Περιγραφή:	Βλάβες ή δυσλειτουργία υλικού λόγω σκόνης			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	2	M_7	73	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Τακτικός έλεγχος της κατάστασης του εξοπλισμού			
Προπομπός Κινδύνου:	Παρατήρηση δυσλειτουργιών λόγω σκόνης			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τακτικός καθαρισμός του χώρου όπου βρίσκεται ο εξοπλισμό του συστήματος			
Διορθωτικά μέτρα:	Τοποθέτηση του εξοπλισμού σε ειδικό χώρο			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εβδομαδιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 84: Φύλλο κινδύνου #72 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #73				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Βλάβη του συστήματος κλιματισμού			
Σύντομη Περιγραφή:	Καταστροφή από υπερθέρμανση του εξοπλισμού του πληροφοριακού συστήματος λόγω βλάβης του κλιματισμού			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	63	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Τακτική παρακολούθηση του συστήματος κλιματισμού			
Προπομπός Κινδύνου:	Παρατήρηση δυσλειτουργιών του συστήματος λόγω υπερθέρμανσης			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τακτικός έλεγχος και συντήρηση του συστήματος κλιματισμού			
Διορθωτικά μέτρα:	Υπαρξη εφεδρικού συστήματος κλιματισμού στους χώρους όπου βρίσκεται ο εξοπλισμός του συστήματος			
Εναλλακτικό σχέδιο:	Αλλαγή του συστήματος κλιματισμού			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 85: Φύλλο κινδύνου #73 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #74				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ηλεκτρομαγνητικές παρεμβολές			
Σύντομη Περιγραφή:	Προβληματική λειτουργία του δικτύου λόγω ηλεκτρομαγνητικών παρεμβολών			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	3	M_8	77	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Περιοδικός έλεγχος της σωστής λειτουργίας του δικτύου από ηλεκτρομαγνητικές παρεμβολές			
Προπομπός Κινδύνου:	Μη σωστή λειτουργία του δικτύου λόγω ηλεκτρομαγνητικών παρεμβολών			
Στρατηγική αντιμετώπισης:	Αποδοχή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Αποθήκευσης των δεδομένων και των προγραμμάτων του πληροφοριακού συστήματος σε περιβάλλον cloud			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 86: Φύλλο κινδύνου #74 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #75				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Στατικός ηλεκτρισμός			
Σύντομη Περιγραφή:	Καταστροφή του εξοπλισμού του πληροφοριακού συστήματος λόγω διαρροής ρεύματος			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	4	X_4	91	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Περιοδικός έλεγχος του κτιρίου που στεγάζεται το πληροφοριακό σύστημα για διαρροή ρεύματος			
Προπομπός Κινδύνου:	Εμφάνιση σημείων του κτιρίου όπου μπορεί να προκληθεί διαρροή ρεύματος - βραχυκύκλωμα			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τακτικός έλεγχος του δικτύου ηλεκτροδότησης όπου στεγάζεται το πληροφοριακό σύστημα			
Διορθωτικά μέτρα:	Ύπαρξη πινάκων ασφαλείας όπου θα διακόπτουν την παροχή ρεύματος σε περίπτωση διαρροής ρεύματος και θα γίνεται η ρευματοδότηση του συστήματος από γεννήτριες			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Μηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 87: Φύλλο κινδύνου #75 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #76				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έκρηξη ηφαιστείου			
Σύντομη Περιγραφή:	Εγκατάσταση του πληροφοριακού συστήματος ή του διακομιστή του πληροφοριακού συστήματος σε περιοχή που είναι επιρρεπής στις ηφαιστειακές εκρήξεις			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	5	X_3	86	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των μετρήσεων που γίνονται από το ηφαιστειολογικό παρατηρητήριο της περιοχής όπου στεγάζεται το πληροφοριακό σύστημα			
Προπομπός Κινδύνου:	Όταν οι μετρήσεις αποκλίνουν από τα επιτρεπτά όρια που έχουν ορισθεί			
Στρατηγική αντιμετώπισης:	Αποφυγή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή που δεν είναι ηφαιστειογενής			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 88: Φύλλο κινδύνου #76 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #77				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Πυρηνικό ατύχημα			
Σύντομη Περιγραφή:	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή όπου βρίσκονται πυρηνικά εργοστάσια			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	5	X_3	87	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των μετρήσεων που γίνονται από τα πυρηνικά εργοστάσια της περιοχής όπου στεγάζεται το πληροφοριακό σύστημα			
Προπομπός Κινδύνου:	Όταν οι μετρήσεις αποκλίνουν από τα επιτρεπτά όρια που έχουν ορισθεί			
Στρατηγική αντιμετώπισης:	Αποφυγή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή όπου δεν υπάρχουν πυρηνικά εργοστάσια			
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 89: Φύλλο κινδύνου #77 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #78				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος εκρήξεων			
Σύντομη Περιγραφή:	Εγκατάσταση του πληροφοριακού συστήματος σε χώρο όπου βρίσκονται εύφλεκτα υλικά			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	5	M_4	51	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος για την ύπαρξη εύφλεκτων υλικών στο χώρο όπου στεγάζεται το πληροφοριακό σύστημα			
Προπομπός Κινδύνου:	Εμφάνιση αποθηκευμένων υλικών που μπορεί να προκαλέσουν εκρήξεις			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Έλεγχος των κτιριακών εγκαταστάσεων και του περιβάλλοντα χώρου για τυχόν εύφλεκτα υλικά όπου μπορεί να προκαλέσουν εκρήξεις και απομάκρυνση αυτών από το χώρο			
Διορθωτικά μέτρα:	Αποθήκευση των δεδομένων του συστήματος και σε άλλους servers σε άλλες περιοχές			
Εναλλακτικό σχέδιο:	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 90: Φύλλο κινδύνου #78 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #79				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Έντομα – τρωκτικά			
Σύντομη Περιγραφή:	Εγκατάσταση του πληροφοριακού συστήματος σε κτίριο όπου δεν έχει την κατάλληλη υποδομή και την απαραίτητη προστασία με αποτέλεσμα να εισβάλλουν στο χώρο διάφορα έντομα και τρωκτικά και να προκαλέσουν ζημιά στο υλικό του συστήματος			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	4	M_2	35	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Τακτικός έλεγχος του κτιρίου για εμφάνιση τρωκτικών			
Προπομπός Κινδύνου:	Εμφάνιση καταστροφών στο υλικό του συστήματος από τρωκτικά			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τακτικός έλεγχος των κτιριακών εγκαταστάσεων και συχνή απολύμανση του χώρου όπου στεγάζεται το πληροφοριακό για τυχόν έντομα και τρωκτικά			
Διορθωτικά μέτρα:	Εγκατάσταση ειδικού εξοπλισμού όπου αποτρέπει τα έντομα και τρωκτικά να εισχωρήσουν στο χώρο			
Εναλλακτικό σχέδιο:	Ύπαρξη εφεδρικού εξοπλισμού σε περίπτωση φθοράς του υπάρχοντος			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εξαμηνιαία			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 91: Φύλλο κινδύνου #79 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #80				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος δονήσεων			
Σύντομη Περιγραφή:	Εγκατάσταση πληροφοριακού συστήματος σε περιοχή κοντά σε σιδηροδρομικό σταθμό ή σε εργοτάξιο			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	64	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα για την ύπαρξη ιδιοτήτων αντικραδασμικής λειτουργίας			
Προπομπός Κινδύνου:	Μη ύπαρξη ιδιοτήτων αντικραδασμικής λειτουργίας			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εγκατάσταση του πληροφοριακού συστήματος σε κτίριο όπου έχει αντικραδασμική λειτουργία			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις όπου βρίσκονται σε περιοχή με μειωμένη κραδασμική δραστηριότητα			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 92: Φύλλο κινδύνου #80 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #81				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Καπνός - Μικροσωματίδια			
Σύντομη Περιγραφή:	Εγκατάσταση πληροφοριακού συστήματος σε σημείο όπου υπάρχουν μεγάλες ποσότητες καπνού και μικροσωματιδίων οι οποίες μπορεί να προκαλέσουν ζημιά στον εξοπλισμό του συστήματος			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	65	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος της καθαρότητας του αέρα			
Προπομπός Κινδύνου:	Εμφάνιση καπνού στο χώρο του πληροφοριακού συστήματος			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τακτικός έλεγχος και συντήρηση του συστήματος εξαερισμού καθώς και τοποθέτηση του εξοπλισμού σε ειδικό χώρο			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις όπου βρίσκονται σε περιοχή με λιγότερο καπνό και ρύπους			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 93: Φύλλο κινδύνου #81 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #82				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Μαγνήτες – μαγνητικά εργαλεία			
Σύντομη Περιγραφή:	Χρήση μαγνητών ή μαγνητικών εργαλείων μπορούν να προκαλέσουν βλάβη σε ευαίσθητο εξοπλισμό ή να διαγράψουν δεδομένα			
Κατηγορία Κινδύνου:	Φυσικοί - Περιβαλλοντικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	5	Y_6	21	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Τακτικός έλεγχος της βάσης δεδομένων και καταμέτρηση των αποθηκευμένων δεδομένων στη βάση			
Προπομπός Κινδύνου:	Απώλεια δεδομένων/μη σωστή αποθήκευση των δεδομένων			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τοποθέτηση πινακίδας απαγόρευσης όπου δεν θα επιτρέπει την είσοδο μαγνητών και μαγνητικών εργαλείων στο χώρο όπου βρίσκονται οι servers του συστήματος			
Διορθωτικά μέτρα:	Τοποθέτηση αισθητήρων ανίχνευσης μαγνητικών εργαλείων στην είσοδο του χώρου όπου βρίσκονται οι servers του συστήματος			
Εναλλακτικό σχέδιο:	Επιβολή ποινών σε όποιον δεν συμμορφώνεται με τους κανονισμούς			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 94: Φύλλο κινδύνου #82 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #83				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Αγωγές – Μηνύσεις			
Σύντομη Περιγραφή:	Παράβλεψη ή καταπάτηση νομοθετικών ρυθμίσεων ή υπάρχουσας νομοθεσίας όσον αφορά τις διαδικασίες μετάδοσης πληροφορίας και τήρησης αρχείων προσωπικών δεδομένων			
Κατηγορία Κινδύνου:	Νομικοί - Κοινωνικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	2	X_6	95	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση ορθής λειτουργίας του συστήματος και αποδοχής του από τα εμπλεκόμενα μέρη			
Προπομπός Κινδύνου:	Ύπαρξη σοβαρών αντιδράσεων			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 95: Φύλλο κινδύνου #83 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #84				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Απώλεια καλής φήμης			
Σύντομη Περιγραφή:	Μη αποτελεσματική λειτουργία του συστήματος λόγω λανθασμένου σχεδιασμού με αποτέλεσμα τη δυσαρέσκεια των τελικών χρηστών του συστήματος			
Κατηγορία Κινδύνου:	Νομικοί - Κοινωνικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	3	X_5	93	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος της αποδοχής και της χρήσης του συστήματος από τα εμπλεκόμενα μέλη			
Προπομπός Κινδύνου:	Μη χρήση της εφαρμογής από τους χρήστες λόγω ύπαρξης λαθών / μη εύχρηστη εφαρμογή για τους τελικούς χρήστες του συστήματος			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 96: Φύλλο κινδύνου #84 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #85				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κλοπή πνευματικής ιδιοκτησίας			
Σύντομη Περιγραφή:	Κλοπή μερών του λογισμικού του πληροφοριακού συστήματος από ανταγωνίστρια εταιρεία το οποίο υπόκειται σε καθεστώς πνευματικής ιδιοκτησίας			
Κατηγορία Κινδύνου:	Νομικοί - Κοινωνικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	2	X_2	79	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των εφαρμογών που χρησιμοποιούν ανταγωνίστριες εταιρείες			
Προπομπός Κινδύνου:	Χρήση εφαρμογής από ανταγωνίστρια εταιρεία με ίδια χαρακτηριστικά			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 97: Φύλλο κινδύνου #85 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #86				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων			
Σύντομη Περιγραφή:	Αλλαγή πολιτικής ηγεσίας με αποτέλεσμα την αλλαγή ή ματαίωση κατασκευής του συστήματος και την ύπαρξη χρονικής καθυστέρησης ή κόστους			
Κατηγορία Κινδύνου:	Πολιτικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	3	X_5	94	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των πολιτικών αποφάσεων και δραστηριοτήτων της κυβέρνησης			
Προπομπός Κινδύνου:	Αποφάσεις μείωσης λειτουργικότητας και περιορισμού χρήσης του πληροφοριακού στο σύστημα υγείας			
Στρατηγική αντιμετώπισης:	Αποδοχή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Συμμετοχή των πολιτικών δυνάμεων στην απόφαση κατασκευής του συστήματος			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 98: Φύλλο κινδύνου #86 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #87				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας			
Σύντομη Περιγραφή:	Εγκατάσταση του πληροφοριακού συστήματος σε περιοχή με πολιτικές αναταραχές / πολέμους			
Κατηγορία Κινδύνου:	Πολιτικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.1	5	X_3	88	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των πολιτικών αποφάσεων και δραστηριοτήτων της κυβέρνησης			
Προπομπός Κινδύνου:	Πολεμικές αναταραχές			
Στρατηγική αντιμετώπισης:	Αποδοχή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Συμμετοχή των πολιτικών δυνάμεων στην απόφαση να μην επηρεαστεί το έργο			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 99: Φύλλο κινδύνου #87 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #88				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κλοπή υλικού			
Σύντομη Περιγραφή:	Εισβολή αγνώστων ατόμων στο κτίριο που στεγάζεται το πληροφοριακό σύστημα με αποτέλεσμα την κλοπή υλικού απαραίτητου για τη σωστή λειτουργία του			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	66	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του εξοπλισμού και επιθεώρηση του χώρου όπου βρίσκεται ο εξοπλισμός σε τακτά χρονικά διαστήματα			
Προπομπός Κινδύνου:	Μη ταύτιση καταγεγραμμένου και υπάρχοντος εξοπλισμού			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εγκατάσταση καμερών στους χώρους όπου βρίσκεται ο εξοπλισμός			
Διορθωτικά μέτρα:	Συνεχής παρακολούθηση του χώρου όλο το 24ώρο			
Εναλλακτικό σχέδιο:	Ύπαρξη εφεδρικού εξοπλισμού			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε 2 μήνες			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 100: Φύλλο κινδύνου #88 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #89				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Βανδαλισμοί			
Σύντομη Περιγραφή:	Καταστροφή του εξοπλισμού από βανδαλισμούς αγνώστων ατόμων			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	67	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος των κτιριακών εγκαταστάσεων όπου στεγάζεται το πληροφοριακό σύστημα καθώς και του εξοπλισμού του πληροφοριακού συστήματος			
Προπομπός Κινδύνου:	Καταστροφή του κτιρίου και του εξοπλισμού			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εγκατάσταση καμερών και συνεχή παρακολούθηση των εισόδων του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα			
Διορθωτικά μέτρα:	Έλεγχος των ατόμων που εισέρχονται στο κτίριο επιδεικνύοντας κάποιο αποδεικτικό στοιχείο (π.χ. ΑΔΤ)			
Εναλλακτικό σχέδιο:	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 101: Φύλλο κινδύνου #89 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #90				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Εισβολείς (Hackers) – Υποκλοπή δεδομένων			
Σύντομη Περιγραφή:	Προσβολή του συστήματος από την επιδρομή hackers με αποτέλεσμα την ύπαρξη κινδύνου υποκλοπής μεταδιδόμενων πληροφοριών			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	5	Y_3	5	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του λογισμικού ασφαλείας			
Προπομπός Κινδύνου:	Υποκλοπή μεταδιδόμενων πληροφοριών			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 102: Φύλλο κινδύνου #90 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #91				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Εισβολείς (Hackers) – Καταστροφή δεδομένων			
Σύντομη Περιγραφή:	Προσβολή του συστήματος από την επιδρομή hackers με αποτέλεσμα την ύπαρξη κινδύνου καταστροφής δεδομένων			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.7	5	Y_3	6	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του λογισμικού ασφαλείας			
Προπομπός Κινδύνου:	Καταστροφή/ διαγραφή δεδομένων			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 103: Φύλλο κινδύνου #91 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #92				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού)			
Σύντομη Περιγραφή:	Προσβολή του συστήματος από ηλεκτρονικούς εγκληματίες με αποτέλεσμα την αλλοίωση ή καταστροφή των αποθηκευμένων δεδομένων του συστήματος			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.9	5	Y_1	2	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του λογισμικού ασφαλείας			
Προπομπός Κινδύνου:	Μετάδοση κακόβουλου λογισμικού			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 104: Φύλλο κινδύνου #92 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #93				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές			
Σύντομη Περιγραφή:	Αντιγραφή μερών ή ολόκληρου του σχεδιασμού του πληροφοριακού συστήματος από πρώην εργαζόμενους			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.5	3	M_4	45	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Παρακολούθηση των εφαρμογών που χρησιμοποιούν ανταγωνίστριες εταιρείες			
Προπομπός Κινδύνου:	Χρήση εφαρμογής από ανταγωνίστρια εταιρεία με ίδια χαρακτηριστικά			
Στρατηγική αντιμετώπισης:	Αποδοχή			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:	Όρος στο συμβόλαιο με τον εργαζόμενο για τη μη γνωστοποίηση σε τρίτους των εφαρμογών που κατασκευάζονται στην εταιρεία			
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Εφόσον προκύψει			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 105: Φύλλο κινδύνου #93 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #94				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κατασκοπεία			
Σύντομη Περιγραφή:	Υποκλοπή ευαίσθητων προσωπικών δεδομένων του πληθυσμού από εχθρικά κράτη			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	68	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του λογισμικού ασφαλείας			
Προπομπός Κινδύνου:	Υποκλοπή ευαίσθητων προσωπικών δεδομένων			
Στρατηγική αντιμετώπισης:	Μεταφορά			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:				
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:	Όρος στο συμβόλαιο με την εταιρεία ανάθεσης του έργου			
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 106: Φύλλο κινδύνου #94 συστήματος E-Prescription

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ #95				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Τρομοκρατικές ενέργειες			
Σύντομη Περιγραφή:	Καταστροφή των εγκαταστάσεων που στεγάζεται το πληροφοριακό σύστημα λόγω τρομοκρατικών επιθέσεων σε διπλανό κτίριο ή και στο ίδιο κτίριο.			
Κατηγορία Κινδύνου:	Εξωτερικοί			
Ημερομηνία αναγνώρισης:	23/10/2013			
Υπεύθυνος:	Κυρίτση Β.			
Ανάλυση Κινδύνου				
Πιθανότητα εμφάνισης	**Συνέπεια/ Επίπτωση**	**Έκθεση**	**Προτεραιότητα**	**Ημερομηνία ενημέρωσης**
0.3	4	M_6	69	26/10/2013
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος του χώρου εγκατάστασης του πληροφοριακού συστήματος και της συμπεριφοράς των εργαζομένων			
Προπομπός Κινδύνου:	Ύποπτες ενέργειες των εργαζομένων/ εύρεση ύποπτου εξοπλισμού στο χώρο			
Στρατηγική αντιμετώπισης:	Μετριασμός			
Ημερομηνία ενημέρωσης:	27/10/2013			
(Προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Συνεχής έλεγχος των εγκαταστάσεων όπου βρίσκεται ο εξοπλισμός για τυχόν εύρεση ύποπτων αντικειμένων εντός και εκτός του χώρου καθώς και ύποπτων συμπεριφορών των εργαζομένων			
Διορθωτικά μέτρα:	Χρήση ειδικού εξοπλισμού ανίχνευσης μετάλλων στην είσοδο του κτιρίου			
Εναλλακτικό σχέδιο:	Μετεγκατάσταση του εξοπλισμού σε άλλες κτιριακές εγκαταστάσεις			
Σχέδιο μετάπτωσης:				
Σχέδιο αποφυγής:				
Σχέδιο μεταφοράς:				
Σχέδιο αποδοχής:				
Παρακολούθηση κινδύνου				
Παρακολούθηση:	Κάθε μέρα			
Κατάσταση:	Ανοιχτή			
Ημερομηνία Κλεισίματος:				
Ημερομηνία Ελέγχου:	31/10/2013			

Πίνακας 107: Φύλλο κινδύνου #95 συστήματος E-Prescription

Εκτός από τα φύλλα κινδύνων, πρέπει να υπάρχει και μία συγκεντρωτική αναφορά των κινδύνων που θα ενημερώνει περιληπτικά τη Διοίκηση για την κατάσταση του κάθε κινδύνου.

# Φύλλο Κινδύνου	Όνομα Κινδύνου	Έκθεση κινδύνου	Κατάσταση Κινδύνου	Ημερομηνία τελευταίας Ενημέρωσης	Υπεύθυνος
1	Ασυμβατότητα λογισμικού με τις απαιτήσεις	X_3	Τελειωμένη	31/10/2013	Κυρίτση Β.
2	Εξάντληση πόρων του συστήματος	Y_6	Ανοιχτή	31/10/2013	Κυρίτση Β.
3	Λανθασμένη βάση δεδομένων αποθήκευσης των στοιχείων	X_3	Τελειωμένη	31/10/2013	Κυρίτση Β.
4	Ελλιπής ασφάλεια των προσωπικών δεδομένων των πολιτών	Y_1	Ανοιχτή	31/10/2013	Κυρίτση Β.
5	Δυσκολία σε αναβάθμιση – συντήρηση λογισμικού	M_6	Ανοιχτή	31/10/2013	Κυρίτση Β.
6	Έλλειψη διασυνδεσιμότητας των φορέων μέσω του συστήματος	M_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
7	Λανθασμένος σχεδιασμός υλικού (αρχιτεκτονική συστήματος)	X_3	Τελειωμένη	31/10/2013	Κυρίτση Β.
8	Λανθασμένος σχεδιασμός λογισμικού (αρχιτεκτονική συστήματος)	X_3	Τελειωμένη	31/10/2013	Κυρίτση Β.
9	Ασυμβατότητα της τεχνολογίας του λογισμικού με τις υπάρχουσες κρατικές υποδομές ροής πληροφοριών	M_4	Κλειστή	31/10/2013	Κυρίτση Β.
10	Χρήση νέων και μη δοκιμασμένων τεχνολογιών ανάπτυξης λογισμικού	M_4	Τελειωμένη	31/10/2013	Κυρίτση Β.
11	Μη αποδεκτή ποιότητα λογισμικού	M_4	Τελειωμένη	31/10/2013	Κυρίτση Β.
12	Ελλιπείς μηχανισμοί ελέγχου ασφάλειας του πληροφοριακού συστήματος	X_3	Ανοιχτή	31/10/2013	Κυρίτση Β.
13	Αδυναμία Σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου	M_2	Ανοιχτή	31/10/2013	Κυρίτση Β.
14	Ανεπαρκής προστασία κρυπτογραφικών κλειδιών	M_6	Ανοιχτή	31/10/2013	Κυρίτση Β.
15	Ελλιπής επικύρωση της επεξεργασίας των δεδομένων	M_6	Τελειωμένη	31/10/2013	Κυρίτση Β.
16	Δυσλειτουργία του υλικού	M_2	Κλειστή	31/10/2013	Κυρίτση Β.
17	Ανεπαρκής έλεγχός του λογισμικού	M_2	Κλειστή	31/10/2013	Κυρίτση Β.
18	Σφάλματα λογισμικού	Y_6	Κλειστή	31/10/2013	Κυρίτση Β.
19	Πολυπλοκότητα λογισμικού	M_4	Κλειστή	31/10/2013	Κυρίτση Β.
20	Μη ασφαλής αρχιτεκτονική δικτύου	M_2	Τελειωμένη	31/10/2013	Κυρίτση Β.
21	Προβλήματα επικοινωνίας με την εταιρεία ανάθεσης έργου	M_7	Κλειστή	31/10/2013	Κυρίτση Β.
22	Μη επαρκώς καθορισμένοι όροι του συμβολαίου μεταξύ του κράτους και του αναδόχου	M_7	Τελειωμένη	31/10/2013	Κυρίτση Β.
23	Μη διαθεσιμότητα ομάδας υποστήριξης του συστήματος	M_2	Τελειωμένη	31/10/2013	Κυρίτση Β.
24	Έλλειψη συνεργασίας μεταξύ των ομάδων κατασκευής του έργου.	M_4	Κλειστή	31/10/2013	Κυρίτση Β.
25	Ελλιπής φύλαξη του κτιρίου όπου στεγάζεται το πληροφοριακό σύστημα από εξειδικευμένα άτομα(φύλακες)	M_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
26	Ελλιπής χρόνος προσαρμογής χρήσης του νέου πληροφοριακού συστήματος	M_5	Κλειστή	31/10/2013	Κυρίτση Β.
27	Ανεπαρκής ή λανθασμένος διαχωρισμός των καθηκόντων	M_1	Κλειστή	31/10/2013	Κυρίτση Β.
28	Ανεπαρκής επίβλεψη των εργαζομένων	M_2	Ανοιχτή	31/10/2013	Κυρίτση Β.
29	Ελλιπής διαδικασία για την αφαίρεση των δικαιωμάτων πρόσβασης κατά τη λήξη της απασχόλησης	M_6	Τελειωμένη	31/10/2013	Κυρίτση Β.

30	Ελλιπής σχεδιασμός τακτικών ελέγχων εύρυθμης λειτουργίας του λογισμικού	M_1	Τελειωμένη	31/10/2013	Κυρίτση Β.
31	Κίνδυνος εσφαλμένης εγκατάστασης υλικού ή λογισμικού από το προσωπικό της αναδόχου εταιρείας	Y_6	Τελειωμένη	31/10/2013	Κυρίτση Β.
32	Ανεπαρκής κάλυψη του κτιρίου από σύστημα συναγερμού	Y_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
33	Ανεπαρκής κάλυψη του κτιρίου από σύστημα πυρανίχνευσης	Y_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
34	Ανεπαρκής κάλυψη του κτιρίου από σύστημα αναγνώρισης και ελέγχου ταυτότητας	Y_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
35	Έλλειψη οικονομικών πόρων	M_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
36	Προβλήματα με την χρηματοδότηση του έργου	M_5	Ανοιχτή	31/10/2013	Κυρίτση Β.
37	Καταστροφή υλικού ή λογισμικού από τους χειριστές του συστήματος λόγω κακής χρήσης του	Y_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
38	Κλοπή υλικού από εργαζομένους	Y_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
39	Απεργίες εργαζομένων που διαχειρίζονται το πληροφοριακό σύστημα	M_2	Κλειστή	31/10/2013	Κυρίτση Β.
40	Κίνδυνος απροθυμίας προσαρμογής στην αλλαγή	Y_4	Κλειστή	31/10/2013	Κυρίτση Β.
41	Καταστροφή εξοπλισμού από υγρά/τρόφιμα	M_2	Ανοιχτή	31/10/2013	Κυρίτση Β.
42	Διαρροή πληροφοριών	Y_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
43	Μη εξουσιοδοτημένη πρόσβαση στους χώρους του πληροφοριακού συστήματος	Y_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
44	Μη εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα από τους εργαζόμενους	Y_3	Ανοιχτή	31/10/2013	Κυρίτση Β.
45	Διαρροή κωδικών εισόδου και διαχείρισης του πληροφοριακού συστήματος	Y_3	Ανοιχτή	31/10/2013	Κυρίτση Β.
46	Μη εξουσιοδοτημένες αλλαγές αρχείων	M_4	Τελειωμένη	31/10/2013	Κυρίτση Β.
47	Ακούσια αλλαγή των δεδομένων του πληροφοριακού συστήματος	M_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
48	Έλλειψη κινήτρων για τους εργαζόμενους	M_2	Ανοιχτή	31/10/2013	Κυρίτση Β.
49	Έλλειψη ευαισθητοποίησης σε θέματα ασφάλειας	Y_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
50	Σύνδεση προσωπικών συσκευών στο εταιρικό δίκτυο	Y_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
51	Εγκατάσταση μη εξουσιοδοτημένου λογισμικού κι εφαρμογών	M_4	Τελειωμένη	31/10/2013	Κυρίτση Β.
52	Ακούσια μεταφορά εμπιστευτικών δεδομένων του πληροφοριακού συστήματος εκτός γραφείου	M_2	Ανοιχτή	31/10/2013	Κυρίτση Β.
53	Έλλειψη της απαιτούμενης εκπαίδευσης του προσωπικού	X_1	Ανοιχτή	31/10/2013	Κυρίτση Β.
54	Εσωτερικοί κίνδυνοι (δόλος)	M_8	Ανοιχτή	31/10/2013	Κυρίτση Β.
55	Λάθος κατανομή του κεφαλαίου	M_8	Τελειωμένη	31/10/2013	Κυρίτση Β.
56	Λανθασμένη κατανομή σημαντικότητας στις εφαρμογές του συστήματος	M_6	Τελειωμένη	31/10/2013	Κυρίτση Β.
57	Έλλειψη εφεδρικού σχεδίου απρόσκοπτης λειτουργίας του συστήματος	M_2	Τελειωμένη	31/10/2013	Κυρίτση Β.
58	Λανθασμένη πρόβλεψη απαιτούμενων πόρων υλικού	M_4	Τελειωμένη	31/10/2013	Κυρίτση Β.
59	Αλλαγή του χρονοδιαγράμματος λόγω λανθασμένου αρχικού προγραμματισμού	M_7	Ανοιχτή	31/10/2013	Κυρίτση Β.
60	Λανθασμένη κοστολόγηση του έργου	M_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
61	Κοινή χρήση εμπιστευτικών δεδομένων με τους συνεργάτες και τους προμηθευτές	M_8	Ανοιχτή	31/10/2013	Κυρίτση Β.
62	Έλλειψη εμπειρίας και τεχνογνωσίας των προσώπων που είναι υπεύθυνα για την παρακολούθηση της υλοποίησης του έργου	M_6	Ανοιχτή	31/10/2013	Κυρίτση Β.

63	Λανθασμένες αποφάσεις διαχείρισης κινδύνων	X_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
64	Κίνδυνος σεισμού	M_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
65	Κίνδυνος Κεραυνού	M_6	Ανοιχτή	31/10/2013	Κυρίτση Β.
66	Κίνδυνος πλημμύρας	M_6	Ανοιχτή	31/10/2013	Κυρίτση Β.
67	Κίνδυνος πυρκαγιάς	Y_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
68	Κίνδυνος διαρροής υδάτων	X_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
69	Κίνδυνος αδυναμίας ηλεκτροδότησης του συστήματος λόγω ελλείψεων στην ηλεκτρολογική εγκατάσταση	M_6	Ανοιχτή	31/10/2013	Κυρίτση Β.
70	Κατολίσθηση/ διάβρωση εδάφους	X_3	Ανοιχτή	31/10/2013	Κυρίτση Β.
71	Ηλιακές εκλάμψεις	X_5	Ανοιχτή	31/10/2013	Κυρίτση Β.
72	Σκόνη	M_7	Ανοιχτή	31/10/2013	Κυρίτση Β.
73	Βλάβη του συστήματος κλιματισμού	M_6	Ανοιχτή	31/10/2013	Κυρίτση Β.
74	Ηλεκτρομαγνητικές παρεμβολές	M_8	Ανοιχτή	31/10/2013	Κυρίτση Β.
75	Στατικός ηλεκτρισμός	X_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
76	Έκρηξη ηφαιστείου	X_3	Ανοιχτή	31/10/2013	Κυρίτση Β.
77	Πυρηνικό ατύχημα	X_3	Ανοιχτή	31/10/2013	Κυρίτση Β.
78	Κίνδυνος εκρήξεων	M_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
79	Έντομα/τρωκτικά	M_2	Ανοιχτή	31/10/2013	Κυρίτση Β.
80	Κίνδυνος δονήσεων	M_6	Ανοιχτή	31/10/2013	Κυρίτση Β.
81	Καπνός/ μικροσωματίδια	M_6	Ανοιχτή	31/10/2013	Κυρίτση Β.
82	Μαγνήτες/μαγνητικά εργαλεία	Y_6	Ανοιχτή	31/10/2013	Κυρίτση Β.
83	Αγωγές – Μηνύσεις	X_6	Ανοιχτή	31/10/2013	Κυρίτση Β.
84	Απώλεια καλής φήμης	X_5	Ανοιχτή	31/10/2013	Κυρίτση Β.
85	Κλοπή πνευματικής ιδιοκτησίας	X_2	Ανοιχτή	31/10/2013	Κυρίτση Β.
86	Αλλαγή σχεδιασμού συστήματος ή ματαίωση κατασκευής του λόγω πολιτικών αποφάσεων	X_5	Ανοιχτή	31/10/2013	Κυρίτση Β.
87	Κίνδυνος καταστροφής του πληροφοριακού συστήματος λόγω πολιτικής αστάθειας	X_3	Ανοιχτή	31/10/2013	Κυρίτση Β.
88	Κλοπή υλικού	M_6	Ανοιχτή	31/10/2013	Κυρίτση Β.
89	Βανδαλισμοί	M_6	Ανοιχτή	31/10/2013	Κυρίτση Β.
90	Εισβολείς (Hackers)- Υποκλοπή δεδομένων	Y_3	Ανοιχτή	31/10/2013	Κυρίτση Β.
91	Εισβολείς (Hackers)- Καταστροφή δεδομένων	Y_3	Ανοιχτή	31/10/2013	Κυρίτση Β.
92	Ηλεκτρονικοί Εγκληματίες(Μετάδοση κακόβουλου λογισμικού)	Y_1	Ανοιχτή	31/10/2013	Κυρίτση Β.
93	Πρώην εργαζόμενοι που εργάζονται για ανταγωνιστές	M_4	Ανοιχτή	31/10/2013	Κυρίτση Β.
94	Κατασκοπεία	M_6	Ανοιχτή	31/10/2013	Κυρίτση Β.
95	Τρομοκρατικές ενέργειες	M_6	Ανοιχτή	31/10/2013	Κυρίτση Β.

Πίνακας 108: Μητρώο κινδύνων–Παρακολούθηση κινδύνων συστήματος E-Prescription

ΚΕΦΑΛΑΙΟ 7

Συμπεράσματα

Σύμφωνα με όλα τα παραπάνω έγινε σαφής η αξία και η επιτακτικότητα της εφαρμογής των διαδικασιών διαχείρισης κινδύνων σε μεγάλα πληροφοριακά έργα. Όσο μεγαλύτερο είναι το κόστος των έργων αυτών, η πολυπλοκότητά τους και η αξία τους για τη λειτουργία ενός οργανισμού τόσο σημαντικότερο εργαλείο για την εξασφάλιση της επιτυχημένης υλοποίησης τους αποτελεί η διαχείριση κινδύνων. Μέσα από αυτή μπορούν να προβλεφθούν τα προβλήματα που ενδέχεται να εμφανιστούν κατά την πορεία υλοποίησης του έργου και να προκαλέσουν σημαντικές απώλειες είτε από πλευράς κόστους, είτε από πλευράς χρόνου ολοκλήρωσης των εργασιών, είτε στην ποιότητα και την αξιοπιστία του. Η ευθύνη της διαχείρισης κινδύνων δεν τελειώνει εδώ καθώς καλείται να παρουσιάσει και τον τρόπο με τον οποίο θα μειωθεί η έκθεση του έργου στον κάθε κίνδυνο, να παρακολουθεί την εφαρμογή των μέτρων που συνέστησε αλλά και τον κίνδυνο που απομένει και μετά την εφαρμογή των μέτρων αυτών.

Η διαχείριση κινδύνων είναι μια αυστηρά δομημένη διαδικασία της οποίας τα βήματα θα πρέπει να εκτελούνται με επιμέλεια και σύνεση, καθώς μόνο έτσι θα καταφέρει να επιτύχει τους στόχους της.

Στην παρούσα εργασία εξετάστηκε η εφαρμογή της διαδικασίας διαχείρισης κινδύνων στο έργο: «Ηλεκτρονική Συνταγογράφηση». Αφού πραγματοποιήθηκε η ανάλυση του έργου και καθορίστηκαν οι στόχοι του, εισήχθησαν οι κίνδυνοι που μπορεί να επηρεάσουν την ποιότητα, την αξιοπιστία, το κόστος και το χρονοδιάγραμμα του έργου. Στη συνέχεια πραγματοποιήθηκε ποιοτική ανάλυση των κινδύνων αυτών και παρουσιάστηκαν κάποιες μετρήσεις όσον αφορά την πιθανότητα εμφάνισης των κινδύνων, το επίπεδο των επιπτώσεων τους και το συνολικό επίπεδο έκθεσης σε κάθε κίνδυνο. Από τα αποτελέσματα που εξήχθησαν έγινε αντιληπτό ποιοι κίνδυνοι μπορεί να επηρεάσουν το έργο. Γι' αυτό το λόγο, προτάθηκαν και τρόποι αντιμετώπισης των κινδύνων αυτών.

Πιο συγκεκριμένα :

- Οι περισσότεροι κίνδυνοι ανήκουν στην κατηγορία των τεχνολογικών κινδύνων εφόσον πρόκειται για έργο πληροφορικής.
- Σύμφωνα με την έκθεση των κινδύνων σημαντικότεροι θεωρούνται οι κίνδυνοι που είναι σχετικοί με την ασφάλεια προσωπικών δεδομένων.
- Λόγω της φύσης του έργου η συνήθης στρατηγική αντιμετώπισης είναι η μεταφορά.
- Όσον αφορά την κατάσταση του κάθε κινδύνου οι περισσότεροι κίνδυνοι έχουν κατάσταση ανοιχτή με δεδομένο ότι δεν έχουν εμφανιστεί.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1) A guide to the project management body of knowledge (PMBOK GUIDE) Fourth Edition
2) Πάγκαλος, Γ. (2012). *Ηλεκτρονική συνταγογράφηση: Διεθνής εμπειρία και αξιοποίηση στην Ελλάδα.* Ανάκτηση 2013 από http://www.hl7.org.gr/sites/default/files/pagalos-hl7-esdy-2012.pdf
3) Πάγκαλος, Γ. (2011). *Ηλεκτρονική συνταγογράφηση.* Ανάκτηση 2013 από http://www.ictplus.gr/files/1_TELECOM_STRATEGIES/PANGALOS_GIORGOS_HDIKA_270711.pdf
4) Ασημακόπουλος, Α. (2011). *Ηλεκτρονική Συνταγογράφηση Προβλήματα & Αποτελέσματα.* Ανάκτηση 2013 από http://www.e-prescription.gr
5) *Threats & Vulnerabilities.* Ανάκτηση 2013 από http://www.infosecpedia.info/threats-vulnerabilities
6) *Information Tecchnology Threats and Vulnerabilities.* Ανάκτηση 2013 από http://www.hq.nasa.gov/security/it_threats_vulnerabilities.htm
7) *The Big List of Information Security Threats.* Ανάκτηση 2013 από *http://simplicable.com/new/the-big-list-of-information-security-threats*
8) *Ηλεκτρονική καταχώρηση και εκτέλεση συνταγών.* Ανάκτηση 2013 από http://www.e-prescription.gr
9) Stoneburner, G., Goguen A. & Feringa, A. (2002).*Risk Management Guide for Information Tecnology Systems*. Ανάκτηση 2013 από http://dl.acm.org/citation.cfm?id=2206240
10) Wallumer, E. *Risk Management for It and Software Projects.* Ανάκτηση 2013 από http://www.itq.ch/pdf/RM_ITProjekteV211.pdf
11) Kyriazoglou, J., Kyriazoglou, C., Sygkouna, I. (2007). *Πρότυπο Διαχείρισης Κινδύνου.* Ανάκτηση 2013 από http://www.theirm.org/media/886331/Risk_Management_Standard_Greek_000.pdf