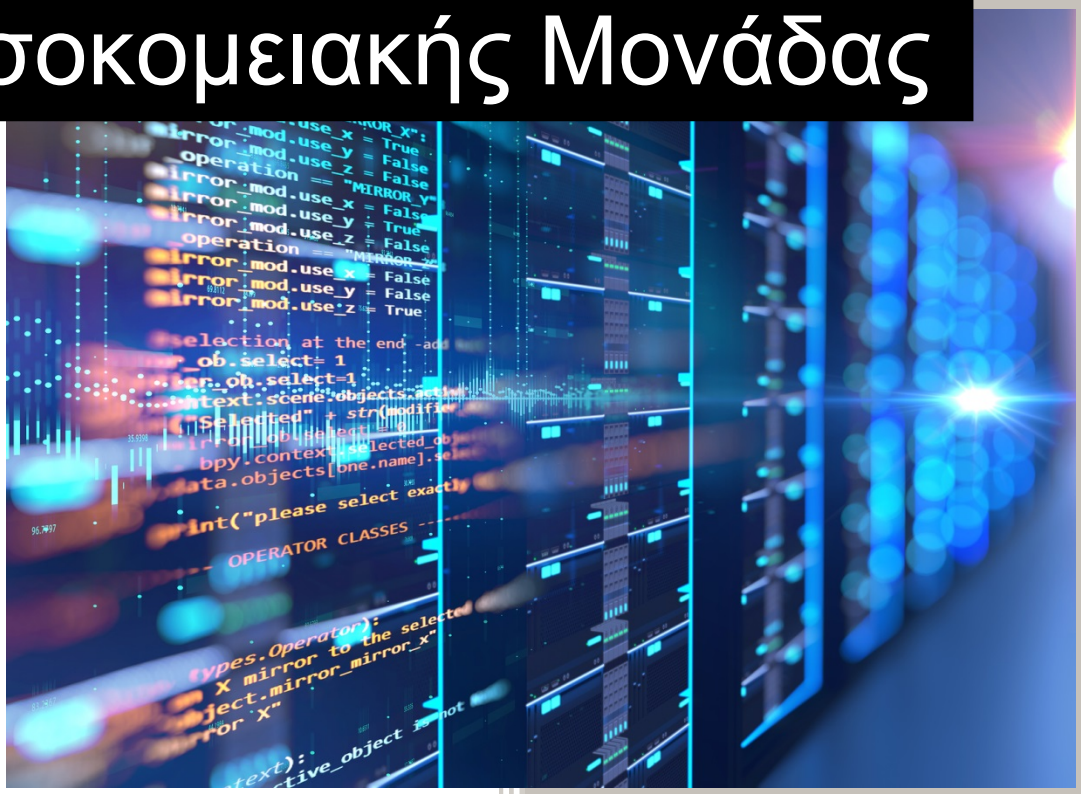
2020

Σχέδιο Έκτακτης Ανάγκης για τα Πληροφοριακά Συστήματα μίας Νοσοκομειακής Μονάδας



MTE1709

Κρίτων Δανόπουλος

Επιβλέπων Καθηγητής:

Κωνσταντίνος Λαμπρινουδάκης

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Περιεχόμενα

1. Εισαγωγή

Η επίτευξη των στόχων ενός οργανισμού εξαρτάται σε μεγάλο βαθμό από τη δυνατότητά του να διασφαλίσει τις υποδομές που είναι απαραίτητες για την αποτελεσματική λειτουργία του. Στους σύγχρονους οργανισμούς οι Τεχνολογίες Πληροφορικής και Επικοινωνιών *(Information and Communication Technologies)* αξιοποιούνται τόσο για την υποστήριξη των ενδοεπιχειρησιακών λειτουργιών, όσο και για την προσφορά υπηρεσιών. Με βάση αυτή τη διαπίστωση προκύπτει ότι τα Πληροφοριακά Συστήματα ενός οργανισμού αποτελούν κρίσιμα στοιχεία της υποδομής του και η αποτελεσματική λειτουργία τους συνδέεται άρρηκτα με την αποτελεσματική λειτουργία του ίδιου του οργανισμού.

Στο πλαίσιο της λειτουργίας μίας Νοσοκομειακής Μονάδας υπάρχει σημαντική ανάγκη διασφάλισης των ΠΣ, ανάγκη η οποία προκύπτει από:

- τις ***νομικές και κανονιστικές*** απαιτήσεις για προστασία ευαίσθητων προσωπικών δεδομένων,
- την ποικιλία και ένταση των ***κινδύνων*** που αντιμετωπίζουν τα σύγχρονα ΠΣ,
- το σημαντικό ***κόστος*** από τυχόν σκόπιμες παραβιάσεις της ασφάλειας ΠΣ και των ακούσιων, τυχαίων και φυσικών γεγονότων που απειλούν ένα σύγχρονο ΠΣ.

Το κοινωνικό ενδιαφέρον για την προστασία των προσωπικών δεδομένων έχει αποτυπωθεί στη σχετική Ευρωπαϊκή και εθνική νομοθεσία και έχει οδηγήσει στη θεσμοθέτηση διοικητικών αρχών προστασίας προσωπικών δεδομένων. Μάλιστα, στην περίπτωση της Ελλάδας, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει κατοχυρωθεί και συνταγματικά ως ανεξάρτητη διοικητική αρχή.

Από τον Μάϊο του 2018 τέθηκε σε λειτουργία και ο νέος Ευρωπαϊκός Κανονισμός Γενικής Προστασίας Δεδομένων (GDPR) κατά τον οποίο οποιαδήποτε μη συμμόρφωση μπορεί να επιφέρει διοικητικά πρόστιμα - κυρώσεις, τα οποία δύνανται να ανέλθουν στα 20 εκατομμύρια ευρώ ή, σε περίπτωση επιχειρήσεων, στο 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους.

Επιπλέον, μία Νοσοκομειακή Μονάδα δραστηριοποιείται σε έναν ιδιαίτερα ευαίσθητο τομέα, τον τομέα της υγείας. Η εμπιστοσύνη του κοινωνικού συνόλου αποτελεί θεμελιώδη προϋπόθεση για την αποτελεσματική λειτουργία της ΝΜ και την παροχή υπηρεσιών υγείας υψηλού επιπέδου.

Η ασφάλεια ενός ΠΣ χαρακτηρίζεται από το πλήθος και την ποικιλομορφία των παραγόντων που πρέπει να ληφθούν υπόψη. Οι παράγοντες αυτοί είναι τόσο τεχνικοί, όσο και διοικητικοί-οργανωτικοί. Για το λόγο αυτό, κάθε προσπάθεια προστασίας ενός ΠΣ θα πρέπει να λαμβάνει υπόψη τις εξής γενικές διαπιστώσεις:

- Η ασφάλεια των ΠΣ εξαρτάται από πολλούς παράγοντες, τεχνικούς, οργανωτικούς και διοικητικούς, κατά συνέπεια πρέπει να αντιμετωπίζεται ανάλογα και όχι ως αμιγώς τεχνικό ζήτημα.
- Η επίτευξη απόλυτης ασφάλειας, για ανοικτά συστήματα όπως είναι τα πληροφοριακά συστήματα, δεν είναι εφικτός στόχος.
- Για κάθε επίπεδο ασφάλειας υπάρχει ένα αντίστοιχο κόστος που θα πρέπει να καταβληθεί για την επίτευξή του.
- Στο πλαίσιο της γενικής *αρχής της αναλογικότητας*, τα μέτρα προστασίας που θα ληφθούν θα πρέπει να αντιστοιχούν στο επίπεδο και τη φύση των πραγματικών κινδύνων που αντιμετωπίζει το ΠΣ.

1.1. Πλαίσιο

Το παρόν κείμενο αποσκοπεί στην ανάπτυξη και τεκμηρίωση του Σχεδίου Αντιμετώπισης Έκτακτων Αναγκών των Πληροφοριακών Συστημάτων (ΠΣ) μίας νοσοκομειακής μονάδας, από την οποία έχουμε ήδη έτοιμο το Σχέδιο Ασφαλείας της το οποίο συμπεριλαμβάνει την αποτίμηση των αγαθών καθώς και την εκτίμηση την επικινδυνότητας. Το παρόν σχέδιο περιλαμβάνει μόνο τις διαδικασίες αποκατάστασης της λειτουργίας των ΠΣ του νοσοκομείου έπειτα από ενδεχόμενη καταστροφή, καθώς και τις προπαρασκευαστικές ενέργειες που απαιτούνται. Στις τελευταίες εντάσσεται και το Σχέδιο Λήψης και Διαχείρισης Εφεδρικών Αντιγράφων *(backup plan)*.

Η ανάπτυξη του Σχεδίου Αντιμετώπισης Έκτακτων Αναγκών στηρίχθηκε στην ανάλυση των πιθανών επιπτώσεων από τη διακοπή της λειτουργίας των ΠΣ του Νοσοκομείου, ή των επιμέρους υποσυστημάτων τους. Με βάση αυτή την υπόθεση προσδιορίστηκαν οι στόχοι του Σχεδίου. Σύμφωνα με την ανάλυση επιπτώσεων, τα πλέον σημαντικά συστήματα, κατά σειρά προτεραιότητας, είναι:

- Οι ***εφαρμογές του Διαχειριστικού Πληροφοριακού Συστήματος Νοσοκομείου*** (ΔΠΣΝ) που χρησιμοποιούνται στο νοσοκομείο. Στις εφαρμογές αυτές περιλαμβάνονται οι εφαρμογές του Τμήματος Εισαγωγής Ασθενών, του Φαρμακείου, του Γραφείου Υλικού, του Λογιστηρίου, του Τμήματος Διατροφής, της Γραμματείας Εξωτερικών Ιατρείων, του Γραφείου Νοσηλίων, του Γραφείου Ιματισμού, και του Γραφείου Υγειονομικού Υλικού. Οι εφαρμογές αυτές εξυπηρετούνται από τον κεντρικό εξυπηρετητή που στεγάζεται στο χώρο του Τμήματος Πληροφορικής και Οργάνωσης.
- Το ***Σύστημα της Αιμοδοσίας***, το οποίο περιλαμβάνει την εφαρμογή i_blood, λειτουργεί σε κλειστό ανεξάρτητο δίκτυο μέσα στο δίκτυο του νοσοκομείου και υποστηρίζεται από έναν εξυπηρετητή και σταθμούς εργασίας που στεγάζονται στο χώρο του Σταθμού Αιμοδοσίας.
- Το ***Σύστημα της Μισθοδοσίας***, το οποίο περιλαμβάνει την αντίστοιχη εφαρμογή και τέσσερις σταθμούς εργασίας που βρίσκονται όλοι στο τμήμα Μισθοδοσίας.

- Τα ***δεδομένα της Διεύθυνσης Προσωπικού***, τα οποία αποθηκεύονται στους προσωπικούς υπολογιστές της Διεύθυνσης.
- Τα ***δεδομένα του Γραφείου Προμηθειών***, τα οποία αποθηκεύονται στους προσωπικούς υπολογιστές του Γραφείου.
- Το ***Σύστημα του Πρωτοκόλλου***, με την αντίστοιχη εφαρμογή Πρωτοκόλλου, για το οποίο υπάρχει ανεξάρτητος εξυπηρετητής που συνδέεται με το εσωτερικό δίκτυο του νοσοκομείου καθώς και δύο σταθμοί εργασίας για τους χρήστες.

Για τα παραπάνω συστήματα έχει τεθεί στόχος αποκατάστασης της λειτουργίας τους το χρονικό διάστημα των ***δύο εβδομάδων***. Σε αυτό το διάστημα περιλαμβάνεται και ο χρόνος που απαιτείται για την προμήθεια του εξοπλισμού που έχει καταστραφεί, δεν περιλαμβάνεται, όμως, ο χρόνος που απαιτείται για την αποκατάσταση των κτηριακών εγκαταστάσεων, στην περίπτωση που αυτές έχουν υποστεί σοβαρή ζημία ή καταστροφή.

Επιπλέον, το Σχέδιο Αντιμετώπισης Έκτακτων Αναγκών που παρουσιάζεται στο υπόλοιπο του κειμένου δέχεται ως ανεκτή απώλεια την απώλεια των δεδομένων που αντιστοιχούν σε εισαγωγή στοιχείων *μίας εργάσιμης ημέρας*. Σε περίπτωση που το επεισόδιο είναι μεγάλης κλίμακας, το Σχέδιο δέχεται ως ανεκτή απώλεια την απώλεια των δεδομένων που έχουν εισαχθεί στο σύστημα *την τελευταία εβδομάδα*.

Το Σχέδιο Αντιμετώπισης Έκτακτων Αναγκών, μεταξύ άλλων, προβλέπει τα ακόλουθα:

- **Έξι σημεία λήψης εφεδρικών αντιγράφων**: (α) στον κεντρικό εξυπηρετητή του συστήματος των ΔΠΣΝ (β) στον εξυπηρετητή του συστήματος Αιμοδοσίας (γ) στον εξυπηρετητή του συστήματος της Μισθοδοσίας (δ) στον εξυπηρετητή της εφαρμογής Πρωτοκόλλου (ε) στους σταθμούς εργασίας του Γραφείου Προμηθειών και (στ) στους σταθμούς εργασίας της Διεύθυνσης Προσωπικού.
- **Τρεις γενιές εφεδρικών αντιγράφων** με ημερήσια, εβδομαδιαία και εξαμηνιαία περιοδικότητα.
- Μεταφορά εφεδρικών αντιγράφων σε χώρο **εκτός** των κτηριακών εγκαταστάσεων του νοσοκομείου.
- Περιγραφή των απαραίτητων **προπαρασκευαστικών ενεργειών** για την εφαρμογή του Σχεδίου Αντιμετώπισης Έκτακτων Αναγκών.

Για την αποτελεσματική εφαρμογή του Σχεδίου απαιτείται η υιοθέτησή του από τη Διοίκηση του νοσοκομείου, η ανάθεση ρόλων και υπευθυνοτήτων σε συγκεκριμένα άτομα, η δοκιμαστική αρχική εφαρμογή, η σταδιακή μετάβαση σε πλήρη εφαρμογή, η πραγματοποίηση δοκιμών και η αναθεώρηση ή απλή επικαιροποίηση του Σχεδίου στην περίπτωση που θα πραγματοποιηθούν σημαντικές μεταβολές στα ΠΣ του νοσοκομείου. Στα κεφάλαια 5 και 6 αντίστοιχα, βρίσκονται συνοπτικά η αποτίμηση των Πληροφοριακών Συστημάτων και η

εκτίμηση επικινδυνότητας, όπως αυτά είχαν ήδη παρουσιαστεί σε προγενέστερη μελέτη για το γενικό Σχέδιο Ασφαλείας του Νοσοκομείου.

1.2. Αντικείμενο, σκοπός και στόχοι

Η παρούσα μελέτη έχει ως αντικείμενο την προετοιμασία της νοσοκομειακής μονάδας για την αντιμετώπιση πιθανών έκτακτων περιστατικών, που θα έχουν ως συνέπεια την απώλεια της ακεραιότητας των δεδομένων που διαχειρίζονται τα Πληροφοριακά Συστήματα της ΝΜ ή θα επιφέρουν εκτεταμένη καταστροφή στον υλικό εξοπλισμό τους. Η ανάπτυξη Σχεδίου Αντιμετώπισης Αναγκών θεωρείται σημαντική για το ΝΜ, λόγω της σημασίας που αποδίδεται:

- Στην προσφορά αξιόπιστων και υψηλής ποιότητας υπηρεσιών υγείας προς το κοινό που χρήζει των υπηρεσιών του.
- Στην προστασία των δεδομένων που τηρούνται στα πληροφοριακά του συστήματα, τα οποία αξιολογούνται ως ιδιαίτερα σημαντικά για τη λειτουργία του Νοσοκομείου και συνεπώς για τη συνέχιση της άρτιας παροχής υπηρεσιών υγείας στο κοινό.
- Στην ασφάλεια των ατόμων που εργάζονται στους χώρους που στεγάζονται πληροφοριακά συστήματα.
- Στη διασφάλιση των επενδύσεων της ΝΜ σε πληροφοριακή τεχνολογία.
- Στη διατήρηση της θετικής δημόσιας εικόνας της ΝΜ και στην ανάδειξη της αξιοπιστίας του.

Σκοπός της παρούσας μελέτης είναι η ανάπτυξη και τεκμηρίωση του Σχεδίου Αντιμετώπισης Έκτακτων Αναγκών ΠΣ της ΝΜ. Το Σχέδιο αποσκοπεί στην επίτευξη των εξής στόχων:

- Στον περιορισμό των συνεπειών από την εκδήλωση φυσικών καταστροφών ή κακόβουλων ενεργειών, που ενδέχεται να έχουν ως αποτέλεσμα την εκτεταμένη καταστροφή των στοιχείων των ΠΣ.
- Στην ανάκαμψη των ΠΣ, έπειτα από πιθανή καταστροφή.
- Στην αποκατάσταση της ομαλής λειτουργίας των ΠΣ και των δεδομένων που διαχειρίζονται.

Η παρούσα μελέτη περιλαμβάνει, επιπλέον, τις προπαρασκευαστικές ενέργειες που απαιτούνται για την εφαρμογή του Σχεδίου Αντιμετώπισης Έκτακτων Αναγκών. Σε αυτό το πλαίσιο εντάσσεται και το Σχέδιο Λήψης και Διαχείρισης Εφεδρικών Αντιγράφων, η εφαρμογή του οποίου αποτελεί απαραίτητη προϋπόθεση για την επιτυχή αντιμετώπιση πιθανών καταστροφών.

1.3. Εύρος και περιορισμοί

Η μελέτη για την ασφάλεια των δεδομένων (backup plan) και την αντιμετώπιση έκτακτων αναγκών (disaster recovery plan) έχει ως αντικείμενο τα Πληροφοριακά Συστήματα και τα αρχεία που περιλαμβάνουν ευαίσθητα δεδομένα της Νοσοκομειακής Μονάδας.

Το Σχέδιο Αντιμετώπισης Έκτακτων Αναγκών αναφέρεται στην αποκατάσταση της λειτουργίας των πληροφοριακών συστημάτων έπειτα από ενδεχόμενη καταστροφή. Ο όρος καταστροφή αναφέρεται σε επεισόδια μεγάλης κλίμακας, και όχι σε περιπτώσεις απώλειας ορισμένων στοιχείων των ΠΣ, που δεν οδηγούν σε ανάσχεση της λειτουργίας των ΠΣ και τα οποία αντιμετωπίζονται με την εφαρμογή των μέτρων που περιγράφει το Σχέδιο Ασφάλειας για τα Πληροφοριακά Συστήματα της Νοσοκομειακής Μονάδας το οποίο περιγράφεται σε προγενέστερη μελέτη και από το οποίο χρησιμοποιήσαμε την αποτίμηση των ΠΣ και την εκτίμηση τη επικινδυνότητας για να συντάξουμε την παρούσα μελέτη.

Με βάση τα αποτελέσματα της μελέτης ασφάλειας, τα οποία παρουσιάζονται αναλυτικά σε προγενέστερη μελέτη, συγκροτήθηκε το Σχέδιο Αντιμετώπισης Έκτακτων αναγκών, το οποίο περιλαμβάνει:

- Τις απαιτούμενες ενέργειες προετοιμασίας εφαρμογής και υποστήριξης του Σχεδίου.
- Το Σχέδιο Δράσης για την αντιμετώπιση έκτακτων περιστατικών, τα οποία δύναται να επιφέρουν ολική καταστροφή.
- Τις ενέργειες αποκατάστασης της λειτουργίας των ΠΣ της ΝΜ.
- Την περιγραφή της απαραίτητης τεκμηρίωσης, η οποία περιλαμβάνει, μεταξύ άλλων, τους καταλόγους τηλεφώνων του προσωπικού και τα έντυπα καταγραφής υλικού και λογισμικού.

Η μελέτη αναφέρεται στην τρέχουσα τεχνολογία, στην παρούσα διάταξη και διαμόρφωση των υπολογιστικών συστημάτων των ΠΣ της ΝΜ, τις κτηριακές υποδομές και εγκαταστάσεις της ΝΜ στην παρούσα κατάστασή τους, καθώς και τις εφαρμογές και λειτουργίες που έχουν υλοποιηθεί στα πλαίσια των ΠΣ του Νοσοκομείου. Ενδεχόμενες σημαντικές αλλαγές σε κάποια από τις παραπάνω συνιστώσες θα επιφέρουν την ανάγκη επικαιροποίησης της μελέτης και του Σχεδίου Αντιμετώπισης Έκτακτων Αναγκών.

1.4. Περιγραφή και Οριοθέτηση των ΠΣ της ΝΜ

Το Σχέδιο Αντιμετώπισης Έκτακτων Αναγκών που παρουσιάζεται στις παραγράφους που ακολουθούν έχει ως αντικείμενο μελέτης τα Πληροφοριακά Συστήματα της Νοσοκομειακής Μονάδας.

Για τους σκοπούς της παρούσας μελέτης υιοθετείται ο εξής ορισμός του Πληροφοριακού Συστήματος (ΠΣ):

Πληροφοριακό Σύστημα είναι ένα οργανωμένο σύνολο στοιχείων, αποτελούμενο από ανθρώπους, λογισμικό, υλικό, διαδικασίες και δεδομένα, που βρίσκονται σε αλληλεπίδραση μεταξύ τους και με το περιβάλλον, με σκοπό την παραγωγή και διαχείριση πληροφορίας για την υποστήριξη ανθρώπινων δραστηριοτήτων, στα πλαίσια ενός οργανισμού.

Τα υπό μελέτη ΠΣ της ΝΜ περιλαμβάνουν τα εξής στοιχεία:

- Υλικός εξοπλισμός (hardware)

Ο υλικός εξοπλισμός των Πληροφοριακών Συστημάτων της ΝΜ που εντάσσεται στο πλαίσιο της μελέτης ασφάλειας περιλαμβάνει τα ακόλουθα:

Εξοπλισμός κεντρικών συστημάτων.

- Ένας (1) εξυπηρετητής τύπου Dell PowerEdge R230 Server με λειτουργικό σύστημα Windows Server 2019, που φιλοξενεί την εφαρμογή Ηλεκτρονικού Πρωτοκόλλου.
- Ένας (1) εξυπηρετητής τύπου Dell PowerEdge R330 Server με λειτουργικό σύστημα Microsoft SQL Server 2019, που φιλοξενεί τις εφαρμογές ΔΠΣΝ (Τμήμα Εισαγωγών Ασθενών, Φαρμακείο, Γραφείο Υλικού, Λογιστήριο, Τμήμα Διατροφής, τη Γραμματεία Εξωτερικών Ιατρείων, τα Γραφεία Νοσηλίων, Ιματισμού και Υγειονομικού Υλικού).
- Ένας (1) εξυπηρετητής τύπου Dell PowerEdge R230 Server με λειτουργικό σύστημα Windows Server 2019, ο οποίος φιλοξενεί τις εφαρμογές του Τμήματος Αιμοδοσίας.
- Προσωπικοί Υπολογιστές με λειτουργικό σύστημα Windows 10 που φιλοξενούν την εφαρμογή της Μισθοδοσίας.
- Ένας (1) κεντρικός εκτυπωτής (Canon), για τον κεντρικό εξυπηρετητή που βρίσκεται στο Τμήμα Πληροφορικής και Οργάνωσης.
- Δικτυακός εξοπλισμός των κεντρικών συστημάτων.

Σταθμοί εργασίας.

- Οι σταθμοί εργασίας που λειτουργούν ως τερματικοί σταθμοί του κεντρικού συστήματος εφαρμογών του ΔΠΣΝ, εξυπηρετούν τους χρήστες των εφαρμογών αυτών.
- Σταθμοί εργασίας για χρήση των τοπικών εφαρμογών (Αιμοδοσία, Πρωτόκολλο, Μισθοδοσία, Προσωπικό και Προμήθειες).
- Προσωπικοί υπολογιστές για επαγγελματική και επιστημονική χρήση του προσωπικού της ΝΜ.

Εξοπλισμός δικτύου. Περιλαμβάνει τις συσκευές του δικτύου, όπως δρομολογητές, τερματικές συσκευές κλπ., που χρησιμοποιούνται για τη λειτουργία των Πληροφοριακών Συστημάτων της ΝΜ.

- Λογισμικό και εφαρμογές

Λογισμικό συστημάτων και ανάπτυξης εφαρμογών. Σε αυτό περιλαμβάνονται τα λειτουργικά συστήματα των εξυπηρετητών και των σταθμών εργασίας (Windows), βοηθητικό λογισμικό (π.χ. MS Office), λογισμικό βάσεων δεδομένων (SQL), λογισμικό διαχείρισης ηλεκτρονικού ταχυδρομείου (email) και λογισμικό για την ασφάλεια των Πληροφορικών Συστημάτων (TrendMicro).

Εφαρμογές Διαχειριστικού Πληροφοριακού Συστήματος Νοσοκομείου (ΔΠΣΝ): Περιλαμβάνονται οι εφαρμογές του Τμήματος Εισαγωγής Ασθενών, του Φαρμακείου, του Γραφείου Υλικού, του Γραφείου Χρηματικού (Λογιστηρίου), του Τμήματος Διατροφής, της Γραμματείας Εξωτερικών Ιατρείων, του Γραφείου Νοσηλίων, του Γραφείου Ιματισμού, και του Γραφείου Υγειονομικού Υλικού.

Τοπικές εφαρμογές: Περιλαμβάνονται οι εφαρμογές της Αιμοδοσίας (i_blood), η εφαρμογή της Μισθοδοσίας και η εφαρμογή Ηλεκτρονικού Πρωτοκόλλου.

Ειδικές εφαρμογές: Λογισμικό που χρησιμοποιείται για ειδικούς σκοπούς, όπως το firewall 4000 της εταιρείας Checkpoint.

- Δεδομένα

Στα δεδομένα που θα περιληφθούν στο Σχέδιο Αντιμετώπισης Έκτακτων Αναγκών εντάσσεται το σύνολο των δεδομένων που διαχειρίζονται οι εφαρμογές που καταγράφονται στην προηγούμενη παράγραφο.

- Διαδικασίες

Καλύπτονται τόσο οι διαδικασίες χρήσης, όσο και οι διαδικασίες διαχείρισης και συντήρησης των Πληροφοριακών Συστημάτων.

- Ανθρώπινο δυναμικό

Το Σχέδιο Αντιμετώπισης Έκτακτων Αναγκών αναφέρεται στους χρήστες των παραπάνω εφαρμογών και συστημάτων καθώς και στους διαχειριστές αυτών.

1.5. Απειλές και κίνδυνοι

Το Σχέδιο Αντιμετώπισης Έκτακτων Αναγκών έχει λάβει υπόψη τις εξής απειλές που δυνητικά αντιμετωπίζουν τα υπό μελέτη ΠΣ της ΝΜ και οι οποίες είναι δυνατόν, κάτω από ορισμένες συνθήκες, να οδηγήσουν σε ολική καταστροφή των ΠΣ:

- Τρομοκρατική ενέργεια
- Καταστροφή μέσου αποθήκευσης δεδομένων
- Παραβίαση συστήματος ελέγχου λογικής πρόσβασης και καταστροφή λογισμικού και δεδομένων
- Πυρκαγιά
- Σεισμός
- Δολιοφθορά
- Κλοπή εξοπλισμού

1.6. Πρότυπα που ακολουθήθηκαν

Τα πρότυπα που ακολουθήθηκαν είναι τα:

- ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems
- ISO/IEC 22301/2019 Security and resilience – Business continuity management systems

2. Διαδικασίες υποστήριξης & προετοιμασίας για την αντιμετώπιση έκτακτων περιστατικών

2.1. Σχέδιο λήψης και διαχείρισης εφεδρικών αντιγράφων

Το παρόν Σχέδιο διαχωρίζει τα δεδομένα σε έξι κατηγορίες: (α) τα δεδομένα που επεξεργάζονται οι εφαρμογές του Διαχειριστικού Πληροφοριακού Συστήματος του Νοσοκομείου (ΔΠΣΝ) (β) τα δεδομένα που διαχειρίζεται το σύστημα της Αιμοδοσίας (γ) τα δεδομένα που διαχειρίζεται το σύστημα της Μισθοδοσίας (δ) τα δεδομένα Προσωπικού (ε) τα δεδομένα που διαχειρίζεται το Τμήμα Προμηθειών (στ) τα δεδομένα του Πρωτοκόλλου.

Για καθεμία από τις παραπάνω κατηγορίες προβλέπεται η λήψη ανεξάρτητων αντιγράφων. Ως μέσο αποθήκευσης για τα δεδομένα του κεντρικού εξυπηρετητή των εφαρμογών ΔΠΣΝ προτείνεται η *μαγνητική ταινία*.

Το Σχέδιο διασφαλίζει τις κύριες ομάδες δεδομένων των ΠΣ της ΝΜ, αποδέχεται όμως, σε εξαιρετικές περιπτώσεις, την πιθανότητα απώλειας των δεδομένων που έχουν εισαχθεί στο σύστημα κατά το χρονικό διάστημα ανάμεσα σε δύο λήψεις εφεδρικών αντιγράφων. Τα τελευταία θα πρέπει να εισαχθούν στο σύστημα εκ νέου, αξιοποιώντας τα χειρόγραφα ή έντυπα αντίγραφα (πρωτογενή δεδομένα).

Η διαχείριση των αντιγράφων προβλέπει την ***τήρηση τριών γενεών αντιγράφων***. Η μία, η πλέον πρόσφατη, θα πρέπει να διατηρείται σε εύκολα προσβάσιμο χώρο εντός του κεντρικού κτηρίου της ΝΜ, η δεύτερη και τρίτη γενιά πρέπει να μεταφέρονται εκτός του κτηρίου της ΝΜ σε χώρο που θα επιλεγεί.

- **Πρώτη γενιά αντιγράφων**

Η πρώτη γενιά αναφέρεται στη λήψη ημερήσιου εφεδρικού αντίγραφου. Τα ημερήσια αντίγραφα φυλάσσονται στο χώρο εντός των εγκαταστάσεων της ΝΜ. Τα ημερήσια αντίγραφα περιλαμβάνουν μόνο *δεδομένα* και όχι λογισμικό συστήματος και εφαρμογών.

- **Δεύτερη γενιά αντιγράφων**

Η δεύτερη γενιά αναφέρεται στην εβδομαδιαία λήψη εφεδρικού αντίγραφου. Το μαγνητικό μέσο εισάγεται στη συσκευή την Παρασκευή και η λήψη γίνεται χωρίς επίβλεψη Σάββατο – Κυριακή. Το αντίγραφο είναι πλήρες. Τη Δευτέρα ελέγχεται η ορθή λήψη του αντίγραφου, αναγράφεται η ημερομηνία και η ταινία μεταφέρεται στο χώρο φύλαξης που βρίσκεται εκτός του κτηρίου της ΝΜ.

- **Ετήσιο αντίγραφο**

Στο τέλος του έτους λαμβάνουμε ένα πλήρες αντίγραφο σε καινούργια μαγνητική ταινία. Το αντίγραφο φυλάσσεται στον εκτός ΝΜ χώρο αποθήκευσης. Αυτό το αντίγραφο δε θα πρέπει να ανακυκλώνεται, αλλά να διατηρείται.

Τα αντίγραφα διακρίνονται σε *αντίγραφα του λογισμικού συστήματος και εφαρμογών* και σε *αντίγραφα των δεδομένων*. Η τεχνική της λήψης επαυξητικών

(incremental) αντιγράφων δεν συνιστάται, διότι η αξιοπιστία της εξαρτάται σε μεγάλο βαθμό από την αξιοπιστία των μέσων αποθήκευσης. Η παραπάνω τεχνική εισάγει εξαρτήσεις μεταξύ των αντιγράφων, υποβαθμίζοντας την αξιοπιστία μίας ολόκληρης ομάδας αντιγράφων στο επίπεδο αξιοπιστίας του πλέον ευπαθούς αντίγραφου.

2.2. Προπαρασκευαστικές Ενέργειες Εφαρμογής Σχεδίου Αντιμετώπισης Έκτακτων Αναγκών

Η εφαρμογή του Σχεδίου Αντιμετώπισης Έκτακτων Αναγκών συνεπάγεται την ενίσχυση του υπάρχοντος εξοπλισμού με συσκευές λήψης αντιγράφων και την εξασφάλιση κατάλληλου χώρου εκτός των κτηριακών εγκαταστάσεων της ΝΜ και σε ικανή από αυτές απόσταση. Οι προπαρασκευαστικές ενέργειες που απαιτούνται είναι οι ακόλουθες:

- **Προμήθεια συσκευών λήψης εφεδρικών αντιγράφων δεδομένων**
- **Επιλογή και διαμόρφωση χώρων φύλαξης αντιγράφων**.

Στις κτηριακές εγκαταστάσεις της ΝΜ θα πρέπει να επιλεγεί και να διαμορφωθεί ένας χώρος για την ασφαλή φύλαξη των εφεδρικών αντιγράφων. Ο χώρος αυτός απαιτείται να είναι εύκολα προσβάσιμος από τους διαχειριστές των συστημάτων. Συνιστάται η τοποθέτηση φωριαμού, κατά προτίμηση στον ίδιο όροφο με το δωμάτιο των εξυπηρετητών. Σε αυτόν θα τοποθετηθούν: η πιο πρόσφατη γενιά εφεδρικών αντιγράφων, οι δισκέτες ή οπτικοί δίσκοι που απαιτούνται για την εγκατάσταση των συσκευών λήψεως αντιγράφων, οι οδηγίες εγκατάστασης και λειτουργίας των συσκευών και ένα αντίγραφο του παρόντος Σχεδίου.

- **Εξασφάλιση χώρου φύλαξης αντιγράφων εκτός κεντρικού κτηρίου ΝΜ**.

Θα πρέπει να επιλεγεί χώρος εκτός του κεντρικού κτηρίου της ΝΜ, για την ασφαλή φύλαξη εφεδρικών αντιγράφων. Για αυτήν τη χρήση είναι δυνατό να μισθωθεί θυρίδα τραπέζης ή να συναφθεί ειδική συμφωνία συνεργασίας με ιδιωτικό ή δημόσιο οργανισμό. Σε αυτό το χώρο θα αποθηκευτούν τα εφεδρικά αντίγραφα δεύτερης και τρίτης γενιάς, το ετήσιο αντίγραφο, καθώς και ένα αντίγραφο του παρόντος Σχεδίου.

- **Δίσκοι επαναφοράς λειτουργίας**

Για την ταχεία αποκατάσταση της λειτουργίας των σταθμών εργασίας συνιστάται η δημιουργία οπτικών δίσκων επαναφοράς στην αρχική κατάσταση για κάθε βασικό τύπο σταθμού εργασίας.

- **Αρχείο λογισμικού και οδηγιών**

Η αποκατάσταση ενός συστήματος συχνά απαιτεί την εγκατάσταση του λογισμικού συστήματος (λειτουργικό σύστημα, διαχειριστής βάσης δεδομένων κ.ά.) και των εφαρμογών. Για την υποστήριξη των ενεργειών αυτών προτείνεται η δημιουργία αρχείου λογισμικού, όπου θα αποθηκεύονται οι μαγνητικές δισκέτες ή οι οπτικοί δίσκοι εγκατάστασης του λογισμικού και οι οδηγίες εγκατάστασης.

2.3. Ρόλοι και Υπευθυνότητες

Η αποτελεσματική εφαρμογή του Σχεδίου προϋποθέτει τον καθορισμό ορισμένων ρόλων και ομάδων και την επιλογή συγκεκριμένων προσώπων για κάθε ρόλο. Ο κύριος ρόλος είναι αυτός του Υπεύθυνου Ασφάλειας και οι κύριες ομάδες είναι οι Ομάδες Ασφάλειας Προσωπικού και οι Ομάδες Αντιμετώπισης Καταστροφών.

2.3.1. *Υπεύθυνος Ασφάλειας*

Ο Υπεύθυνος Ασφάλειας έχει την ευθύνη για τη διερεύνηση, αλλά και για το συντονισμό της αντιμετώπισης τυχόν επεισοδίων που θέτουν σε κίνδυνο την ασφάλεια του συστήματος. Ο ρόλος αυτός θεωρείται θεμελιώδης για κάθε πληροφοριακό σύστημα και η παρουσία του απαιτείται για την εύρυθμη λειτουργία του πληροφοριακού συστήματος.

Το άτομο που θα αναλάβει αυτόν τον ρόλο είναι δυνατόν είτε να έχει αποκλειστικά και μόνο την ευθύνη της ασφάλειας των πληροφοριακών συστημάτων της ΝΜ, είτε να έχει στις αρμοδιότητές του και ζητήματα ασφάλειας προσωπικού, εγκαταστάσεων κ.ά.

2.3.2. *Ομάδες Ασφάλειας Προσωπικού*

Η αντιμετώπιση έκτακτων γεγονότων, τα οποία είναι πιθανόν να θέσουν σε κίνδυνο την ασφάλεια του προσωπικού, προϋποθέτει την ανάπτυξη μίας αντίστοιχης οργανωτικής δομής. Οι ομάδες ασφάλειας προσωπικού έχουν ως αρμοδιότητα το συντονισμό των ενεργειών του προσωπικού σε περιπτώσεις έκτακτων γεγονότων, όπως για παράδειγμα η εκκένωση του κτηρίου σε περίπτωση πυρκαγιάς.

2.3.3. *Ομάδα Αντιμετώπισης Καταστροφών*

Η Ομάδα Αντιμετώπισης Καταστροφών έχει ως στόχο το συντονισμό των ενεργειών που απαιτούνται για την αντιμετώπιση πιθανών καταστροφών. Στην ομάδα αυτή θα πρέπει να μετέχουν ανώτερα στελέχη της Διοίκησης του Νοσοκομείου. Σημειώνεται ότι η αποκατάσταση των πληροφοριακών συστημάτων αποτελεί ένα μόνο τμήμα της αποκατάστασης της όλης λειτουργίας του Νοσοκομείου.

3. Εφαρμογή και συντήρηση Σχεδίου Αντιμετώπισης Εκτάκτων Αναγκών

3.1. Εκπαίδευση και ενημέρωση

Η εφαρμογή του Σχεδίου προϋποθέτει ότι τα άτομα που θα κληθούν να το εφαρμόσουν γνωρίζουν το Σχέδιο και έχουν τις απαιτούμενες δεξιότητες για να το εφαρμόσουν. Για αυτόν το λόγο προτείνονται οι εξής ενέργειες:

- Προσδιορισμός ενός *υπευθύνου* για την επίβλεψη *εφαρμογής* του Σχεδίου.
- Προσδιορισμός των ατόμων που εμπλέκονται στην εφαρμογή του Σχεδίου.
- Παρουσίαση του Σχεδίου από τον υπεύθυνο εφαρμογής.
- Μελέτη του Σχεδίου από τα παραπάνω άτομα με στόχο να προσδιοριστούν πιθανές δυσκολίες εφαρμογής, πιθανά προβλήματα συντονισμού και αρμοδιοτήτων κ.λπ.
- Οργάνωση μίας ημερίδας, στην οποία θα εξεταστούν όλα τα σχετικά ζητήματα και θα προγραμματιστή η εφαρμογή του Σχεδίου.
- Ενημέρωση των χρηστών για το Σχέδιο.

3.2. Δοκιμές

Η εφαρμογή του σχεδίου θα πρέπει να δοκιμάζεται ετησίως. Το σενάριο της δοκιμής δεν θα πρέπει να είναι προδιαγεγραμμένο και σταθερό, αλλά σε κάθε ετήσια δοκιμή θα πρέπει να ακολουθείται διαφορετικό σενάριο, το οποίο θα έχει προετοιμαστεί για αυτόν το σκοπό και θα ανακοινώνεται λίγες ημέρες πριν την εφαρμογή του. Σε κάθε περίπτωση το σενάριο θα πρέπει να περιλαμβάνει τουλάχιστον τα εξής:

- Πλήρη αποκατάσταση ενός συστήματος, χρησιμοποιώντας έναν υπολογιστή δοκιμής (απλό προσωπικό υπολογιστή), χωρίς να απαιτείται η διακοπή λειτουργίας του κανονικού συστήματος.
- Ανάγνωση τουλάχιστον ενός αρχείου από τα εφεδρικά αντίγραφα πρώτης, δεύτερης και τρίτης γενιάς.

3.3. Διαχείριση αλλαγών

Το παρόν Σχέδιο λαμβάνει υπόψη τις προδιαγραφόμενες εξελίξεις, τόσο στον τομέα των Τεχνολογιών Πληροφορικής και Επικοινωνιών, όσο και στη λειτουργία της ΝΜ. Είναι φανερό, όμως, ότι ενδεχόμενες σημαντικές αλλαγές σε μία από τις παραπάνω συνιστώσες θα επιφέρουν την ανάγκη για επικαιροποίηση του Σχεδίου.

Κατά συνέπεια απαιτείται το παρόν Σχέδιο να αναπροσαρμόζεται σε κάθε σημαντική αλλαγή των ΠΣ της ΝΜ. Σε κάθε αναπροσαρμογή θα πρέπει να εξασφαλίζεται ότι:

- Όλα τα άτομα που έχουν ρόλο στην εφαρμογή του Σχεδίου έχουν την τελευταία έκδοση του Σχεδίου.
- Όλα τα άτομα που έχουν ρόλο στην εφαρμογή του Σχεδίου έχουν ενημερωθεί για το ποιες μεταβολές έχουν γίνει και ποιες ενέργειες απαιτούνται εκ μέρους τους για τη μετάβαση στο νέο Σχέδιο.

4. Σχέδιο Αντιμετώπισης Έκτακτων Αναγκών

4.1. Στόχοι του Σχεδίου Αντιμετώπισης Έκτακτων Αναγκών

Το Σχέδιο Αντιμετώπισης Έκτακτων Αναγκών αποσκοπεί στην αποκατάσταση της λειτουργίας των ΠΣ σε εύλογο χρονικό διάστημα μετά από την πραγματοποίηση καταστροφικού γεγονότος.

- Το Σχέδιο Αντιμετώπισης Έκτακτων Αναγκών έχει ως στόχο την αποκατάσταση της λειτουργίας των ΠΣ εντός δύο εβδομάδων.
- Τα συστήματα κατατάσσονται κατά σειρά προτεραιότητας αποκατάστασης ως εξής:
    - Οι εφαρμογές του Διαχειριστικού Πληροφοριακού Συστήματος Νοσοκομείου (ΔΠΣΝ) (εφαρμογές του Τμήματος Εισαγωγής Ασθενών, του Φαρμακείου, του Γραφείου Υλικού, του Γραφείου Χρηματικού (Λογιστηρίου), του Τμήματος Διατροφής, της Γραμματείας Εξωτερικών Ιατρείων, του Γραφείου Νοσηλίων, του Γραφείου Ιματισμού, και του Γραφείου Υγειονομικού Υλικού).
    - Το σύστημα της Αιμοδοσίας.
    - Το σύστημα της Μισθοδοσίας.
    - Το σύστημα του Πρωτοκόλλου.
    - Τα δεδομένα του Γραφείου Προμηθειών.
    - Τα δεδομένα της Διεύθυνσης Προσωπικού.

4.2. Εφεδρικά Αντίγραφα Δεδομένων

Να λαμβάνονται εφεδρικά αντίγραφα των δεδομένων.

- Τουλάχιστον ένα αντίγραφο να φυλάσσεται σε μέρος τέτοιο, ώστε να είναι απίθανο αυτό και τα πρωτότυπα δεδομένα να επηρεαστούν από το ίδιο γεγονός.
    - *Επιτρέπεται η τήρηση ενός εφεδρικού ημερήσιου αντιγράφου στον ίδιο χώρο με τους εξυπηρετητές.*
    - *Το εβδομαδιαίο αντίγραφο να αποθηκεύεται σε κτήριο της ΝΜ διαφορετικό από εκείνο στο οποίο φιλοξενούνται οι εξυπηρετητές.*
    - *Η μεταφορά του αντιγράφου να γίνεται με διαδικασία που εγγυάται την υπευθυνότητα κατά τη μεταφορά και την παράδοση/παραλαβή.*
- Τα εφεδρικά αντίγραφα να απολαμβάνουν του ίδιου επιπέδου προστασίας με τα «εν ενεργεία» δεδομένα.
    - *Τα εφεδρικά αντίγραφα να φυλάσσονται σε κατάλληλους χώρους που τα προστατεύουν από φυσικούς και κλιματολογικούς παράγοντες.*
    - *Τα εφεδρικά αντίγραφα να φυλάσσονται σε χώρο που τα προστατεύει από μη εξουσιοδοτημένη πρόσβαση.*

  - *Τα μέσα αποθήκευσης των εφεδρικών αντιγράφων να χρησιμοποιούνται σύμφωνα με τις οδηγίες του κατασκευαστή.*
  - *Τα εφεδρικά αντίγραφα που περιλαμβάνουν ευαίσθητα προσωπικά δεδομένα να κρυπτογραφούνται.*
- Να τηρούνται τουλάχιστον τρεις γενιές εφεδρικών αντιγράφων.
  - *Οι τρεις γενιές να είναι ημερήσια, εβδομαδιαία, μηνιαία. Για δεδομένα με μικρότερες απαιτήσεις διαθεσιμότητας (πχ. δεδομένα προμηθευτών και συμβάσεων) και με ολιγάριθμες ημερήσιες εισαγωγές δεδομένων (πχ. δεδομένα προσωπικού) δεν απαιτείται η λήψη ημερήσιου αντιγράφου.*
  - *Μία γενιά να περιλαμβάνει εκτός των δεδομένων και το λογισμικό συστήματος (full system back-up).*
- Κάθε εφεδρικό αντίγραφο να φέρει κωδικό αναγνώρισης.
  - *Ο κωδικός αναγνώρισης να χρησιμοποιείται για αντιστοίχιση του εφεδρικού αντιγράφου με τα δεδομένα που περιέχει και τις αντίστοιχες εφαρμογές. Να προσδιορίζεται επίσης και η συγκεκριμένη έκδοση της εφαρμογής.*
- Οι διαδικασίες λήψης εφεδρικών αντιγράφων και αποκατάστασης να ελέγχονται τουλάχιστον μία φορά το χρόνο.
- Σε κάθε ουσιαστική μεταβολή του λογισμικού εφαρμογών πρέπει να λαμβάνονται εφεδρικά αντίγραφα όλων των εφαρμογών λογισμικού.
- Επιπλέον των αντιγράφων δεδομένων, να διατηρούνται και οι εφαρμογές που χρησιμοποιούνται για την ανάγνωση των δεδομένων.
- Οι μαγνητικές ταινίες, ή όποιο άλλο αποθηκευτικό μέσο επιλεχθεί να χρησιμοποιηθεί, να ανανεώνονται τακτικά, σύμφωνα με όσα προβλέπει ο κατασκευαστής τους.
- Για κάθε νέο σύστημα που εγκαθίσταται στο ΝΜ να λαμβάνεται μέριμνα για τον εξοπλισμό που είναι αναγκαίος για τη λήψη και διαχείριση των εφεδρικών αντιγράφων.
- Οι φωριαμοί που χρησιμοποιούνται για τη φύλαξη εφεδρικών αντιγράφων δεδομένων *(back-up)* να είναι πυράντοχοι και να ανθίστανται στη θερμότητα για τουλάχιστον τριάντα (30) λεπτά.

4.3. Επιλογή & προμήθεια συστήματος λήψεως εφεδρικών αντιγράφων δεδομένων

Η ανάκτηση των δεδομένων εξαρτάται από την ποιότητα των εφεδρικών αντιγράφων δεδομένων. Για το λόγο αυτό η επιλογή και προμήθεια κατάλληλων συστημάτων λήψεως εφεδρικών αντιγράφων δεδομένων είναι ιδιαίτερα σημαντική.

- Το σύστημα λήψεως εφεδρικών αντιγράφων θα πρέπει να έχει τουλάχιστον τα παρακάτω χαρακτηριστικά:
  - *Να ανιχνεύει αν το μέσο αποθήκευσης είναι ακατάλληλο ή έχει βλάβη.*

- *Η χωρητικότητα των μέσων αποθήκευσης θα πρέπει να είναι αντίστοιχη του όγκου των δεδομένων για τα οποία απαιτείται η λήψη εφεδρικών αντιγράφων.*
- *Σε περίπτωση αποτυχίας της λήψης εφεδρικού αντίγραφου το σύστημα θα πρέπει να μπορεί να ενημερώνει αυτόματα.*
- *Με την ολοκλήρωση της λήψης του αντιγράφου, το σύστημα να συγκρίνει τα πρωτότυπα δεδομένα με τα δεδομένα του αντίγραφου.*
- *Να δίνει τη δυνατότητα επιλεκτικής επαναφοράς (restore) ορισμένων αρχείων και καταλόγων.*

4.4. Εφεδρικές εγκαταστάσεις

Να προσδιοριστεί ο χώρος στον οποίο θα εγκατασταθούν προσωρινά τα συστήματα πληροφορικής, σε περίπτωση έκτακτης ανάγκης .

- Ο εφεδρικός χώρος εγκατάστασης να είναι σε διαφορετικό κτήριο.
  - *Ο χώρος αυτός δύναται να χρησιμοποιείται για άλλους σκοπούς, με την προϋπόθεση ότι θα διατεθεί άμεσα εφόσον παραστεί ανάγκη.*
- Να συνταχθεί κατάλογος με τον απαραίτητο εξοπλισμό που θα πρέπει να διατεθεί για την εγκατάσταση και λειτουργία στο νέο χώρο.
  - *Να καταρτιστεί σχέδιο βασισμένο σε τεχνολογίες ασύρματων δικτύων.*
- Ο εφεδρικός χώρος να διαθέτει επαρκείς εγκαταστάσεις παροχής ηλεκτρικής ενέργειας, καθώς και τηλεφωνικές γραμμές VDSL.
- Ο εφεδρικός χώρος να διαθέτει σύστημα συναγερμού και να παρέχει ικανή προστασία από απόπειρες παράνομης εισόδου.

4.5. Επείγουσα προμήθεια

Θα πρέπει να διασφαλιστεί η δυνατότητα άμεσης προμήθειας εξοπλισμού για τη λειτουργία των συστημάτων που έχουν πληγεί.

- Για το βασικό υλικό εξοπλισμό (πχ. κεντρικός εξυπηρετητής εφαρμογής ΔΠΣΝ, εξυπηρετητής Αιμοδοσίας) να υπάρχουν συμβόλαια συντήρησης που προβλέπουν αντικατάσταση των συστημάτων σε χρονικό διάστημα που δε θα υπερβαίνει τη μία (1) εβδομάδα.
  - *Τα συστήματα θα πρέπει να είναι απολύτως συμβατά με τα υπάρχοντα συστήματα και να έχουν εγκαταστημένο το ίδιο ή συμβατό λειτουργικό σύστημα.*
  - *Τα σχετικά συμβόλαια θα πρέπει να προβλέπουν ρήτρες σε περίπτωση καθυστέρησης παράδοσης των νέων συστημάτων.*
- Να διαμορφωθεί κατάλογος με τον ελάχιστο απαραίτητο εξοπλισμό (π.χ. συσκευές δικτύου), να διερευνηθεί ο απαιτούμενος χρόνος προμήθειας και να προβλεφθούν διαδικασίες επείγουσας προμήθειας.

5. Αποτίμηση των Πληροφοριακών Συστημάτων

5.1. Εισαγωγή

Στο κεφάλαιο αυτό περιγράφονται τα αποτελέσματα της αποτίμησης των δεδομένων που διαχειρίζονται τα πληροφοριακά συστήματα του Νοσοκομείου. Η ακολουθούμενη μεθοδολογία αποδίδει ιδιαίτερη βαρύτητα στα *δεδομένα* και λιγότερο στο *υλικό* και *λογισμικό*, καθώς τα τελευταία δύναται να αποτιμηθούν με βάση το κόστος αντικατάστασής τους, ενώ τα δεδομένα θα πρέπει να αποτιμηθούν με βάση τις επιπτώσεις της απώλειας των βασικών χαρακτηριστικών ασφάλειας και συγκεκριμένα την απώλεια της *διαθεσιμότητας*, της *ακεραιότητας* και της *εμπιστευτικότητάς* τους.

5.2. Αποτίμηση αξίας δεδομένων

Τα δεδομένα αξιολογούνται με βάση τις απόψεις των τελικών χρηστών των πληροφοριών που παρέχουν τα πληροφοριακά συστήματα της ΝΜ. Στο πλαίσιο της ακολουθούμενης μεθοδολογίας, η αποτίμηση δε λαμβάνει υπόψη την πιθανότητα εκδήλωσης μίας απειλής, αλλά μόνο την επίπτωση από την ενδεχόμενη επιτυχή πραγματοποίηση της απειλής αυτής. Η ακρίβεια της αποτίμησης συναρτάται με την ακρίβεια και πληρότητα των δεδομένων και των σχετικών εκτιμήσεων που κοινοποιήθηκαν στους μελετητές.

Η αξιολόγηση γίνεται αριθμητικά σε κλίμακα 0-10 και οι τιμές που έχουν αποδοθεί προκύπτουν από τους Πίνακες Αποτίμησης που συνοδεύουν τη μέθοδο η οποία χρησιμοποιήθηκε κατά την προγενέστερη μελέτη για το Σχέδιο Ασφαλείας της ΝΜ.

Σε αυτό το πλαίσιο ζητήθηκε από τα στελέχη της ΝΜ να περιγράψουν το πιο απαισιόδοξο, κατά την άποψή τους, σενάριο για την επίπτωση που θα είχε κάθε ένα από τα παρακάτω ενδεχόμενα, αγνοώντας τα υφιστάμενα μέτρα ασφάλειας:

- απώλεια της διαθεσιμότητας των δεδομένων
- απώλεια της ακεραιότητας των δεδομένων
- αποκάλυψη των δεδομένων.

Σε ορισμένες περιπτώσεις, όπου απαιτείται περαιτέρω ανάλυση, εξετάζονται χωριστά και οι υποπεριπτώσεις ολικής καταστροφής των δεδομένων και σκόπιμης αλλοίωσης των δεδομένων.

Σημειώνεται ότι το σύνολο των δεδομένων που διαχειρίζονται τα ΠΣ-ΝΜ διαχωρίστηκαν και μελετήθηκαν σε αντιπροσωπευτικές ομάδες, ανάλογα με τα χαρακτηριστικά και τις ανάγκες ασφάλειας που έχουν. Συγκεκριμένα, αποτιμήθηκαν οι συνέπειες για τις εξής ομάδες δεδομένων: *Δεδομένα Αιμοδοσίας – Αιματολογικού Εργαστηρίου, Δεδομένα Εργαστηρίων, Δεδομένα Φαρμακείου, Δεδομένα Προσωπικού, Δεδομένα Μισθοδοσίας, Δεδομένα Προμηθευτών και Συμβάσεων, Δεδομένα Λογιστηρίου, Δεδομένα Επισκέψεων στα Εξωτερικά Ιατρεία, Δεδομένα Νοσηλίων, Δεδομένα Κίνησης Ασθενών,*

Δεδομένα Επικοινωνίας και Δεδομένα Πρωτοκόλλου. Κατά συνέπεια, τα συμπεράσματα που προκύπτουν ανάγονται στο σύνολο των δεδομένων της κάθε ομάδας.

Σε μελλοντική αναθεώρηση του Σχεδίου Ασφάλειας, τα πιθανά ενδεχόμενα θα πρέπει να εξεταστούν εκ νέου, με βάση τις μείζονες αλλαγές που ενδεχομένως έχουν πραγματοποιηθεί στα πληροφοριακά συστήματα της ΝΜ και στις υπηρεσίες που προσφέρουν.

5.3. Αποτελέσματα αποτίμησης

Στις ακόλουθες παραγράφους περιγράφεται αναλυτικά η αποτίμηση των επιπτώσεων από την παραβίαση της ασφάλειας των ομάδων δεδομένων που αξιολογήθηκαν στο πλαίσιο της μελέτης.

5.3.1. *Δεδομένα Αιμοδοσίας – Αιματολογικού Εργαστηρίου*

Περιεχόμενο: Τα Δεδομένα Αιμοδοσίας περιλαμβάνουν προσωπικά δεδομένα των νοσηλευόμενων, και μη, αιμοδοτών και ληπτών αίματος. Τα στοιχεία αυτά καταγράφονται στο *Δελτίο Αιμοδότη*. Επιπλέον, τηρούνται ευαίσθητα ιατρικά δεδομένα, τα οποία σχετίζονται με την κατάσταση του αίματος (επιδημιολογικά στοιχεία, αποτελέσματα ιολογικού ελέγχου κλπ.). Στην ίδια ομάδα δεδομένων περιλαμβάνονται τα προσωπικά στοιχεία πασχόντων από Μεσογειακή Αναιμία και τα ευαίσθητα ιατρικά δεδομένα που είναι απαραίτητα για μεταγγίσεις αίματος.

Σχετικό Σύστημα: Τα Δεδομένα Αιμοδοσίας τηρούνται στην *εφαρμογή Αιμοδοσίας*, η οποία βρίσκεται στο σύστημα που στεγάζεται στο Σταθμό Αιμοδοσίας στον 2ο όροφο της ΝΜ. Επίσης, τα πρωτογενή παραστατικά που περιλαμβάνουν τα προσωπικά στοιχεία των αιμοδοτών τηρούνται σε αρχείο («Καρτέλα Αιμοδότη») στον ίδιο όροφο. Τα Δεδομένα που αφορούν στη Μεσογειακή Αναιμία τηρούνται στην πιλοτικής μορφής *εφαρμογή Μεσογειακής Αναιμίας* στο ίδιο σύστημα. Παράλληλα, τηρείται χειρόγραφος φάκελος των στοιχείων πασχόντων Μεσογειακής Αναιμίας.

Απώλεια Διαθεσιμότητας Δεδομένων Αιμοδοσίας - Αιματολογικού Εργαστηρίου

Επιπτώσεις: Τα Δεδομένα Αιμοδοσίας είναι απαραίτητα για τον έλεγχο του ασκού αίματος πριν αυτός δοθεί για μετάγγιση σε ασθενή ή σε άλλα νοσοκομεία στα οποία το ΝΜ παρέχει ασκούς αίματος. Παρόλα αυτά, η μη διαθεσιμότητα των Δεδομένων Αιμοδοσίας δεν επηρεάζει σημαντικά τη λειτουργία του σταθμού Αιμοδοσίας και της Μονάδας Μεσογειακής Αναιμίας, καθώς οι διαδικασίες λήψης και μετάγγισης αίματος μπορούν να πραγματοποιηθούν με τη χρήση των χειρόγραφων παραστατικών.

Αποτίμηση: Με βάση τις παραπάνω επιπτώσεις, η συνέπεια της απώλειας διαθεσιμότητας για διάστημα μίας ώρας αποτιμάται με βαθμό **ένα (1)**, για διάστημα δώδεκα ωρών αποτιμάται με βαθμό **τρία (3)** και για διάστημα δύο ημερών και περισσότερο με βαθμό **πέντε (5)**, στην κλίμακα 0-10.

Ολική καταστροφή Δεδομένων Αιμοδοσίας - Αιματολογικού Εργαστηρίου

Επιπτώσεις: Η ολική καταστροφή των δεδομένων, τόσο των πρωτογενών όσο και των εφεδρικών αντιγράφων, συνεπάγεται την εκ νέου εισαγωγή των δεδομένων στην εφαρμογή βάσει των πρωτογενών παραστατικών, με την προϋπόθεση ότι αυτά έχουν διατηρηθεί και είναι ακέραια. Κατά συνέπεια εκτιμάται ότι το σύστημα θα υποστεί κάποια καθυστέρηση αποκατάστασης πλήρους λειτουργίας, η οποία όμως δε θα επηρεάσει σημαντικά τη δυνατότητα άμεσης και, κυρίως, αξιόπιστης παροχής αίματος στους ασθενείς της ΝΜ, γεγονός που θα είχε σημαντικές επιπτώσεις στην υγεία και την προσωπική ασφάλεια των ασθενών αυτών.

Αποτίμηση: Σύμφωνα με τις παραπάνω διαπιστώσεις η επίπτωση από την ολική καταστροφή των δεδομένων αποτιμάται με βαθμό **τρία (3)**, στην κλίμακα 0-10.

Μερική καταστροφή ή απώλεια ακεραιότητας Δεδομένων Αιμοδοσίας - Αιματολογικού Εργαστηρίου

Επιπτώσεις: Η απώλεια των δεδομένων Αιμοδοσίας που έχουν εισαχθεί έπειτα από τη λήψη του τελευταίου εφεδρικού αντιγράφου, συνεπάγεται την εκ νέου εισαγωγή των δεδομένων που έχουν απολεσθεί, με την προϋπόθεση ότι τα πρωτογενή παραστατικά διασώζονται και ότι το εφεδρικό αντίγραφο λαμβάνεται και φυλάσσεται με σωστή διαδικασία. Πιο σημαντικές επιπτώσεις προκύπτουν από την ύπαρξη σφαλμάτων στα δεδομένα, καθώς αν τα λάθη αυτά εισαχθούν σε δεδομένα που σχετίζονται με την ασφαλή διάθεση του αίματος σε ασθενείς (π.χ. ομάδα αίματος δότη, αποτελέσματα ιολογικού ελέγχου), ενδέχεται να υ-πάρξουν σημαντικές επιπτώσεις στην υγεία και προσωπική ασφάλεια των ασθενών.

Αποτίμηση: Η επίπτωση από την απώλεια ακεραιότητας των δεδομένων αποτιμάται με βαθμό **τρία (3)** για τη μερική απώλεια των δεδομένων, με βαθμό **πέντε (5)** για την περίπτωση περιορισμένης ύπαρξης λαθών και με βαθμό **έξι (6)** για την περίπτωση εισαγωγής λαθών σε ευρεία κλίμακα, σε κλίμακα 0-10.

Σκόπιμη Αλλοίωση Δεδομένων Αιμοδοσίας - Αιματολογικού Εργαστηρίου

Επιπτώσεις: Η σκόπιμη αλλοίωση των στοιχείων που αφορούν την ασφαλή διάθεση του αίματος σε ασθενείς (π.χ. ομάδα αίματος δότη, αποτελέσματα ιολογικού ελέγχου), μπορεί να θέσει σε σημαντικό κίνδυνο την υγεία και την προσωπική ασφάλεια των ασθενών της ΝΜ, καθώς η μετάγγιση σε ασθενείς μη ασφαλούς ή ακατάλληλου αίματος μπορεί να έχει πολύ σημαντικές επιπτώσεις στην υγεία ενός ή περισσότερων ασθενών. Δευτερεύουσα συνέπεια είναι ότι η εικόνα και η αξιοπιστία του σταθμού Αιμοδοσίας του Νοσοκομείου θα υποστεί σημαντικό πλήγμα, ενώ η υλοποίηση του γεγονότος αυτού θα έχει σημαντικές επιπτώσεις στην αξιοπιστία των υπηρεσιών παροχής αίματος γενικότερα.

Αποτίμηση: Σύμφωνα με το παραπάνω σενάριο η συνέπεια σκόπιμης αλλοίωσης των δεδομένων Αιμοδοσίας αποτιμάται με βαθμό **έξι (6)**, σε κλίμακα 0-10.

Αποκάλυψη Δεδομένων Αιμοδοσίας - Αιματολογικού Εργαστηρίου

Επιπτώσεις: Στα Δεδομένα Αιμοδοσίας περιλαμβάνονται προσωπικά, καθώς και ευαίσθητα ιατρικά δεδομένα (πχ. αποτελέσματα ιολογικού ελέγχου) που αφορούν τους αιμοδότες και τους λήπτες αίματος της ΝΜ. Η αποκάλυψη των στοιχείων αυτών σε τρίτους, όπως ιατρικούς επισκέπτες ή δημοσιογράφους, θα είχε ως ενδεχόμενη συνέπεια οικονομικά και άλλα οφέλη γι' αυτούς, αλλά θα προκαλούσε και σημαντική ενόχληση στα άτομα που αφορούν τα αποκαλυφθέντα ιατρικά δεδομένα. Στην περίπτωση αυτή το ΝΜ ενδεχομένως να υποστεί κυρώσεις λόγω της παράβασης του Ν. 2472/ 97, που προβλέπει σημαντικά χρηματικά πρόστιμα. Επιπλέον θα συγκέντρωνε σημαντική αρνητική δημοσιότητα, με άμεσες επιπτώσεις στη δημόσια εικόνα και την αξιοπιστία της ΝΜ.

Αποτίμηση: Η συνέπεια από την αποκάλυψη των Δεδομένων Αιμοδοσίας σε τρίτους αποτιμάται με βαθμό **έξι (6)**, σε κλίμακα 0-10.

5.3.2. *Δεδομένα Εργαστηρίων*

Περιεχόμενο: Τα Δεδομένα Εργαστηρίων περιλαμβάνουν προσωπικά στοιχεία των νοσηλευομένων, και μη, ασθενών που έχουν εξεταστεί από το εργαστήριο, καθώς και ευαίσθητα ιατρικά δεδομένα (π.χ. διαγνώσεις ασθενειών, αποτελέσματα εξετάσεων). Τα δεδομένα αυτά δεν περιλαμβάνουν στοιχεία που αφορούν σε μολυσματικές ασθένειες.

Σχετικό Σύστημα: Τα Δεδομένα των Εργαστηρίων τηρούνται στο σύστημα των αντίστοιχων εγκαταστάσεων κάθε Εργαστηρίου. Παράλληλα, τηρείται χειρόγραφο αρχείο Εργαστηρίων, στο οποίο φυλάσσονται παραπεμπτικά από κλινικές και αναλύσεις των εργαστηρίων. Μέρος των στοιχείων αυτών καταστρέφεται έπειτα από τη χρήση τους, ενώ τα βιβλία που τηρούνται αποθηκεύονται στο Αρχείο.

Απώλεια Διαθεσιμότητας Δεδομένων Εργαστηρίων

Επιπτώσεις: Η μη διαθεσιμότητα των δεδομένων Εργαστηρίων δε θα επιφέρει σημαντικές επιπτώσεις στην ομαλή λειτουργία της ΝΜ, καθώς τηρούνται χειρόγραφα βιβλία. Επιπλέον, τα αποτελέσματα των εξετάσεων επιστρέφονται στην κλινική που τα ζήτησε και έπειτα τμήμα των δεδομένων καταστρέφεται.

Αποτίμηση: Με βάση τις παραπάνω επιπτώσεις, η συνέπεια της απώλειας διαθεσιμότητας για χρονικό διάστημα έως δύο ημέρες αποτιμάται με βαθμό **δύο (2)** και για διάστημα μιας εβδομάδος και περισσότερο με βαθμό **τρία (3)**, στην κλίμακα 0-10.

Ολική καταστροφή Δεδομένων Εργαστηρίων

Επιπτώσεις: Η ολική καταστροφή των δεδομένων, περιλαμβανομένων και των εφεδρικών αντιγράφων, συνεπάγεται την εκ νέου εισαγωγή των δεδομένων βάσει των χειρόγραφων βιβλίων, με την προϋπόθεση ότι αυτά έχουν διατηρηθεί και είναι ακέραια. Κατά συνέπεια εκτιμάται ότι το σύστημα θα υποστεί κάποια καθυστέρηση αποκατάστασης πλήρους λειτουργίας, η οποία όμως δε θα επηρεάσει σημαντικά τη λειτουργία των εργαστηρίων.

Αποτίμηση: Σύμφωνα με τις παραπάνω διαπιστώσεις η επίπτωση από την ολική καταστροφή των δεδομένων αποτιμάται με βαθμό **τρία (3)**, στην κλίμακα 0-10.

Μερική καταστροφή ή απώλεια ακεραιότητας Δεδομένων Εργαστηρίων

Επιπτώσεις: Η απώλεια των δεδομένων που έχουν εισαχθεί έπειτα από τη λήψη του τελευταίου εφεδρικού αντιγράφου συνεπάγεται την εκ νέου εισαγωγή στη βάση δεδομένων των εξετάσεων με βάση τα χειρόγραφα βιβλία. Η ύπαρξη σφαλμάτων στα δεδομένα κρίνεται περιορισμένη, καθώς τα αποτελέσματα των εξετάσεων που φυλάσσονται έχουν αποσταλεί και στην κλινική που τα ζήτησε.

Αποτίμηση: Η επίπτωση από την μερική απώλεια ακεραιότητας των δεδομένων ή την εισαγωγή λαθών σε ευρεία κλίμακα αποτιμάται με βαθμό **δύο (2)**, σε κλίμακα 0-10.

Σκόπιμη Αλλοίωση Δεδομένων Εργαστηρίων

Επιπτώσεις: Η σκόπιμη αλλοίωση των αποτελεσμάτων των εξετάσεων των εργαστηρίων μπορεί να θέσει σε κίνδυνο τη ζωή και την ασφάλεια των εξετασθέντων, καθώς τα αποτελέσματα των εξετάσεων λαμβάνονται υπόψη για την ιατρική παρακολούθηση των ασθενών. Κατ' επέκταση, μια επιτυχής σκόπιμη αλλοίωση αυτών των δεδομένων ενδέχεται να βλάψει την ασφάλεια των ασθενών της ΝΜ.

Αποτίμηση: Σύμφωνα με το παραπάνω σενάριο η συνέπεια σκόπιμης αλλοίωσης αποτιμάται με βαθμό **πέντε (5)**, σε κλίμακα 0-10.

Αποκάλυψη Δεδομένων Εργαστηρίων

Επιπτώσεις: Τα Δεδομένα Εργαστηρίων αποτελούν ευαίσθητα προσωπικά δεδομένα. Ενδεχόμενη αποκάλυψή τους αποτελεί παράβαση του Ν. 4624/2019 και επιφέρει ποινικές κυρώσεις. Ο νόμος 4624/2019 προβλέπει σημαντικά χρηματικά πρόστιμα. Επιπλέον το ΝΜ θα συγκέντρωνε σημαντική αρνητική δημοσιότητα, με άμεσες επιπτώσεις στη δημόσια εικόνα και την αξιοπιστία του.

Αποτίμηση: Η επίπτωση της αποκάλυψης σε τρίτους των δεδομένων υγείας των ασθενών αποτιμάται με βαθμό **έξι (6)** σε κλίμακα 0-10.

5.3.3. *Δεδομένα Φαρμακείου*

Περιεχόμενο: Τα δεδομένα αυτά περιλαμβάνουν τα λογιστικής φύσεως στοιχεία (περιγραφή, ποσότητα παραγγελιών και παραλαβών) των φαρμάκων που φυλάσσονται στο φαρμακείο και διατίθενται στις κλινικές, κατόπιν συγκεντρωτικών παραγγελιών. Παράλληλα, περιλαμβάνουν και τα ευαίσθητα προσωπικά δεδομένα εξωτερικών ασθενών, ατόμων με εξάρτηση σε ναρκωτικές ουσίες ή απόρων, στους οποίους διατίθενται φάρμακα κατόπιν συνταγοδότησης. Ακόμη, τα προσωπικά στοιχεία ασθενών όταν χορηγούνται ειδικά αντιβιοτικά και φάρμακα που δεν καλύπτονται από τα ασφαλιστικά ταμεία (φάρμακα εκτός κλειστού νοσηλίου). Επιπλέον, τα δεδομένα αυτής της ομάδας περιλαμβάνουν

τα προσωπικά στοιχεία των ασθενών για τους οποίους γίνεται παραγγελία άλλων υλικών πλην των φαρμάκων (π.χ. υλικά για ορθοπεδικές εγχειρήσεις).

Σχετικό Σύστημα: Τα Δεδομένα Φαρμακείου τηρούνται στην *εφαρμογή Φαρμακείου* στο *κεντρικό σύστημα διαχείρισης,* που στεγάζεται στις εγκαταστάσεις του Τμήματος Πληροφορικής *(Computer Room)*, στο υπόγειο της ΝΜ. Ακόμα, τα πρωτότυπα έντυπα συνταγών φυλάσσονται σε φυσικό αρχείο το οποίο βρίσκεται στο τμήμα του Φαρμακείου.

Απώλεια Διαθεσιμότητας Δεδομένων Φαρμακείου

Επιπτώσεις: Η μη διαθεσιμότητα των δεδομένων του Φαρμακείου δε θα επιφέρει σημαντικές επιπτώσεις στην ομαλή λειτουργία του φαρμακείου και κατ' επέκταση στην άμεση διάθεση φαρμάκων στις κλινικές και τους ασθενείς, καθώς γίνεται χρήση χειρόγραφων παραστατικών. Δευτερογενή προβλήματα ανακύπτουν αν το διάστημα μη διαθεσιμότητας του συστήματος είναι μεγαλύτερο της μιας ημέρας, καθώς δεν καθίσταται δυνατή η ενημέρωση των αποθεμάτων της αποθήκης και η διαχείρισή τους.

Αποτίμηση: Η συνέπεια της μη διαθεσιμότητας των στοιχείων αυτών αποτιμάται για διάστημα έως μια ημέρα με βαθμό **δύο (2)** και για διάστημα πλέον της μίας ημέρας με βαθμό **πέντε (5)**, σε κλίμακα 0-10.

Ολική καταστροφή Δεδομένων Φαρμακείου

Επιπτώσεις: Η ολική καταστροφή των δεδομένων, περιλαμβανομένων και των εφεδρικών αντιγράφων, συνεπάγεται την εκ νέου εισαγωγή των δεδομένων βάσει απογραφής των αποθεμάτων της αποθήκης. Κατά συνέπεια εκτιμάται ότι θα υπάρξει κόστος που σχετίζεται με τις ανθρωποώρες που απαιτούνται για την εισαγωγή των δεδομένων. Επίσης, κατά τη διάρκεια της αναγκαίας εργασίας αποκατάστασης των δεδομένων, δε θα είναι δυνατή η κανονική ροή της εργασίας των χρηστών.

Αποτίμηση: Σύμφωνα με τις παραπάνω επιπτώσεις η επίπτωση από την ολική καταστροφή των δεδομένων του Φαρμακείου αποτιμάται με βαθμό **τέσσερα (4)** στην κλίμακα 0-10.

Μερική καταστροφή ή απώλεια ακεραιότητας Δεδομένων Φαρμακείου

Επιπτώσεις: Η απώλεια των δεδομένων που έχουν εισαχθεί έπειτα από τη λήψη του τελευταίου εφεδρικού αντιγράφου συνεπάγεται την εκ νέου εισαγωγή των δεδομένων με βάση πρωτογενή παραστατικά-τιμολόγια και επιφέρει κόστος που προκύπτει από τον απαιτούμενο χρόνο επανεισαγωγής των δεδομένων και τις αντίστοιχες ανθρωποώρες. Σημαντικότερες επιπτώσεις ανακύπτουν όταν στα δεδομένα έχουν εισαχθεί λάθη. Τα λάθη αυτά μπορεί να επιφέρουν οικονομικές επιπτώσεις για το ΝΜ ή λαθεμένη εκτίμηση αποθέματος κάποιου φαρμάκου και ενδεχομένως έλλειψή του.

Αποτίμηση: Η επίπτωση από την απώλεια ακεραιότητας των δεδομένων αποτιμάται με βαθμό **δύο (2)** για τη μερική απώλεια των δεδομένων, με βαθμό

τρία (3) για την περίπτωση περιορισμένης ύπαρξης λαθών και με βαθμό **πέντε (5)** για την περίπτωση εισαγωγής λαθών σε ευρεία κλίμακα, σε κλίμακα 0-10.

Σκόπιμη Αλλοίωση Δεδομένων Φαρμακείου

Επιπτώσεις: Η σκόπιμη αλλοίωση των στοιχείων που αφορούν τις παραγγελίες φαρμάκων και το απόθεμα της αποθήκης μπορεί να πλήξει την εικόνα και η αξιοπιστία του Φαρμακείου και γενικότερα της ΝΜ. Παράλληλα, η έλλειψη αποθέματος συγκεκριμένων φαρμάκων (π.χ. ναρκωτικά) που θα προκύψει σε περίπτωση που το απόθεμα που αναφέρεται δεν είναι σωστό, μπορεί να οδηγήσει σε πολύ σημαντικές επιπτώσεις στην υγεία ενός ή περισσότερων ασθενών όταν η χορήγηση του φαρμάκου κρίνεται άμεση.

Αποτίμηση: Σύμφωνα με το παραπάνω σενάριο η συνέπεια σκόπιμης αλλοίωσης των δεδομένων Φαρμακείου αποτιμάται με βαθμό **έξι (6)**, σε κλίμακα 0-10.

Αποκάλυψη Δεδομένων Φαρμακείου

Επιπτώσεις: Τα Δεδομένα Φαρμακείου περιλαμβάνουν οικονομικά στοιχεία, τα οποία γενικά θεωρούνται εμπιστευτικής φύσεως και συγκεντρώνουν επιχειρηματικό και οικονομικό ενδιαφέρον. Η αποκάλυψή τους σε τρίτους (π.χ. φαρμακευτικές εταιρίες) θα μπορούσε να έχει οικονομικό, εμπορικό ή άλλο όφελος για αυτούς. Παράλληλα, περιλαμβάνουν και ευαίσθητα προσωπικά δεδομένα ασθενών, των οποίων ενδεχόμενη αποκάλυψη αποτελεί σοβαρή παράβαση του Ν. 4624/2019 και επιφέρει ποινικές κυρώσεις.

Αποτίμηση: Σύμφωνα με τα παραπάνω, η επίπτωση της αποκάλυψης των στοιχείων αυτών σε τρίτους αποτιμάται με βαθμό **έξι (6)** σε κλίμακα 0-10.

5.3.4. *Δεδομένα Προσωπικού*

Περιεχόμενο: Τα Δεδομένα Προσωπικού περιλαμβάνουν προσωπικά δεδομένα που αφορούν τους εργαζόμενους στο ΝΜ και την επαγγελματική τους θέση, αλλά και στοιχεία μακροχρόνιων αναρρωτικών αδειών των εργαζομένων, χωρίς να αναφέρεται η πάθηση. Ακόμη, τα δεδομένα αυτής της ομάδας περιλαμβάνουν ευαίσθητα προσωπικά στοιχεία που αφορούν στο ποινικό μητρώο του κάθε υπαλλήλου.

Σχετικό Σύστημα: Τα Δεδομένα Προσωπικού τηρούνται στην *εφαρμογή Προσωπικού* που στεγάζεται στις εγκαταστάσεις του Τμήματος Πληροφορικής *(Computer Room)*, στο υπόγειο της ΝΜ. Επιπλέον, όλες οι σχετικές πληροφορίες (π.χ. προσωπικά στοιχεία και ποινικό μητρώο) φυλάσσονται σε έντυπα σε φυσικό αρχείο το οποίο βρίσκεται στο Τμήμα Προσωπικού στο ισόγειο των κεντρικών κτηριακών εγκαταστάσεων της ΝΜ.

Απώλεια Διαθεσιμότητας Δεδομένων Προσωπικού

Επιπτώσεις: Η μη διαθεσιμότητα των στοιχείων αυτών δε θα δυσχεράνει ιδιαίτερα την εργασία του τμήματος Προσωπικού και τη ομαλή λειτουργία του. Η μη διαθεσιμότητα των δεδομένων του Προσωπικού δε θα επιφέρει σημαντικές

επιπτώσεις στην ομαλή λειτουργία του τμήματος, καθώς γίνεται χρήση των χειρόγραφων φακέλων.

Αποτίμηση: Η επίπτωση της απώλειας διαθεσιμότητας των δεδομένων αυτών αποτιμάται με βαθμό **τρία (3)** για διάστημα έως μία ημέρα και με βαθμό **πέντε (5)** για διάστημα μιας εβδομάδος και πλέον, σε κλίμακα 0-10.

Ολική καταστροφή Δεδομένων Προσωπικού

Επιπτώσεις: Η ολική καταστροφή των Δεδομένων Προσωπικού, περιλαμβανομένων και των εφεδρικών αντιγράφων, συνεπάγεται την εκ νέου εισαγωγή των δεδομένων στην εφαρμογή, βάσει των πρωτογενών παραστατικών που τηρούνται στο φυσικό αρχείο Προσωπικού. Κατά συνέπεια εκτιμάται ότι θα υπάρξει οικονομικό κόστος που αφορά τις ανθρωποώρες που απαιτούνται για την εισαγωγή των δεδομένων.

Αποτίμηση: Η επίπτωση του ενδεχομένου ολικής καταστροφής των στοιχείων αποτιμάται με βαθμό **πέντε (5)**, σε κλίμακα 0-10.

Απώλεια Μερικής Ακεραιότητας Δεδομένων Προσωπικού

- **Επιπτώσεις:** Η απώλεια των δεδομένων που έχουν εισαχθεί έπειτα από τη λήψη του τελευταίου εφεδρικού αντιγράφου, ή η εισαγωγή σφαλμάτων στα δεδομένα, συνεπάγεται την εκ νέου εισαγωγή τους. Σημαντική επίπτωση προκύπτει από τη λανθασμένη εισαγωγή στοιχείων ποινικού μητρώου, που μπορεί να επηρεάσει την επαγγελματική εξέλιξη των εργαζομένων. Άλλη επίπτωση σε αυτήν την περίπτωση αφορά στο κόστος που προκύπτει από τον απαιτούμενο χρόνο επανεισαγωγής και τις αντίστοιχες ανθρωποώρες.
- **Αποτίμηση:** Η συνέπεια από απώλεια της ακεραιότητας των δεδομένων σύμφωνα με τα παραπάνω αποτιμάται με βαθμό **τρία (3)** για την περίπτωση εισαγωγής λαθών σε μικρή κλίμακα και με βαθμό **πέντε (5)** για τις περιπτώσεις μερικής απώλειας και εισαγωγής εκτεταμένων λαθών, σε κλίμακα 0-10.

Σκόπιμη Αλλοίωση Δεδομένων Προσωπικού

Επιπτώσεις: Η σκόπιμη αλλοίωση των δεδομένων του Προσωπικού της ΝΜ θα είχε ως αποτέλεσμα ίδιο οικονομικό ή άλλο όφελος για το άτομο που πραγματοποίησε την αλλοίωση. Όφελος από τη σκόπιμη αλλοίωση των δεδομένων του Προσωπικού θα μπορούσε να έχει άτομο που δε διαθέτει λευκό ποινικό μητρώο.

Αποτίμηση: Σύμφωνα με το παραπάνω σενάριο η συνέπεια σκόπιμης αλλοίωσης των στοιχείων του Προσωπικού αποτιμάται με βαθμό **πέντε (5)** σε κλίμακα 0-10.

Αποκάλυψη Δεδομένων Προσωπικού

Επιπτώσεις: Η αποκάλυψη των προσωπικών δεδομένων των εργαζομένων σε άλλους εργαζομένους ή τρίτους, θα είχε ως συνέπεια προσωπικά, οικονομικά και άλλα οφέλη γι' αυτούς. Στην περίπτωση αυτή το ΝΜ θα υποστεί τις σημαντικές συνέπειες που ορίζει ο νόμος για την απώλεια της εμπιστευτικότητας των

προσωπικών στοιχείων, στις οποίες περιλαμβάνονται τόσο χρηματικά πρόστιμα όσο και ποινικές συνέπειες για τον υπεύθυνο επεξεργασίας. Καθώς όμως στα δεδομένα αυτά εντάσσονται και τα ευαίσθητα προσωπικά δεδομένα του ποινικού μητρώου κάθε εργαζομένου, η ενδεχόμενη αποκάλυψη αποτελεί σοβαρή παράβαση του Ν. 4624/2019 και θα επιφέρει ποινικές κυρώσεις.

Αποτίμηση: Η επίπτωση της αποκάλυψης των Δεδομένων Προσωπικού σε τρίτους αποτιμάται με βαθμό **έξι (6)**.

5.3.5. *Δεδομένα Μισθοδοσίας*

Περιεχόμενο: Τα δεδομένα αυτά περιλαμβάνουν και προσωπικά, αλλά κυρίως οικονομικά στοιχεία που αφορούν τους εργαζόμενους στο ΝΜ. Ακόμη, περιλαμβάνουν στοιχεία που αφορούν στις άδειες, αναρρωτικές και άλλες, που λαμβάνουν οι εργαζόμενοι καθώς και δεδομένα δανείων που λαμβάνουν εργαζόμενοι μέσω της ΝΜ.

Σχετικό Σύστημα: Τα Δεδομένα Μισθοδοσίας τηρούνται στην *εφαρμογή Μισθοδοσίας* που στεγάζεται στις εγκαταστάσεις του Τμήματος Μισθοδοσίας στο ισόγειο της ΝΜ.

Απώλεια Διαθεσιμότητας Δεδομένων Μισθοδοσίας

Επιπτώσεις: Η μη διαθεσιμότητα των στοιχείων αυτών δε θα εμποδίσει την ομαλή λειτουργία του Τμήματος Μισθοδοσίας. Η λειτουργία του τμήματος μπορεί να διεξαχθεί ομαλά αν η εφαρμογή δεν είναι διαθέσιμη για μέρες, καθώς οι μισθολογικές καταστάσεις μπορούν να συμπληρωθούν με χρήση των χειρόγραφων στοιχείων. Οι επιπτώσεις που θα προκύψουν αφορούν κυρίως τη δυσκολία έκδοσης των μισθοδοτικών καταστάσεων και τις επιπλέον ανθρωποώρες που απαιτούνται.

Αποτίμηση: Η επίπτωση της απώλειας διαθεσιμότητας των δεδομένων αυτών αποτιμάται με βαθμό **ένα (1)** για διάστημα έως μία ημέρα και με βαθμό **τρία (3)** για διάστημα μιας εβδομάδος και πλέον, σε κλίμακα 0-10.

Ολική καταστροφή Δεδομένων Μισθοδοσίας

Επιπτώσεις: Η ολική καταστροφή των Δεδομένων Μισθοδοσίας, περιλαμβανομένων και των εφεδρικών αντιγράφων, συνεπάγεται την εκ νέου εισαγωγή των δεδομένων στην εφαρμογή, βάσει των πρωτογενών παραστατικών που τηρούνται στο φυσικό αρχείο Μισθοδοσίας. Σε περίπτωση απώλειας και του φυσικού αρχείου Μισθοδοσίας, τα στοιχεία μπορεί να αντληθούν από το Τμήμα Προσωπικού. Κατά συνέπεια εκτιμάται ότι θα υπάρξει οικονομικό κόστος που αφορά τις ανθρωποώρες που απαιτούνται για την εισαγωγή των δεδομένων. Προβλήματα προκύπτουν αναφορικά με τα στοιχεία δανείων των εργαζομένων (οφειλές, δόσεις κλπ.). Κατά συνέπεια θα υπάρξει επιπλέον κόστος αποκατάστασης των στοιχείων αυτών, μέσω του αντίστοιχου πιστωτικού φορέα.

Αποτίμηση: Η επίπτωση του ενδεχομένου ολικής καταστροφής των στοιχείων αποτιμάται με βαθμό **τρία (3)**, σε κλίμακα 0-10.

Μερική Καταστροφή ή Απώλεια Ακεραιότητας Δεδομένων Μισθοδοσίας

Επιπτώσεις: Η απώλεια των δεδομένων που έχουν εισαχθεί μετά τη λήψη του τελευταίου εφεδρικού αντιγράφου συνεπάγεται την εκ νέου εισαγωγή τους. Η κύρια επίπτωση αφορά στο κόστος που προκύπτει από τον απαιτούμενο χρόνο επανεισαγωγής και τις αντίστοιχες ανθρωποώρες. Σοβαρότερες επιπτώσεις έχει η εισαγωγή σφαλμάτων στα δεδομένα, καθώς μπορεί να έχει ως συνέπεια οικονομικές απώλειες για το ΝΜ.

Αποτίμηση: Η επίπτωση από την απώλεια ακεραιότητας των δεδομένων αποτιμάται με βαθμό **ένα (1)** για τη μερική απώλεια των δεδομένων και την περιορισμένη ύπαρξη λαθών, και με βαθμό **τρία (3)** για την περίπτωση εκτεταμένων λαθών, σε κλίμακα 0-10.

Σκόπιμη Αλλοίωση Δεδομένων Μισθοδοσίας

Επιπτώσεις: Η σκόπιμη αλλοίωση των Δεδομένων Μισθοδοσίας θα είχε ως αποτέλεσμα οικονομικό ή άλλο όφελος για το άτομο που πραγματοποίησε την αλλοίωση και συνεπώς οικονομικές απώλειες για το ΝΜ. Στα πλαίσια του σεναρίου αυτού θα πρέπει να σημειωθεί ότι το ενδεχόμενο πιθανής αλλοίωσης κρίνεται περιορισμένο, καθώς οι επαναλαμβανόμενοι έλεγχοι και οι διασταυρώσεις στοιχείων που πραγματοποιούνται θα αποκαλύψουν τις ανακρίβειες.

Αποτίμηση: Σύμφωνα με το παραπάνω σενάριο η συνέπεια σκόπιμης αλλοίωσης των δεδομένων Μισθοδοσίας αποτιμάται με βαθμό **τρία (3)**, σε κλίμακα 0-10.

Αποκάλυψη Δεδομένων Μισθοδοσίας

Επιπτώσεις: Τα στοιχεία μισθοδοσίας είναι γενικά, εμπιστευτικής φύσης. Πιθανή μη- εξουσιοδοτημένη δημοσιοποίησή τους σε άλλους εργαζομένους ή τρίτους, θα είχε ως συνέπεια προσωπικά, οικονομικά και άλλα οφέλη γι' αυτούς. Στην περίπτωση αυτή το ΝΜ θα υποστεί τις συνέπειες που ορίζει ο νόμος για την απώλεια της εμπιστευτικότητας των προσωπικών στοιχείων, στις οποίες περιλαμβάνονται τόσο χρηματικά πρόστιμα όσο και ποινικές συνέπειες για τον υπεύθυνο επεξεργασίας

Αποτίμηση: Με βάση τα παραπάνω, η συνέπεια της αποκάλυψης των στοιχείων αυτών αποτιμάται με βαθμό **τρία (3)**, σε κλίμακα 0-10.

5.3.6. *Δεδομένα Προμηθευτών και Συμβάσεων*

Περιεχόμενο: Τα Δεδομένα Προμηθευτών και Συμβάσεων περιλαμβάνουν προσωπικά στοιχεία για όλους τους προμηθευτές που συνεργάζεται ή είχε συνεργαστεί το ΝΜ. Περιλαμβάνουν Επωνυμία επιχείρησης, Αριθμό Φορολογικού Μητρώου, στοιχεία διεύθυνσης κλπ. Επιπλέον, στα δεδομένα αυτά συμπεριλαμβάνονται εγγυητικές επιστολές, προκηρύξεις και προσφορές προμηθειών, καθώς και συμβάσεις προμηθειών που πραγματοποιήθηκαν.

Σχετικό Σύστημα: Τα Δεδομένα Προμηθευτών και Συμβάσεων τηρούνται σε εφαρμογές αυτοματισμού γραφείου σε τοπικούς υπολογιστές που στεγάζονται

στο Τμήμα Προμηθειών στο ισόγειο της ΝΜ. Επίσης, τα δεδομένα τηρούνται σε χειρόγραφο Φάκελο Προμηθειών, ο οποίος φυλάσσεται στον ίδιο χώρο.

Απώλεια Διαθεσιμότητας Δεδομένων Προμηθευτών και Συμβάσεων

Επιπτώσεις: Η πρόσβαση στα Δεδομένα Προμηθευτών και Συμβάσεων είναι απαραίτητη για τις οικονομικές λειτουργίες της ΝΜ (έκδοση τιμολογίων, καταχώριση συμβάσεων κλπ.). Συνεπώς, οι ανάγκες διαθεσιμότητας για τα στοιχεία αυτά προκύπτουν με βάση και την ανάγκη διαθεσιμότητας των δεδομένων συμβάσεων και των λογιστικών δεδομένων. Το Τμήμα Προμηθειών μπορεί να λειτουργήσει ομαλά στην περίπτωση που τα ηλεκτρονικά δεδομένα δεν είναι διαθέσιμα, καθώς όλα τα στοιχεία μπορούν να αντληθούν από το χειρόγραφο φάκελο.

Αποτίμηση: Με βάση τα παραπάνω, η συνέπεια από την απώλεια διαθεσιμότητας για διάστημα έως 12 ώρες αποτιμάται με βαθμό **ένα (1)** και για διάστημα μιας ημέρας και άνω με βαθμό **τρία (3)**, σε κλίμακα 0-10.

Ολική καταστροφή Δεδομένων Προμηθευτών και Συμβάσεων

Επιπτώσεις: Η ολική καταστροφή των Δεδομένων Προμηθευτών και Συμβάσεων, περιλαμβανομένων και των εφεδρικών αντιγράφων, συνεπάγεται την εκ νέου εισαγωγή των δεδομένων, βάσει πρωτογενών παραστατικών και εκτυπώσεων. Κατά συνέπεια εκτιμάται ότι θα υπάρξει κόστος που αφορά τις ανθρωποώρες που απαιτούνται για την εισαγωγή των δεδομένων.

Αποτίμηση: Με βάση τα παραπάνω, η συνέπεια από την ολική καταστροφή αποτιμάται με βαθμό **τρία (3)**, σε κλίμακα 0-10.

Μερική καταστροφή ή απώλεια ακεραιότητας Δεδομένων Προμηθευτών και Συμβάσεων

Επιπτώσεις: Η απώλεια των δεδομένων που έχουν εισαχθεί μετά τη λήψη του τελευταίου εφεδρικού αντιγράφου συνεπάγεται την εκ νέου εισαγωγή τους. Συνεπώς η κύρια επίπτωση αφορά στο κόστος που προκύπτει από τον απαιτούμενο χρόνο επανεισαγωγής και τις αντίστοιχες ανθρωποώρες. Όσον αφορά στην εισαγωγή λαθών το ΝΜ μπορεί να αντιμετωπίσει σοβαρότερες επιπτώσεις, καθώς μπορεί να υποστεί οικονομικές απώλειες από την έκδοση εσφαλμένων παραστατικών.

Αποτίμηση: Η συνέπεια της απώλειας ακεραιότητας των δεδομένων αυτών, καθώς και της περιορισμένης ύπαρξης λαθών αποτιμάται με βαθμό **ένα (1)** και της ευρείας ύπαρξης λαθών με βαθμό **τρία (3)**, σε κλίμακα 0-10.

Σκόπιμη Αλλοίωση Δεδομένων Προμηθευτών και Συμβάσεων

Επιπτώσεις: Οι επιπτώσεις από τη σκόπιμη αλλοίωση των Δεδομένων Προμηθευτών και Συμβάσεων της ΝΜ μπορεί να είναι οικονομικές, καθώς επηρεάζει τις οικονομικές συναλλαγές της ΝΜ με τρίτους.

Αποτίμηση: Επομένως η συνέπεια σκόπιμης αλλοίωσης των στοιχείων των Προμηθευτών αποτιμάται με βαθμό **πέντε (5)**, σε κλίμακα 0-10.

Αποκάλυψη Δεδομένων Προμηθευτών και Συμβάσεων και Συμβάσεων

Επιπτώσεις: Τα Δεδομένα Προμηθευτών και Συμβάσεων δε θεωρούνται γενικά εμπιστευτικής φύσεως από τους χρήστες των ΠΣ της ΝΜ και σε μερικές περιπτώσεις η αποκάλυψή τους θεωρείται επιβεβλημένη για λόγους διαφάνειας. Εντούτοις η αποκάλυψη των δεδομένων σε τρίτους θα μπορούσε να έχει οικονομικό, εμπορικό ή άλλο όφελος γι' αυτούς.

Αποτίμηση: Κατά συνέπεια η αποτίμηση της επίπτωσης αποκάλυψης των στοιχείων των Προμηθευτών σε τρίτους είναι **δύο (2)**, σε κλίμακα 0-10.

5.3.7. *Δεδομένα Λογιστηρίου*

Περιεχόμενο: Τα Δεδομένα Λογιστηρίου περιλαμβάνουν όλα τα οικονομικά στοιχεία που χειρίζεται το Λογιστήριο, δηλαδή στοιχεία ισολογισμών, τιμολογίων κλπ.

Σχετικό Σύστημα: Τα Δεδομένα Λογιστηρίου τηρούνται στην *εφαρμογή Χρηματικού* στο *κεντρικό σύστημα διαχείρισης* που στεγάζεται στις εγκαταστάσεις του Τμήματος Πληροφορικής *(Computer Room)*, στο υπόγειο της ΝΜ. Παράλληλα, τηρούνται στον ίδιο χώρο χειρόγραφα λογιστικά βιβλία, εντάλματα πληρωμών, γραμμάτια είσπραξης κλπ.

Απώλεια Διαθεσιμότητας Δεδομένων Λογιστηρίου

Επιπτώσεις: Η μη διαθεσιμότητα των στοιχείων αυτών θα εμποδίσει κυρίως την ομαλή λειτουργία του Λογιστηρίου. Το τμήμα αυτό δεν μπορεί να λειτουργήσει με χειρόγραφο τρόπο και οι εργασίες του είναι απαραίτητες για την εκπλήρωση των οικονομικών υποχρεώσεων της ΝΜ προς τρίτους ή για την ομαλή παραλαβή υλικού, τροφίμων ή φαρμάκων. Τα τελευταία είναι μείζονος σημασίας για την σωστή ιατρική περίθαλψη των ασθενών. Απώλεια διαθεσιμότητας των δεδομένων για περισσότερες από μία ημέρες θα δημιουργήσει σοβαρό πρόβλημα στην είσπραξη των γραμματίων πληρωμών και γενικά στο σύνολο των οικονομικών λειτουργιών της ΝΜ.

Αποτίμηση: Με βάση τα παραπάνω, η συνέπεια από την απώλεια διαθεσιμότητας για διάστημα μιας ώρας αποτιμάται με βαθμό **ένα (1),** για διάστημα δώδεκα ωρών με βαθμό **δύο (2)** και για διάστημα μιας ημέρας και άνω με βαθμό **πέντε (5),** σε κλίμακα 0-10.

Ολική καταστροφή Δεδομένων Λογιστηρίου

Επιπτώσεις: Η ολική καταστροφή των Λογιστικών Δεδομένων, περιλαμβανομένων και των εφεδρικών αντιγράφων, συνεπάγεται την εκ νέου εισαγωγή των δεδομένων στην εφαρμογή βάσει πρωτογενών παραστατικών. Κατά συνέπεια εκτιμάται ότι θα υπάρξει σημαντικό οικονομικό κόστος που αφορά τις ανθρωποώρες που απαιτούνται για την εισαγωγή των δεδομένων, λόγω του σημαντικού όγκου δεδομένων. Επίσης, κατά τη διάρκεια της αναγκαίας εργασίας αποκατάστασης των δεδομένων, δε θα είναι δυνατή η ομαλή λειτουργία του λογιστηρίου και η ικανοποίηση των οικονομικών υποχρεώσεων

της ΝΜ προς τους ενδιαφερόμενους, γεγονός που θα έχει σημαντικές επιπτώσεις στην ευρύτερη λειτουργία της ΝΜ.

Αποτίμηση: Η συνέπεια από την ολική καταστροφή αποτιμάται με βαθμό **έξι (6)**, σε κλίμακα 0-10.

Μερική καταστροφή ή απώλεια ακεραιότητας Δεδομένων Λογιστηρίου

Επιπτώσεις: Η απώλεια των λογιστικών στοιχείων που έχουν εισαχθεί μετά τη λήψη του τελευταίου εφεδρικού αντιγράφου ή η ύπαρξη σφαλμάτων συνεπάγεται την εκ νέου εισαγωγή τους. Η κύρια επίπτωση αφορά στο κόστος που προκύπτει από τον απαιτούμενο χρόνο επαναεισαγωγής και τις αντίστοιχες ανθρωποώρες. Παράλληλα, η εισαγωγή σφαλμάτων στα δεδομένα μπορεί να έχει σοβαρότερες επιπτώσεις, καθώς μπορεί να προκαλέσει ασήμαντες ή σημαντικές οικονομικές απώλειες για το ΝΜ.

Αποτίμηση: Η συνέπεια της απώλειας ακεραιότητας των Λογιστικών Δεδομένων αποτιμάται με βαθμό **τρία (3)**, η περιορισμένη ύπαρξη λαθών αποτιμάται με βαθμό **δύο (2)**, ενώ η ευρεία ύπαρξη λαθών με βαθμό **τέσσερα (4)**, σε κλίμακα 0-10.

Σκόπιμη Αλλοίωση Δεδομένων Λογιστηρίου

Επιπτώσεις: Η σκόπιμη αλλοίωση των Λογιστικών Δεδομένων επηρεάζει τις οικονομικές συναλλαγές της ΝΜ με τρίτους και μπορεί να έχει ως αποτέλεσμα σοβαρές οικονομικές επιπτώσεις για το ΝΜ.

Αποτίμηση: Σύμφωνα με τα παραπάνω η συνέπεια σκόπιμης αλλοίωσης των στοιχείων αυτών αποτιμάται με βαθμό **πέντε (5)**, σε κλίμακα 0-10.

Αποκάλυψη Δεδομένων Λογιστηρίου

Επιπτώσεις: Το ΝΜ είναι ένα δημόσιο νοσοκομείο, οπότε τα Λογιστικά Δεδομένα δεν θεωρούνται εμπιστευτικής φύσεως και απαιτείται να είναι διαθέσιμα σε νομίμως αιτούντες για λόγους διαφάνειας. Επειδή η πρόσβαση στα δεδομένα αυτά επιτρέπει και τη διάθεση κάποιων προσωπικών δεδομένων των προμηθευτών, η αποκάλυψη τους μπορεί να έχει πολύ μικρές επιπτώσεις στη σχέση της ΝΜ με τους προμηθευτές, χωρίς όμως να υπάρχουν νομικές κυρώσεις.

Αποτίμηση: Κατά συνέπεια η αποτίμηση της επίπτωσης αποκάλυψης των Λογιστικών στοιχείων είναι **ένα (1)**, σε κλίμακα 0-10.

5.3.8. *Δεδομένα Επισκέψεων στα Εξωτερικά Ιατρεία*

Περιεχόμενο: Τα Δεδομένα Επισκέψεων στα Εξωτερικά Ιατρεία είναι τα στοιχεία που τηρούνται από τη γραμματεία Εξωτερικών Ιατρείων για τον προγραμματισμό επισκέψεων των ασθενών στα εξωτερικά ιατρεία της ΝΜ. Τα στοιχεία αυτά περιλαμβάνουν τα στοιχεία του ασθενούς, τη διάγνωση και την κλινική την οποία θα επισκεφτούν. Επίσης, τηρούνται στοιχεία που είναι απαραίτητα για την οικονομική τακτοποίηση των παρακλινικών εξετάσεων εξωτερικών ασθενών από τα ασφαλιστικά ταμεία.

Σχετικό Σύστημα: Ο προγραμματισμός των επισκέψεων γίνεται από την *εφαρμογή της Γραμματείας Εξωτερικών Ιατρείων* στο *κεντρικό σύστημα διαχείρισης* που στεγάζεται στις εγκαταστάσεις του Τμήματος Πληροφορικής *(Computer Room)*. Χειρόγραφα στοιχεία που τηρούνται αφορούν στις καθημερινές λίστες ραντεβού για όλες τις ειδικότητες.

Απώλεια Διαθεσιμότητας Δεδομένων Επισκέψεων στα Εξωτερικά Ιατρεία

Επιπτώσεις: Η μη διαθεσιμότητα των Δεδομένων Επισκέψεων θα καταστήσει αδύνατο τον προγραμματισμό επισκέψεων και θα εμποδίσει την ομαλή λειτουργία της Γραμματείας Εξωτερικών Ιατρείων. Οι καθυστερήσεις που θα προκύψουν θα έχουν σημαντική επίπτωση στην εξυπηρέτηση των ασθενών, προκαλώντας έντονη δυσαρέσκεια και πλήττοντας την αξιοπιστία και τη δημόσια εικόνα της ΝΜ προς τους ασθενείς του και το κοινό. Ταυτόχρονα, θα προκληθεί καθυστέρηση είσπραξης των χρημάτων παρακλινικών εξετάσεων της ΝΜ από τα ασφαλιστικά ταμεία.

Αποτίμηση: Με βάση τα παραπάνω, η συνέπεια από την απώλεια διαθεσιμότητας για διάστημα μιας ώρας αποτιμάται με βαθμό **ένα (1)**, για διάστημα δώδεκα ωρών με βαθμό **τρία (3)** και για διάστημα μιας ημέρας και άνω με βαθμό **πέντε (5)**, σε κλίμακα 0-10.

Ολική καταστροφή Δεδομένων Επισκέψεων στα Εξωτερικά Ιατρεία

Επιπτώσεις: Η ολική καταστροφή των δεδομένων των επισκέψεων θα έχει σημαντικές επιπτώσεις, καθώς δε θα είναι άμεσα δυνατή η πραγματοποίηση επισκέψεων σε εξωτερικά ιατρεία, γεγονός που επηρεάζει τη γενικότερη λειτουργία της ΝΜ και την παροχή υπηρεσιών υγείας στους ασθενείς. Σημαντική επίπτωση επίσης αφορά στην είσπραξη των χρημάτων παρακλινικών εξετάσεων, γεγονός που συνεπάγεται οικονομικό κόστος της ΝΜ. Δευτερεύουσες συνέπειες είναι η καθυστέρηση στην έκδοση πιστοποιητικών, αλλά και το σημαντικό κόστος που απαιτείται για την επανεισαγωγή των δεδομένων των επισκέψεων, λόγω του μεγάλου όγκου του αρχείου των επισκέψεων, καθώς επίσης και η αρνητική επίπτωση στη καλή φήμη και δημόσια εικόνα του Νοσοκομείου.

Αποτίμηση: Η συνέπεια από την ολική καταστροφή αποτιμάται με βαθμό **πέντε (5)**, σε κλίμακα 0-10.

Μερική καταστροφή ή απώλεια ακεραιότητας Δεδομένων Επισκέψεων σε Εξωτερικά Ιατρεία

Επιπτώσεις: Η απώλεια των στοιχείων των ραντεβού που έχουν εισαχθεί μετά τη λήψη του τελευταίου εφεδρικού αντιγράφου ή η ύπαρξη σφαλμάτων δημιουργεί προβλήματα στην πραγματοποίηση επισκέψεων στα εξωτερικά ιατρεία. Η κύρια επίπτωση αφορά στη μη εξυπηρέτηση των ασθενών που επισκέπτονται το ΝΜ και στα προβλήματα που θα δημιουργηθούν στη σχέση του νοσοκομείου με αυτούς. Επιπλέον, τυχόν λάθη στα στοιχεία παρακλινικών εξετάσεων θα οδηγήσουν σε οικονομικό κόστος της ΝΜ.

Αποτίμηση: Η συνέπεια της απώλειας ακεραιότητας, καθώς και της περιορισμένης ύπαρξης λαθών αποτιμάται με βαθμό **τρία (3)** και της ευρείας ύπαρξης λαθών με βαθμό **πέντε (5)**, σε κλίμακα 0-10.

Σκόπιμη Αλλοίωση Δεδομένων Επισκέψεων στα Εξωτερικά Ιατρεία

Επιπτώσεις: Οι επιπτώσεις από τη σκόπιμη αλλοίωση των δεδομένων είναι ανάλογες με την ύπαρξη εκτεταμένων σφαλμάτων, καθώς δυσχεραίνεται η ομαλή λειτουργία της γραμματείας και των εξωτερικών ιατρείων, με αντίκτυπο στην ιατρική εξυπηρέτηση των ασθενών της ΝΜ και στην εικόνα του νοσοκομείου.

Αποτίμηση: Σύμφωνα με τα παραπάνω η συνέπεια σκόπιμης αλλοίωσης των Επισκέψεων στα Εξωτερικά Ιατρεία αποτιμάται με βαθμό **πέντε (5)**, σε κλίμακα 0-10.

Αποκάλυψη Δεδομένων Επισκέψεων στα Εξωτερικά Ιατρεία

Επιπτώσεις: Στην εφαρμογή της Γραμματείας Εξωτερικών Ιατρείων δεν καταγράφονται στοιχεία, όπως η διάγνωση του ασθενούς, ενώ τα αναλυτικότερα στοιχεία της επίσκεψης του ασθενούς στα Εξωτερικά Ιατρεία καταγράφονται στη χειρόγραφη καρτέλα ασθενούς που φυλάσσεται στην κλινική και το γραφείου του ιατρού τον οποίο επισκέφτηκε. Καθώς, όμως, το αρχείο περιέχει τις επισκέψεις ενός ασθενούς σε κάποιο ιατρείο και συγκεκριμένη ειδικότητα για σημαντικό βάθος χρόνου, είναι δυνατή η εξαγωγή συμπερασμάτων για ευαίσθητα προσωπικά δεδομένα του ασθενούς, η αποκάλυψη των οποίων επιδέχεται νομικές κυρώσεις. Τέλος, η αποκάλυψη των δεδομένων που περιέχει η εφαρμογή δε επιδέχεται νομικές κυρώσεις.

Αποτίμηση: Κατά συνέπεια η αποτίμηση της επίπτωσης αποκάλυψης των Δεδομένων Επισκέψεων είναι **τέσσερα (4)**, σε κλίμακα 0-10.

5.3.9. *Δεδομένα Νοσηλίων*

Περιεχόμενο: Τα Δεδομένα Νοσηλίων περιλαμβάνουν όλα τα δεδομένα, προσωπικά και ευαίσθητα, ιατρικής φύσεως, που απαιτούνται για την οικονομική συναλλαγή της ΝΜ με τα ασφαλιστικά ταμεία, δηλαδή για την κάλυψη του κόστους νοσηλείας από τους ασφαλιστικούς φορείς.

Σχετικό Σύστημα: Τα Δεδομένα Νοσηλίων τηρούνται από το *κεντρικό σύστημα διαχείρισης* που στεγάζεται στις εγκαταστάσεις του Τμήματος Πληροφορικής *(Computer Room)*, στο υπόγειο της ΝΜ, και χρησιμοποιούνται από το γραφείο Νοσηλίων. Παράλληλα, τηρείται και χειρόγραφο αρχείο Ασθενών που φυλάσσεται στο χώρο του γραφείου.

Απώλεια Διαθεσιμότητας Δεδομένων Νοσηλίων

Επιπτώσεις: Τα Δεδομένα Νοσηλίων δεν είναι δεδομένα με υψηλές απαιτήσεις διαθεσιμότητας, καθώς συνήθως δεν υπάρχουν ιδιαίτερα βραχυπρόθεσμοι περιορισμοί στην απαίτηση είσπραξης νοσηλίων από τα ασφαλιστικά ταμεία.

Συνεπώς η απώλεια διαθεσιμότητας του συστήματος δε θα δημιουργούσε σημαντικά προβλήματα στη λειτουργία του γραφείου Νοσηλίων.

Αποτίμηση: Με βάση τα παραπάνω, η συνέπεια από την απώλεια διαθεσιμότητας για διάστημα έως δώδεκα ωρών αποτιμάται με βαθμό **ένα (1)**, για διάστημα μιας ημέρας με βαθμό **δύο (2)** και για διάστημα μιας εβδομάδος και άνω με βαθμό **πέντε (5)**, σε κλίμακα 0-10.

Ολική καταστροφή Δεδομένων Νοσηλίων

Επιπτώσεις: Στην περίπτωση ολικής καταστροφής των Δεδομένων Νοσηλίων το ΝΜ θα αντιμετωπίσει οικονομικές κυρίως επιπτώσεις, καθώς δε θα μπορέσει να θέσει εμπρόθεσμα τις οικονομικές απαιτήσεις του στα ασφαλιστικά ταμεία. Παράλληλα, θα υποστεί σημαντικό κόστος για την επανεισαγωγή των στοιχείων από το μεγάλου όγκου χειρόγραφο αρχείο, υπό την προϋπόθεση ότι το τελευταίο φυλάσσεται σε άρτια κατάσταση.

Αποτίμηση: Η συνέπεια από την ολική καταστροφή αποτιμάται με βαθμό **τέσσερα (4)**, σε κλίμακα 0-10.

Μερική καταστροφή ή απώλεια ακεραιότητας Δεδομένων Νοσηλίων

Επιπτώσεις: Η απώλεια των δεδομένων που έχουν εισαχθεί μετά τη λήψη του τελευταίου εφεδρικού αντιγράφου συνεπάγεται την εκ νέου εισαγωγή τους. Συνεπώς, η κύρια επίπτωση αφορά στο κόστος που προκύπτει από τον απαιτούμενο χρόνο επανεισαγωγής και τις αντίστοιχες ανθρωποώρες. Όσον αφορά στην εισαγωγή εκτεταμένων λαθών το ΝΜ μπορεί να αντιμετωπίσει σοβαρότερες επιπτώσεις, λόγω της οικονομικής φύσεως των δεδομένων. Συνεπώς, η εισαγωγή σφαλμάτων σε μικρή ή μεγαλύτερη κλίμακα, μπορεί να έχει ως αποτέλεσμα οικονομικές απώλειες για το ΝΜ.

Αποτίμηση: Η συνέπεια της απώλειας ακεραιότητας αποτιμάται με βαθμό **δύο (2)**, της περιορισμένης ύπαρξης λαθών με βαθμό **ένα (1)** και της ευρείας ύπαρξης λαθών με βαθμό **τρία (3)**, σε κλίμακα 0-10.

Σκόπιμη Αλλοίωση Δεδομένων Νοσηλίων

Επιπτώσεις: Η σκόπιμη αλλοίωση των Δεδομένων Νοσηλίων θα είχε ως αποτέλεσμα οικονομικό ή άλλο όφελος για το άτομο που πραγματοποίησε την αλλοίωση και συνεπώς οικονομικές απώλειες για το ΝΜ.

Αποτίμηση: Σύμφωνα με τα παραπάνω η συνέπεια σκόπιμης αλλοίωσης των στοιχείων αυτών αποτιμάται με βαθμό **τέσσερα (4)**, σε κλίμακα 0-10.

Αποκάλυψη Δεδομένων Νοσηλίων

Επιπτώσεις: Τα δεδομένα που απαιτούνται για την είσπραξη των νοσηλίων εμπεριέχουν και ευαίσθητα προσωπικά δεδομένα, οπότε υφίσταται ζήτημα εμπιστευτικότητας. Δεδομένου όμως ότι τα στοιχεία αυτά είναι πολύ περιορισμένα σε έκταση, εκτιμάται ότι το ΝΜ θα αντιμετωπίσει ήπιες κυρώσεις από την αποκάλυψη τους.

Αποτίμηση: Κατά συνέπεια η αποτίμηση της επίπτωσης αποκάλυψης των δεδομένων αυτών σε τρίτους είναι **τρία (3)**, σε κλίμακα 0-10.

5.3.10. *Δεδομένα Κίνησης Ασθενών*

Περιεχόμενο: Τα Δεδομένα Κίνησης Ασθενών περιλαμβάνουν προσωπικά και ευαίσθητα προσωπικά δεδομένα ασθενών, καθώς στο σύστημα εισάγονται, εκτός από προσωπικά στοιχεία του ασθενούς, και ιατρικές πληροφορίες, όπως η διάγνωση εισόδου και εξόδου.

Σχετικό Σύστημα: Τα Δεδομένα Κίνησης Ασθενών τηρούνται από το *κεντρικό σύστημα διαχείρισης* που στεγάζεται στις εγκαταστάσεις του Τμήματος Πληροφορικής και Οργάνωσης, στο υπόγειο της ΝΜ και χρησιμοποιούνται από το γραφείο Κίνησης. Παράλληλα, τηρούνται χειρόγραφοι Φάκελοι Ασθενών από τους ιατρούς, οι οποίοι περιλαμβάνουν ευαίσθητα ιατρικά δεδομένα και φυλάσσονται στα αντίστοιχα γραφεία του κάθε ιατρού.

Απώλεια Διαθεσιμότητας Δεδομένων Κίνησης Ασθενών

Επιπτώσεις: Η μη διαθεσιμότητα των Δεδομένων Κίνησης Ασθενών δημιουργεί προβλήματα κυρίως σε σχέση με την επικοινωνία του γραφείου με τους ασθενείς. Ακόμη και μικρά χρονικά διαστήματα μη διαθεσιμότητας μπορεί να δημιουργήσουν έντονη δυσαρέσκεια στο κοινό και να πλήξουν την εικόνα του νοσοκομείου. Παράλληλα, μη διαθεσιμότητα των Δεδομένων Κίνησης Ασθενών θα εμποδίσει την έκδοση πιστοποιητικών Νοσηλείας και την είσπραξη των Νοσηλίων από τα ασφαλιστικά ταμεία, γεγονός που δημιουργεί προβλήματα στην ομαλή λειτουργία των οικονομικών συναλλαγών της ΝΜ. Μεγαλύτερες καθυστερήσεις δημιουργούν προβλήματα στη γενικότερη λειτουργία του νοσοκομείου, καθώς δεν είναι δυνατή η παρακολούθηση των εισαγωγών ασθενών ή η έκδοση εξιτηρίων.

Αποτίμηση: Με βάση τα παραπάνω, η συνέπεια από την απώλεια διαθεσιμότητας για διάστημα μιας ώρας αποτιμάται με βαθμό **ένα (1)**, για διάστημα δώδεκα ωρών με βαθμό **τρία (3)** και για διάστημα μίας ημέρας και άνω με βαθμό **πέντε (5)**, σε κλίμακα 0-10.

Ολική καταστροφή Δεδομένων Κίνησης Ασθενών

Επιπτώσεις: Στην περίπτωση ολικής καταστροφής των Δεδομένων Κίνησης Ασθενών το ΝΜ θα υποστεί σημαντικό κόστος για την επανεισαγωγή των στοιχείων από το μεγάλου όγκου χειρόγραφο αρχείο, υπό την προϋπόθεση ότι το τελευταίο φυλάσσεται σε άρτια κατάσταση. Παράλληλα, δε θα είναι δυνατή η ομαλή λειτουργία του γραφείου Κίνησης Ασθενών, το οποίο αποτελεί κρίσιμο σημείο επικοινωνίας του νοσοκομείου με τους νοσηλευόμενους και επηρεάζει σε σημαντικό βαθμό τη λειτουργία και υπόλοιπων τμημάτων του νοσοκομείου, όπως τις κλινικές. Επιπλέον, οικονομικές επιπτώσεις της ΝΜ προκύπτουν σχετικά με την είσπραξη των Νοσηλίων από τα ασφαλιστικά Ταμεία.

Αποτίμηση: Σύμφωνα με το παραπάνω σενάριο, η συνέπεια από την ολική καταστροφή αποτιμάται με βαθμό **πέντε (5)**, σε κλίμακα 0-10.

Μερική καταστροφή ή απώλεια ακεραιότητας Δεδομένων Κίνησης Ασθενών

Επιπτώσεις: Σε περιπτώσεις μερικής απώλειας ή εισαγωγής σφαλμάτων καταστροφής στα Δεδομένα Νοσηλευόμενων, η συνέπεια περιορίζεται στο κόστος για την επανεισαγωγή των στοιχείων από το χειρόγραφο αρχείο, υπό την προϋπόθεση ότι το τελευταίο φυλάσσεται σε άρτια κατάσταση. Παράλληλα, κατά τη διάρκεια επανεισαγωγής των δεδομένων δυσχεραίνεται η ομαλή λειτουργία του γραφείου Κίνησης Ασθενών, καθώς οι εργασίες του θα χρειαστεί να διεκπεραιώνονται χειρόγραφα.

Αποτίμηση: Η συνέπεια της περιορισμένης ύπαρξης λαθών αποτιμάται με βαθμό **ένα (1)** και της απώλειας ακεραιότητας του, καθώς και της ευρείας ύπαρξης λαθών με βαθμό **τρία (3)**, σε κλίμακα 0-10.

Σκόπιμη Αλλοίωση Δεδομένων Κίνησης Ασθενών

Επιπτώσεις: Οι επιπτώσεις από τη σκόπιμη αλλοίωση των Δεδομένων Κίνησης Ασθενών της ΝΜ θα μπορούσε να προσδώσει προσωπικό, οικονομικό ή άλλο όφελος στο άτομο που θα πραγματοποιούσε την αλλοίωση και να δυσχεραίνει την ομαλή λειτουργία του γραφείου Κίνησης.

Αποτίμηση: Σύμφωνα με τα παραπάνω η συνέπεια σκόπιμης αλλοίωσης των στοιχείων αυτών αποτιμάται με βαθμό **τρία (3)**, σε κλίμακα 0-10.

Αποκάλυψη Δεδομένων Κίνησης Ασθενών

Επιπτώσεις: Τα Δεδομένα Κίνησης Ασθενών αποτελούν ευαίσθητα προσωπικά δεδομένα. Ενδεχόμενη αποκάλυψή τους αποτελεί παράβαση του Ν. 4624/2019 και επιφέρει ποινικές κυρώσεις. Ο νόμος 4624/2019 προβλέπει σημαντικά χρηματικά πρόστιμα, καθώς και ποινές φυλάκισης για τον υπεύθυνο επεξεργασίας που δε συμμορφώνεται, οι οποίες φτάνουν μέχρι τα δέκα έτη σε εξαιρετικές περιπτώσεις. Επιπλέον το ΝΜ θα συγκέντρωνε σημαντική αρνητική δημοσιότητα, με άμεσες επιπτώσεις στη δημόσια εικόνα και την αξιοπιστία του.

Αποτίμηση: Κατά συνέπεια η αποτίμηση της επίπτωσης αποκάλυψης των στοιχείων αυτών σε τρίτους είναι **έξι (6)**.

5.3.11. *Δεδομένα Επικοινωνίας*

Περιεχόμενο: Τα Δεδομένα περιλαμβάνουν όλα τα δεδομένα που ανταλλάσσουν οι εργαζόμενοι της ΝΜ μεταξύ τους ή με τρίτους μέσω ηλεκτρονικού ταχυδρομείου, καθώς και όλα τα δεδομένα που προκύπτουν από την περιήγηση των εργαζομένων σε ιστοσελίδες του Διαδικτύου και την αποθήκευση πληροφοριών από την περιήγηση αυτή.

Σχετικό Σύστημα: Τα Δεδομένα Επικοινωνίας τηρούνται στους προσωπικούς υπολογιστές που συνδέονται με το Διαδίκτυο και βρίσκονται σε διάφορους χώρους της ΝΜ (π.χ. γραφεία γιατρών). Επίσης, τηρούνται στο *κεντρικό σύστημα διαχείρισης* που στεγάζεται στις εγκαταστάσεις του Τμήματος Πληροφορικής *(Computer Room)*, στο υπόγειο της ΝΜ, όπου και

πραγματοποιείται ο έλεγχος των εισερχόμενων και εξερχόμενων δεδομένων μέσω Διαδικτύου.

Απώλεια Διαθεσιμότητας Δεδομένων Επικοινωνίας

Επιπτώσεις: Τα Δεδομένα Επικοινωνίας περιλαμβάνουν πληροφορίες επιμόρφωσης των γιατρών μέσω Διαδικτύου (π.χ. επιμορφωτικά σεμινάρια ή ιατρικές ανακοινώσεις), προσφορές προμηθευτών υλικού και νοσηλίων, προκηρύξεις, αλλά και δεδομένα επικοινωνίας με άλλα νοσοκομεία. Η μη διαθεσιμότητα αυτών των δεδομένων δεν κρίνεται ότι μπορεί να επηρεάσει παρά μόνο να δυσχεράνει τη λειτουργία της ΝΜ, καθώς υπάρχουν εναλλακτικοί τρόποι επικοινωνίας (π.χ. φαξ). Περισσότερο ζημιογόνα μπορεί να αποβεί η μη διαθεσιμότητα των στοιχείων φορολογικής ενημερότητας προμηθευτών, που αιτούνται μέσω Διαδικτύου οι εργαζόμενοι του Χρηματικού Τμήματος. Παρόλα αυτά, το κόστος από τη μη διαθεσιμότητα αυτών των δεδομένων είναι η καθυστέρηση που προκύπτει από τους εναλλακτικούς τρόπους αίτησης αυτών (π.χ. με προσωπική παρουσία στην αντίστοιχη εφορία).

Αποτίμηση: Με βάση τα παραπάνω, η συνέπεια της, η διαθεσιμότητας των Δεδομένων Επικοινωνίας αποτιμάται με **ένα (1)** έως μία εβδομάδα και με **τρία (3)** πλέον της μίας εβδομάδας.

Ολική καταστροφή Δεδομένων Επικοινωνίας

Επιπτώσεις: Η ολική καταστροφή των Δεδομένων Επικοινωνίας, περιλαμβανομένων και των εφεδρικών αντιγράφων, συνεπάγεται την εκ νέου εισαγωγή ορισμένων δεδομένων στους αντίστοιχους προσωπικούς υπολογιστές, βάσει πρωτογενών παραστατικών ή μέσω νέας αναζήτησης στο Διαδίκτυο. Κατά συνέπεια εκτιμάται ότι θα υπάρξει οικονομικό κόστος που αφορά τις ανθρωποώρες που απαιτούνται για την εισαγωγή των δεδομένων ή σε λόγω απώλειας δεδομένων που δε βρίσκονται πλέον στο Διαδίκτυο και δεν έχουν τηρηθεί αντίγραφα (π.χ. υπηρεσιακά e-mail).

Αποτίμηση: Με βάση τα παραπάνω, η ολική καταστροφή των Δεδομένων Επικοινωνίας αποτιμάται με **ένα (1),** σε κλίμακα 0-10.

Μερική καταστροφή ή απώλεια ακεραιότητας Δεδομένων Επικοινωνίας

Επιπτώσεις: Η απώλεια των δεδομένων που έχουν εισαχθεί μετά τη λήψη του τελευταίου εφεδρικού αντιγράφου συνεπάγεται την εκ νέου εισαγωγή τους, όπου αυτό είναι εφικτό. Συνεπώς, η κύρια επίπτωση αφορά στο κόστος που προκύπτει από τον απαιτούμενο χρόνο επανεισαγωγής ή αναζήτησής τους στο Διαδίκτυο. Όσον αφορά στην εισαγωγή λαθών (σε μικρή ή μεγαλύτερη κλίμακα) το ΝΜ δε μπορεί να αντιμετωπίσει σοβαρές επιπτώσεις, καθώς τα λάθη αυτά περιορίζονται σε πληροφορίες που μπορεί να αντληθούν ξανά και να επιβεβαιωθούν από το Διαδίκτυο.

Αποτίμηση: Η συνέπεια της περιορισμένης ύπαρξης ή ευρείας ύπαρξης λαθών αποτιμάται με βαθμό **ένα (1)** και της απώλειας ακεραιότητας με βαθμό **ένα (1)**, σε κλίμακα 0-10.

Σκόπιμη Αλλοίωση Δεδομένων Επικοινωνίας

Επιπτώσεις: Η σκόπιμη αλλοίωση των Δεδομένων Επικοινωνίας συνίσταται στην τροποποίηση του περιεχομένου ηλεκτρονικού μηνύματος, η οποία μπορεί να επιφέρει επιπτώσεις στην καλή φήμη της ΝΜ, σε περίπτωση που αφορά στην επικοινωνία με εξωτερικούς συνεργάτες ή άλλα νοσοκομεία ή και στην παρεμπόδιση της ομαλής εκτέλεσης των καθηκόντων των εργαζομένων του νοσοκομείου.

Αποτίμηση: Η συνέπεια της σκόπιμης αλλοίωσης Δεδομένων Επικοινωνίας αποτιμάται με βαθμό **τρία (3)**, σε κλίμακα 0-10.

Αποκάλυψη Δεδομένων Επικοινωνίας

Επιπτώσεις: Τα Δεδομένα Επικοινωνίας περιλαμβάνουν προσωπικές πληροφορίες των εργαζομένων, όπως τις πληροφορίες ανταλλαγής ηλεκτρονικών μηνυμάτων ή τη λίστα των επαφών που τηρούν. Η ηλεκτρονική διεύθυνση αλληλογραφίας καθώς και το περιεχόμενο αυτών των πληροφοριών συνιστούν προσωπικά δεδομένα, αλλά αποτελούν επαγγελματικής φύσεως πληροφορίες. Κατ' επέκταση η αποκάλυψή τους θα οδηγήσει σε ενόχληση των εργαζομένων, αλλά δε θα επιφέρει ποινικές κυρώσεις στο ΝΜ.

Αποτίμηση: Κατά συνέπεια, η αποτίμηση της επίπτωσης αποκάλυψης των στοιχείων αυτών σε τρίτους είναι **τέσσερα (4)**.

5.3.12. *Δεδομένα Πρωτοκόλλου*

Περιεχόμενο: Τα Δεδομένα Πρωτοκόλλου περιλαμβάνουν τα στοιχεία που είναι απαραίτητα για τη συσχέτιση των υπηρεσιακών εγγράφων που εισέρχονται και εξέρχονται από το ΝΜ με τον αύξοντα αριθμό που τα χαρακτηρίζει.

Σχετικό Σύστημα: Τα Δεδομένα Πρωτοκόλλου τηρούνται στην εφαρμογή Ηλεκτρονικού Πρωτοκόλλου, η οποία βρίσκεται στο σύστημα που στεγάζεται στο ισόγειο της ΝΜ. Χειρόγραφα των δεδομένων αυτής της ομάδας δεν τηρούνται.

Απώλεια Διαθεσιμότητας Δεδομένων Πρωτοκόλλου

Επιπτώσεις: Η μη διαθεσιμότητα των στοιχείων αυτών δε θα εμποδίσει την ομαλή λειτουργία του Τμήματος Πρωτοκόλλου. Η λειτουργία του τμήματος δυσχεραίνεται αν η εφαρμογή δεν είναι διαθέσιμη, αλλά μπορεί να διεξαχθεί ομαλά καθώς είναι δυνατό να λειτουργήσει προσωρινά χειρόγραφα και να αποθηκευτούν αργότερα τα νέα δεδομένα που προέρχονται από τα συσσωρευμένα εισερχόμενα και εξερχόμενα έγγραφα. Παρόλα αυτά, μη διαθεσιμότητα που διαρκεί παραπάνω από δύο μέρες θα δημιουργήσει πρόβλημα στη λειτουργία, καθώς θα συσσωρευτεί όγκος δεδομένων που θα πρέπει να εισαχθεί στο σύστημα.

Αποτίμηση: Η επίπτωση της απώλειας διαθεσιμότητας των δεδομένων αυτών αποτιμάται με βαθμό **ένα (1)** για διάστημα έως δύο ημέρες και με βαθμό **τέσσερα (4**) για διάστημα δύο ημερών και πλέον, σε κλίμακα 0-10.

Ολική καταστροφή Δεδομένων Πρωτοκόλλου

Επιπτώσεις: Η ολική καταστροφή των Δεδομένων Πρωτοκόλλου, περιλαμβανομένων και των εφεδρικών αντιγράφων, συνεπάγεται την αδυναμία εκ νέου εισαγωγή των δεδομένων καθώς δεν τηρείται χειρόγραφο αρχείο. Κατά συνέπεια εκτιμάται ότι θα υπάρχει απώλεια της καλής εικόνας της ΝΜ, καθώς δεν θα είναι εφικτός ο έλεγχος στοιχείων που αφορούν την αξιοκρατία και τη διαφάνεια της ΝΜ (π.χ. διαγωνισμούς).

Αποτίμηση: Σύμφωνα με τις παραπάνω διαπιστώσεις η επίπτωση από την ολική καταστροφή των δεδομένων αποτιμάται με βαθμό **πέντε (5),** στην κλίμακα 0-10.

Μερική καταστροφή ή απώλεια ακεραιότητας Δεδομένων Πρωτοκόλλου

Επιπτώσεις: Η απώλεια των δεδομένων που έχουν εισαχθεί μετά τη λήψη του τελευταίου εφεδρικού αντιγράφου συνεπάγεται την αδυναμία επαναεισαγωγής τους, καθώς δεν τηρείται χειρόγραφο αρχείο. Η ακεραιότητα των Δεδομένων πρωτοκόλλου είναι ιδιαίτερα σημαντική, καθώς εξασφαλίζεται η διαφάνεια των διαδικασιών της ΝΜ. Επομένως, η εισαγωγή λαθών, σε μικρή ή μεγαλύτερη κλίμακα, πλήττει την εικόνα της ΝΜ και μπορεί να επιφέρει σοβαρές ποινικές κυρώσεις.

Αποτίμηση: Η επίπτωση από την μερική απώλεια ακεραιότητας των δεδομένων ή την εισαγωγή λαθών σε ευρεία κλίμακα αποτιμάται με βαθμό **πέντε (5)**, σε κλίμακα 0-10.

Σκόπιμη Αλλοίωση Δεδομένων Πρωτοκόλλου

Επιπτώσεις: Η σκόπιμη αλλοίωση των Δεδομένων Πρωτοκόλλου μπορεί να υποκινείται από κίνητρα προσωπικού ή οικονομικού συμφέροντος οφέλους. Κατ' επέκταση τέτοια παραβίαση θα είχε ως συνέπεια οικονομικές απώλειες, αλλά και απώλεια καλής εικόνας της ΝΜ.

Αποτίμηση: Η σκόπιμη αλλοίωση Δεδομένων Πρωτοκόλλου αποτιμάται με βαθμό **πέντε (5)**, σε κλίμακα 0-10.

Αποκάλυψη Δεδομένων Πρωτοκόλλου

Επιπτώσεις: Τα Δεδομένα Πρωτοκόλλου δεν είναι εμπιστευτικής φύσεως και κατ' επέκταση η αποκάλυψή τους δε θα επιφέρει επιπτώσεις στο ΝΜ.

Αποτίμηση: Η αποκάλυψη των Δεδομένων Πρωτοκόλλου αποτιμάται με βαθμό **ένα (1),** σε κλίμακα 0-10.

5.4. Συνοπτική Αποτίμηση Αξίας Δεδομένων

Ο **Πίνακας** παρουσιάζει συγκεντρωτικά την αποτίμηση των επιπτώσεων από την πραγματοποίηση των απειλών, όπως περιεγράφηκε στις προηγούμενες παραγράφους. Να σημειωθεί ότι για τις απειλές των οποίων οι συνέπειες αποτιμήθηκαν με περισσότερους του ενός βαθμούς, ανάλογα με το σενάριο

υλοποίησης της απειλής (π.χ. περιπτώσεις μερικής απώλειας) στον Πίνακα αναγράφεται ο υψηλότερος μόνο βαθμός.

	Απώλεια διαθεσιμότητας					**Απώλεια ακεραιότητας**			**Αποκάλυψη σε τρίτους**
	1 ώρα	12 ώρες	1 ημέρα	2 ημέρες	1 εβδομάδα	Ολική καταστροφή	Μερική απώλεια	Σκόπιμη αλλοίωση	
Δεδομένα Αιμοδοσίας – Αιματολογικού Εργαστηρίου	1	3		**5**		3	**6**	**6**	**6**
Δεδομένα Εργαστηρίων			2	2	3	3	2	**5**	**6**
Δεδομένα Φαρμακείου	2	2	**5**			4	**5**	**6**	**6**
Δεδομένα Προσωπικού		3	3		**5**	**5**	**5**	**5**	**6**
Δεδομένα Μισθοδοσίας	1		1		3	3	3	3	3
Δεδομένα Προμηθευτών και Συμβάσεων		1	3		3	3	3	5	2
Δεδομένα Λογιστηρίου	1	2	**5**			**6**	4	**5**	1
Δεδομένα Επισκέψεων σε Εξωτερικά Ιατρεία	1	3	**5**			**5**	**5**	**5**	4
Δεδομένα Νοσηλίων		1	2		**5**	4	3	4	3
Δεδομένα Κίνησης Ασθενών	1	3	**5**			**5**	3	3	**6**
Δεδομένα Επικοινωνίας			1	1	3	1	1	3	4
Δεδομένα Πρωτοκόλλου		1		4	4	**5**	**5**	**5**	1

Πίνακας 1: Συγκεντρωτική καταγραφή αποτίμησης των επιπτώσεων στα δεδομένα των ΠΣ της ΝΜ

6. Εκτίμηση επικινδυνότητας

6.1. Εισαγωγή

Η αποτίμηση των αγαθών αποτελεί τον έναν από τους δύο παράγοντες που συνθέτουν την επικινδυνότητα των ΠΣ, *την επίπτωση*. Ο δεύτερος παράγοντας, *η πιθανότητα (ενδεχόμενο)*, συντίθεται από την απειλή και την ευπάθεια, ως εξής:

Απειλή x Ευπάθεια = **Πιθανότητα** (Ενδεχόμενο)
Πιθανότητα (Ενδεχόμενο) x Επίπτωση = **Επικινδυνότητα**

Για παράδειγμα, αν μια απειλή είναι σημαντική και το ΠΣ είναι ευπαθές ως προς αυτήν, τότε η πιθανότητα πραγματοποίησής της είναι μεγάλη και αν και η επίπτωσή της είναι σημαντική, τότε η επικινδυνότητα καθίσταται υψηλή.

Στο κεφάλαιο αυτό παρουσιάζονται και αποτιμώνται οι απειλές που αντιμετωπίζουν τα ΠΣ της ΝΜ, ομαδοποιημένες στις εξής κατηγορίες:

- Πρόσβαση μη εξουσιοδοτημένων ατόμων στο σύστημα
- Αστοχία υλικού και λογισμικού
- Ακούσια πρόκληση ζημίας, ανθρώπινα σφάλματα
- Φυσικές απειλές και καταστροφές.

Οι απειλές εξειδικεύονται και δημιουργούνται σενάρια - ενδεχόμενα απειλών, η πιθανότητα πραγματοποίησης των οποίων αξιολογείται στην κλίμακα 1-5 (πολύ χαμηλή, χαμηλή, μέτρια, υψηλή, πολύ υψηλή). Για κάθε συνδυασμό απειλής - αγαθού των ΠΣ υπολογίζεται ένα επίπεδο ευπάθειας σε κλίμακα 1-3 (χαμηλή, μέτρια, υψηλή).

Ο βαθμός επιπέδου επικινδυνότητας υπολογίζεται σε κλίμακα 1-7. Ο υπολογισμός της επικινδυνότητας του ΠΣ προκύπτει, αυτομάτως, ως συνδυασμός των παρακάτω παραγόντων:

- Επίπτωση από την απώλεια της διαθεσιμότητας, της ακεραιότητας ή της εμπιστευτικότητας των αγαθών του συστήματος
- Επίπεδο των απειλών που αντιμετωπίζουν τα αγαθά του συστήματος
- Επίπεδο των ευπαθειών - αδυναμιών του συστήματος.

6.2. Απειλές

Ο πίνακας που ακολουθεί παρουσιάζει τις κυριότερες απειλές που αντιμετωπίζουν τα ΠΣ και οι βασικές κτηριακές εγκαταστάσεις της ΝΜ μαζί με τις αντίστοιχες απαιτήσεις μέτρων ασφάλειας.

Απειλή	Απαιτήσεις σχετικές με ασφάλεια
Πλαστοπροσωπία	Αυθεντικοποίηση
Μη εξουσιοδοτημένη χρήση εφαρμογής	Έλεγχος Εξουσιοδότησης
Εισαγωγή Ιομορφικού Λογισμικού	Μηχανισμοί πρόληψης εισαγωγής Ιομορφικού Λογισμικού
Διήθηση – Παρεμβολές Επικοινωνιών	Εμπιστευτικότητα - Ακεραιότητα - Διαθεσιμότητα
Βλάβη Εξυπηρετητή	Τεχνική Υποστήριξη
Βλάβη Εξυπηρετητή Διαχείρισης Δικτύου ή Συσκευής ή Πύλης Δικτύου	Τεχνική Υποστήριξη
Λάθος Χειρισμού ή Χρήστη	Εκπαίδευση Προσωπικού
Διακοπή Ηλεκτροδότησης	Τροφοδοτικά Αδιάλειπτης Λειτουργίας
Βλάβη Κλιματισμού	Τεχνική Υποστήριξη
Αστοχία Λογισμικού Συστήματος και Λογισμικού Δικτύου	Ποιότητα Λογισμικού
Αστοχία Λογισμικού Εφαρμογών	Δοκιμές και Ποιότητα Εφαρμογών
Σφάλμα Συντήρησης Υλικού	Τεχνική Υποστήριξη
Σφάλμα Συντήρησης Λογισμικού	Τεχνική Υποστήριξη
Φωτιά	Μηχανισμοί Πρόληψης Πυρκαγιάς
Πλημμύρα	Μηχανισμοί Πρόληψης Πλημμύρας
Φυσική Καταστροφή	Σχέδιο Συνέχισης Λειτουργιών
Έλλειψη Προσωπικού	Σχέδιο Συνέχισης Λειτουργιών
Κλοπή	Προστασία ενάντια σε κλοπές
Ηθελημένη πρόκληση βλάβης - βανδαλισμός	Έλεγχος Προσωπικού

Στο πλαίσιο εφαρμογής της μεθοδολογίας που χρησιμοποιήθηκε για την προγενέστερη μελέτη έχουν δημιουργηθεί πολλά σενάρια, τα οποία καλύπτουν τα ενδεχόμενα απειλών για όλα τα στοιχεία του συστήματος με βάση τις πιο πάνω κατηγορίες. Σύμφωνα με τα σενάρια αυτά, κάθε απειλή είναι δυνατό να αφορά περισσότερα από ένα στοιχεία του συστήματος και μάλιστα σε διαφορετικό βαθμό.

Για τη ΝΜ οι σημαντικότερες από τις απειλές αυτές (πιθανότητα εμφάνισης *Πολύ Υψηλή* ή *Υψηλή* σε κλίμακα Πολύ υψηλή, Υψηλή, Μέτρια, Χαμηλή, Πολύ χαμηλή) παρατίθενται στη συνέχεια (*Αναλυτική περιγραφή των απειλών περιλαμβάνεται στο Παράρτημα Γ)*.

- *Πλαστοπροσωπία από Εσωτερικούς Χρήστες*
- *Πλαστοπροσωπία από Εξωτερικούς Χρήστες*
- *Αστοχία Λογισμικού Συστήματος και Λογισμικού Δικτύου (αφορά την εφαρμογή Μισθοδοσίας)*
- *Αστοχία Λογισμικού Εφαρμογών*
- *Λάθος του Χρήστη*
- *Διακοπή Ηλεκτροδότησης*
- *Κλοπή εγγράφων ή άλλων αγαθών του ΠΣ (από άτομα εκτός της ΝΜ)*

6.3. Αδυναμίες και προβλήματα ασφάλειας

Οι αδυναμίες και ευπάθειες αφορούν σημεία του ΠΣ της ΝΜ που μπορεί να επιτρέψουν ή να διευκολύνουν μία απειλή να προξενήσει ζημία σε αυτό. Πέρα από τη χρήση σεναρίων για την αποτίμηση της ευπάθειας του ΠΣ, που έχει γίνει στο πλαίσιο της μεθοδολογίας, οι αδυναμίες ενός ΠΣ εντοπίζονται με επιτόπιο έλεγχο, παρατήρηση και συνεντεύξεις με αρμόδια στελέχη. Βάσει των συνεντεύξεων με στελέχη της ΝΜ και της εμπειρίας των μελετητών, η ομάδα έργου εντόπισε στα ακόλουθα σημεία τις σημαντικότερες αδυναμίες και προβλήματα ασφαλείας που αφορούν το ΠΣ της ΝΜ:

Βασικές αδυναμίες και προβλήματα ασφάλειας ΠΣ της ΝΜ
1. Τα ΠΣ της ΝΜ διαχειρίζονται ευαίσθητα προσωπικά δεδομένα, τα οποία έχουν κρίσιμη σημασία για την υγεία των νοσηλευόμενων ασθενών.
2. Περιορισμένος βαθμός ευαισθητοποίησης και κατάρτισης σημαντικού ποσοστού των χρηστών σε θέματα ασφάλειας.
3. Απουσία οργανωτικό-διοικητικού σχήματος διαχείρισης της ασφάλειας των ΠΣ.
4. Αποσπασματική εφαρμογή ειδικών μέτρων προστασίας προσωπικών και - κυρίως – ευαίσθητων προσωπικών δεδομένων.

Βασικές αδυναμίες και προβλήματα ασφάλειας ΠΣ της ΝΜ
5. Χρήση συστημάτων/εφαρμογών τα οποία δε διαχειρίζεται το Τμήμα Πληροφορικής.
6. Προβλήματα των εγκαταστάσεων που στεγάζουν τα ΠΣ, που σχετίζονται με τη φυσική ασφάλεια των ΠΣ (π.χ. πλημμελής συντήρηση εγκαταστάσεων, ύπαρξη σωληνώσεων σε χώρους που φιλοξενούν εξυπηρετητές ή άλλο υλικό αξίας).
7. Φόρτος εργασίας προσωπικού, σε συνδυασμό με ελλιπή κατάρτιση στη χρήση εφαρμογών, μεγάλου ποσοστού του προσωπικού

Στη συνέχεια παρουσιάζονται τα αποτελέσματα της αποτίμησης των κυριότερων απειλών (πιθανότητα εμφάνισης *Πολύ Υψηλή* ή *Υψηλή* σε κλίμακα Πολύ υψηλή, Υψηλή, Μέτρια, Χαμηλή, Πολύ χαμηλή) και των αντίστοιχων αδυναμιών για τα ΠΣ και τις εγκαταστάσεις της ΝΜ (*Τα αναλυτικά αποτελέσματα δεν χρησίμευσαν για την παρούσα μελέτη για αυτό τον λόγο δεν συμπεριλήφθηκαν)*.

Πλαστοπροσωπία από Εσωτερικούς Χρήστες

Αγαθό	**Συμβάν(τα)** (σε περίπτωση πραγματοποίησης της απειλής)	**Πιθανότητα Απειλής**	**Επίπεδο Αδυναμίας**
Δεδομένα Αιμοδοσίας, Δεδομένα Εργαστηρίων, Δεδομένα Προσωπικού	Απώλεια διαθεσιμότητας (μέχρι και 2 ημέρες), Μερική καταστροφή δεδομένων, Αποκάλυψη δεδομένων εντός του Νοσοκομείου	Υψηλή	Μέτρια
	Ηθελημένη τροποποίηση δεδομένων	Υψηλή	Υψηλή
Δεδομένα Επικοινωνίας	Απώλεια διαθεσιμότητας (μέχρι και 2 ημέρες), Μερική καταστροφή δεδομένων, Αποκάλυψη δεδομένων εντός του Νοσοκομείου, Ηθελημένη τροποποίηση δεδομένων	Πολύ Υψηλή	Υψηλή
Δεδομένα Φαρμακείου	Απώλεια διαθεσιμότητας (μέχρι και 2 ημέρες), Μερική καταστροφή δεδομένων, Αποκάλυψη δεδομένων εντός του Νοσοκομείου	Πολύ Υψηλή	Μέτρια
	Ηθελημένη τροποποίηση δεδομένων	Πολύ Υψηλή	Υψηλή
Δεδομένα Κίνησης, Δεδομένα Εξωτερικών Ιατρείων	Απώλεια διαθεσιμότητας (μέχρι και 2 ημέρες), Μερική καταστροφή δεδομένων, Αποκάλυψη δεδομένων εντός του Νοσοκομείου	Υψηλή	Χαμηλή
	Ηθελημένη τροποποίηση δεδομένων	Υψηλή	Μέτρια
Δεδομένα Λογιστηρίου	Απώλεια διαθεσιμότητας (μέχρι και 2 ημέρες), Μερική καταστροφή δεδομένων, Αποκάλυψη δεδομένων εντός του Νοσοκομείου	Υψηλή	Χαμηλή
	Ηθελημένη τροποποίηση δεδομένων	Πολύ Υψηλή	Μέτρια
Δεδομένα Μισθοδοσίας	Ηθελημένη τροποποίηση δεδομένων	Υψηλή	Υψηλή
Δεδομένα Νοσηλίων	Απώλεια διαθεσιμότητας (μέχρι και 2 ημέρες), Μερική καταστροφή δεδομένων, Αποκάλυψη δεδομένων εντός του Νοσοκομείου	Πολύ Υψηλή	Χαμηλή
	Ηθελημένη τροποποίηση δεδομένων	Πολύ Υψηλή	Μέτρια
Δεδομένα Προμηθευτών – Συμβάσεων	Ηθελημένη τροποποίηση δεδομένων	Υψηλή	Μέτρια

Πλαστοπροσωπία από Εξωτερικούς Χρήστες

Αγαθό	**Συμβάν(τα)** (σε περίπτωση πραγματοποίησης της απειλής)	**Πιθανότητα Απειλής**	**Επίπεδο Αδυναμίας**
Δεδομένα Αιμοδοσίας	Απώλεια διαθεσιμότητας (μέχρι και 2 ημέρες), Μερική καταστροφή δεδομένων, Ηθελημένη τροποποίηση δεδομένων	Υψηλή	Χαμηλή
	Αποκάλυψη δεδομένων εκτός του Νοσοκομείου	Πολύ Υψηλή	Χαμηλή
Δεδομένα Επικοινωνίας, Δεδομένα Εργαστηρίων, Δεδομένα Λογιστηρίου, Δεδομένα Μισθοδοσίας, Δεδομένα Προσωπικού	Απώλεια διαθεσιμότητας (μέχρι και 2 ημέρες), Μερική καταστροφή δεδομένων, Αποκάλυψη δεδομένων εκτός του Νοσοκομείου, Ηθελημένη τροποποίηση δεδομένων	Υψηλή	Χαμηλή
Δεδομένα Φαρμακείου	Απώλεια διαθεσιμότητας (μέχρι και 2 ημέρες), Μερική καταστροφή δεδομένων	Υψηλή	Χαμηλή
	Αποκάλυψη δεδομένων εκτός του Νοσοκομείου, Ηθελημένη τροποποίηση δεδομένων	Πολύ Υψηλή	Χαμηλή
Δεδομένα Κίνησης, Δεδομένα Εξωτερικών Ιατρείων	Απώλεια διαθεσιμότητας (μέχρι και 2 ημέρες), Μερική καταστροφή δεδομένων, Ηθελημένη τροποποίηση δεδομένων	Υψηλή	Χαμηλή
	Αποκάλυψη δεδομένων εκτός του Νοσοκομείου	Πολύ Υψηλή	Χαμηλή
Δεδομένα Νοσηλίων, Δεδομένα Προμηθευτών - Συμβάσεων	Απώλεια διαθεσιμότητας (μέχρι και 2 ημέρες), Μερική καταστροφή δεδομένων, Αποκάλυψη δεδομένων εκτός του Νοσοκομείου	Υψηλή	Χαμηλή
	Ηθελημένη τροποποίηση δεδομένων	Πολύ Υψηλή	Χαμηλή

Αστοχία Λογισμικού Συστήματος και Λογισμικού Δικτύου (αφορά την εφαρμογή Μισθοδοσίας)

Αγαθό	**Συμβάν(τα)** (σε περίπτωση πραγματοποίησης της απειλής)	**Πιθανότητα Απειλής**	**Επίπεδο Αδυναμίας**
Εξυπηρετητής Εφαρμογής Μισθοδοσίας	Απώλεια διαθεσιμότητας μέχρι και 15 λεπτά	Πολύ Υψηλή	Υψηλή
	Απώλεια διαθεσιμότητας από 1 ώρα μέχρι και 12 ώρες	Υψηλή	Χαμηλή

Αστοχία Λογισμικού Εφαρμογών

Αγαθό	**Συμβάν(τα)** (σε περίπτωση πραγματοποίησης της απειλής)	**Πιθανότητα Απειλής**	**Επίπεδο Αδυναμίας**
Εφαρμογές ΔΠΣΝ, *Εφαρμογές Γραφείου,* *Εφαρμογές Αιμοδοσίας,* *Εφαρμογές Μισθοδοσίας,* *Firewall,* *Βάση Δεδομένων*	Απώλεια διαθεσιμότητας μέχρι και 15 λεπτά	Πολύ Υψηλή	Υψηλή

Λάθος του Χρήστη

Αγαθό	**Συμβάν(τα)** (σε περίπτωση πραγματοποίησης της απειλής)	**Πιθανότητα Απειλής**	**Επίπεδο Αδυναμίας**
Δεδομένα Αιμοδοσίας, *Δεδομένα Λογιστηρίου,* *Δεδομένα Μισθοδοσίας,*	Μη εξουσιοδοτημένη μεταβολή δεδομένων (Μικρής Κλίμακας)	Υψηλή	Μέτρια
Δεδομένα Εξωτερικών Ιατρείων, *Δεδομένα Φαρμακείου,* *Δεδομένα Κίνησης,* *Δεδομένα Νοσηλίων,* *Δεδομένα Προμηθευτών – Συμβάσεων,* *Δεδομένα Προσωπικού*	Μη εξουσιοδοτημένη μεταβολή δεδομένων (Μικρής Κλίμακας)	Υψηλή	Υψηλή

Διακοπή Ηλεκτροδότησης

Αγαθό	**Συμβάν(τα)** (σε περίπτωση πραγματοποίησης της απειλής)	**Πιθανότητα Απειλής**	**Επίπεδο Αδυναμίας**
Κτηριακές Εγκαταστάσεις ΝΜ *Σταθμός Αιμοδοσίας* *Τμήμα Μισθοδοσίας* *Τμήμα Πληροφορικής και Οργάνωσης* *Τμήμα Προσωπικού*	Απώλεια διαθεσιμότητας μέχρι και 15 λεπτά	Υψηλή	Χαμηλή

Κλοπή εγγράφων ή άλλων αγαθών του ΠΣ (από άτομα εκτός της ΝΜ)

Αγαθό	**Συμβάν(τα)** (σε περίπτωση πραγματοποίησης της απειλής)	**Πιθανότητα Απειλής**	**Επίπεδο Αδυναμίας**
Κτηριακές Εγκαταστάσεις ΝΜ	Αποκάλυψη δεδομένων εκτός του Νοσοκομείου	Υψηλή	Μέτρια

6.4. Εκτίμηση επικινδυνότητας ΠΣ

Ο βαθμός επικινδυνότητας υπολογίζεται για κάθε συνδυασμό απειλής, αδυναμίας και αγαθού και αποτιμάται σε κλίμακα 1-7. Στον υπολογισμό δε λαμβάνονται υπόψη τα ήδη εγκατεστημένα αντίμετρα. Η τιμή του βαθμού επικινδυνότητας χρησιμοποιείται για την επιλογή συγκεκριμένων μέτρων προστασίας στα πλαίσια του Σχεδίου Ασφάλειας.

Στους Πίνακες που ακολουθούν παρουσιάζονται οι συνδυασμοί αγαθών (δεδομένων) των ΠΣ της ΝΜ και απειλών, για τους οποίους υπολογίστηκαν οι υψηλότεροι βαθμοί επικινδυνότητας (5-6) (*Τα αναλυτικά αποτελέσματα δεν χρησίμευσαν για την παρούσα μελέτη για αυτό τον λόγο δεν συμπεριλήφθηκαν)*.

Απειλή: Πλαστοπροσωπία από Εσωτερικούς Χρήστες

Αγαθό	Επίπτωση	Επικινδυνότητα
Δεδομένα Φαρμακείου	Ηθελημένη τροποποίηση δεδομένων	6
	Απώλεια διαθεσιμότητας από 1 μέχρι και 2 μέρες	5
Δεδομένα Αιμοδοσίας, *Δεδομένα Λογιστηρίου,* *Δεδομένα Προσωπικού*	Ηθελημένη τροποποίηση δεδομένων	5

Απειλή: Πλαστοπροσωπία από Εξωτερικούς Χρήστες

Αγαθό	Επίπτωση	Επικινδυνότητα
Δεδομένα Αιμοδοσίας, *Δεδομένα Φαρμακείου,* *Δεδομένα Κίνησης*	Αποκάλυψη δεδομένων εκτός του Νοσοκομείου	5
Δεδομένα Φαρμακείου	Ηθελημένη τροποποίηση δεδομένων	5

Απειλή: Εισαγωγή Ιομορφικού Λογισμικού

Αγαθό	Επίπτωση	Επικινδυνότητα
Σταθμοί Εργασίας	Ολική καταστροφή δεδομένων, Μη εξουσιοδοτημένη μεταβολή δεδομένων (Μεγάλης Κλίμακας), Ηθελημένη τροποποίηση δεδομένων	5

6.5. Εκτίμηση επικινδυνότητας εγκαταστάσεων

Όπως και για τα δεδομένα των ΠΣ, για τις κτηριακές εγκαταστάσεις ο βαθμός επικινδυνότητας υπολογίζεται για κάθε συνδυασμό απειλής, αδυναμίας και αγαθού (εγκατάστασης) και αποτιμάται σε κλίμακα 1-7. Στον υπολογισμό δε λαμβάνονται υπόψη τα ήδη εγκατεστημένα αντίμετρα. Η τιμή του βαθμού επικινδυνότητας χρησιμοποιείται για την επιλογή συγκεκριμένων μέτρων προστασίας στα πλαίσια του Σχεδίου Ασφάλειας.

Στους Πίνακες που ακολουθούν παρουσιάζονται οι συνδυασμοί εγκαταστάσεων της ΝΜ και απειλών, για τους οποίους υπολογίστηκαν οι υψηλότεροι βαθμοί επικινδυνότητας (5-6) (*Τα αναλυτικά αποτελέσματα δεν χρησίμευσαν για την παρούσα μελέτη για αυτό τον λόγο δεν συμπεριλήφθηκαν)*.

Απειλή: Κλοπή εγγράφων ή άλλων αγαθών του ΠΣ (από άτομα εκτός της ΝΜ)

Αγαθό	Επίπτωση	Επικινδυνότητα
Κτηριακές εγκαταστάσεις ΝΜ	Αποκάλυψη δεδομένων εκτός του Νοσοκομείου	5

7. Συμπεράσματα

Μία Νοσοκομειακή Μονάδα αποδίδει υψηλή σημασία στην Ασφάλεια των Πληροφοριακών της Συστημάτων και των προσωπικών δεδομένων που διαχειρίζεται. Με βάση αυτή την αρχή, έχει θέσει σε εφαρμογή συγκεκριμένη Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων, την οποία θα πρέπει να εφαρμόζουν όλοι οι χρήστες και οι συμμετέχοντες στη λειτουργία των Πληροφοριακών Συστημάτων.

Όλοι οι χρήστες, ή με άλλο τρόπο εμπλεκόμενοι στη λειτουργία των Πληροφοριακών Συστημάτων, θα πρέπει να τηρούν τους ακόλουθους κανόνες:

- Να μελετήσουν προσεκτικά το κείμενο της Πολιτικής Ασφαλείας και να την εφαρμόζουν χωρίς παρεκκλίσεις.
- Να μελετήσουν προσεκτικά το Σχέδιο Έκτακτης Ανάγκης για τα Πληροφοριακά Συστήματα και να γνωρίζουν τον ρόλο τους σε αυτό.
- Κατά την επεξεργασία προσωπικών δεδομένων να εφαρμόζουν τον Κώδικα Δεοντολογίας που έχει αναπτυχθεί.
- Να ακολουθούν τις σχετικές οδηγίες που εκδίδει το Τμήμα Πληροφορικής και Οργάνωσης.
- Να αναφέρουν άμεσα στο Τμήμα Πληροφορικής και Οργάνωσης κάθε γεγονός ή ενέργεια που ενδέχεται να θέσει σε κίνδυνο τα Πληροφοριακά Συστήματα του Νοσοκομείου.
- Να σέβονται τη Νομοθεσία περί προστασίας προσωπικών δεδομένων.
- Να προστατεύουν το συνθηματικό τους και να μην το αποκαλύπτουν σε κανέναν.
- Να μην εκθέτουν σε κίνδυνο τους υπολογιστές του Νοσοκομείου.

8. Ακρωνύμια

ΝΜ:	Νοσοκομειακή Μονάδα
ΠΣ:	Πληροφοριακό Σύστημα
ΓΚΠΔ:	Γενικός Κανονισμός Προστασίας Δεδομένων
GDPR:	General Data Protection Regulation
ΔΠΣΝ:	Διαχειριστικό Πληροφοριακό Σύστημα Νοσοκομείου

9. Αναφορές

GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary: https://www.iso.org/standard/73906.html

Νόμος 4624/2019: https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/nomos-4624-2019-phek-137a-29-8-2019.html

ISO/IEC 22301/2019 Security and resilience – Business continuity management systems – Requirements: https://www.iso.org/standard/75106.html