ΚΕΦΑΛΑΙΟ 9ο
ΕΛΕΓΧΟΣ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Περιεχόμενα

Σε αυτό το κεφάλαιο 2

Λέξεις κλειδιά 2

9.1 Ερωτηματολόγιο 2

9.1 Ερωτηματολόγιο συστημάτων και διεύθυνσης πληροφορικής 2

- Ερώτημα κατανόησης: Κατανόηση περιβάλλοντος και λειτουργίας 8

9.3 Πρόγραμμα ελέγχου – γενικά 8

9.4. Πρόγραμμα ελέγχου Συστημάτων και Διεύθυνσης Πληροφορικής 9

Βήματα ελέγχου 9

Διαχωρισμός καθηκόντων 9

Οργάνωση μηχανογράφησης 9

Ασφάλεια πληροφοριακών συστημάτων 10

Στοιχεία μηχανογραφικού προγράμματος 11

Λήψη αρχείων back-up 12

Πλάνο εναλλακτικής λειτουργίας 12

- Ερώτημα κατανόησης: Έλεγχος πληροφοριακών συστημάτων 12

Περιεχόμενα ερωτημάτων / παραδειγμάτων κεφαλαίου 13

Σε αυτό το κεφάλαιο

- Παρουσιάζονται οι σκοποί του ελέγχου των συστημάτων πληροφορικής.
- Παρουσιάζονται πληθώρα ερωτήσεων ανά περίπτωση με σκοπό τη διευκόλυνση του αναγνώστη ως προς την κατανόηση των επιμέρους λειτουργιών.
- Παρουσιάζεται πρόγραμμα Εσωτερικού Ελέγχου για τον έλεγχο των συστημάτων πληροφορικής.

Λέξεις κλειδιά

- Επαρκής κατανόηση,
- Εντοπισμός αδύναμων σημείων,
- Δικλείδες ασφαλείας,
- Αποτελεσματικότητα δικλείδων,
- Δικαιώματα και περιορισμός πρόσβασης,
- Διαχωρισμός καθηκόντων,
- Πρόγραμμα Εσωτερικού Ελέγχου.

9.1 Ερωτηματολόγιο

Σκοπό του ερωτηματολογίου ως χρήσιμο και πρακτικό εργαλείο, είναι η συγκέντρωση των όσο το δυνατό περισσότερων πληροφοριών σχετικά με τις υπό έλεγχο διαδικασίες και λειτουργίες. Η πληθώρα των ερωτήσεων, αποσκοπεί στην όσο το δυνατόν πληρέστερη κατανόηση του συναλλακτικού κύκλου από την πλευρά του αναγνώστη. Γενικά στο παρακάτω ερωτηματολόγιο, παρατίθενται σειρά ερωτήσεων που σχετίζονται με θέματα **ασφάλειας** και περιβάλλοντος των πληροφοριακών συστημάτων, θέματα **προσβάσεων** και **κωδικών πρόσβασης**, καθώς επίσης και **εναλλακτικό πλάνο λειτουργίας**.

9.1 Ερωτηματολόγιο συστημάτων και διεύθυνσης πληροφορικής

Σκοπός του ελέγχου των συστημάτων πληροφορικής είναι η εξασφάλιση των παρακάτω:

- Η ανάγκη προμήθειας ή ανάπτυξης εφαρμογών πληροφορικής τεκμηριώνεται επαρκώς.
- Οι δαπάνες σε συστήματα και εφαρμογές πληροφορικής είναι **εγκεκριμένες**.
- Η **ασφάλεια** του περιβάλλοντος στο οποίο λειτουργούν τα πληροφοριακά συστήματα είναι **επαρκής**.
- Έχουν ορισθεί και εγκριθεί **επίπεδα πρόσβασης** ανά χρήστη και εφαρμογή.
- Ο **διαχωρισμός καθηκόντων** μεταξύ προγραμματιστών, χρηστών, systems administrator, υπευθύνου ασφαλείας πληροφοριακών συστημάτων είναι σαφής και επαρκής.
- Όλα τα συστήματα πληροφορικής συντηρούνται επαρκώς.
- Τηρούνται αρχεία **back up**.
- Εξασφαλίζεται η **συνέχεια** των **κρίσιμων δραστηριοτήτων** του οργανισμού, μέσω εναλλακτικού πλάνου λειτουργίας.

Οι αντίστοιχες ερωτήσεις που θα μπορούσαν να τεθούν, προκειμένου να κατανοηθεί επαρκώς, η λειτουργία της διεύθυνσης πληροφορικής, χωρίς φυσικά να θεωρούνται οι αποκλειστικές ή να είναι οι δεσμευτικές, παρατίθενται ακολούθως.
Με βάση τις απαντήσεις και τις πληροφορίες που θα συλλεχθούν, ο Εσωτερικός Ελεγκτής, θα είναι σε θέση να κατανοήσει όχι μόνο την αντίστοιχη λειτουργία, αλλά και να εντοπίσει τυχόν αδύναμα σημεία όπως επίσης και δικλείδες που θα πρέπει να δοκιμάσει την αποτελεσματικότητα τους.

- Υφίσταται **εγκεκριμένο οργανόγραμμα** στη διεύθυνση πληροφορικής;
- Στελεχώνεται η διεύθυνση από επαρκές και κατάλληλο προσωπικό;
- Ποια είναι η βασική αποστολή και οι ευθύνες της διεύθυνσης;
- Συνδέονται οι στόχοι της διεύθυνσης με τους στρατηγικούς στόχους;
- Ποιοι είναι οι εσωτερικοί και εξωτερικοί πελάτες της διεύθυνσης;
- Υφίστανται εγκεκριμένες διαδικασίες αναφορικά με τις δραστηριότητες της διεύθυνσης όπως ασφάλεια πληροφοριακών συστημάτων, λήψη back up, ανάπτυξη εφαρμογών;
- Ποιες περιοχές θεωρούνται **υψηλού κινδύνου**, οι ποίες θα είχαν επίδραση στη λειτουργία του οργανισμού;
- Έχει εξεταστεί η πιθανότητα και η επίδραση των επικίνδυνων σημείων / περιοχών;
- Οι στόχοι της διεύθυνσης είναι ρεαλιστικοί και μετρήσιμοι;
- Πως παρακολουθείται η απόδοση της διεύθυνσης;
- Έχουν καθορισθεί **επίπεδα πρόσβασης ανά χρήστη**;
- Ποιος εγκρίνει την πρόσβαση στα υποσυστήματα;

- Ποιοι **μηχανισμοί** αποτρέπουν τη μη εξουσιοδοτημένη πρόσβαση στα πληροφοριακά συστήματα;
- Είναι αναγκαίοι οι **κωδικοί πρόσβασης** για την είσοδο στα πληροφοριακά συστήματα;
- Με ποια συχνότητα αλλάζουν οι κωδικοί;
- Υφίστανται συγκεκριμένοι κανόνες για τη χρήση κωδικών πρόσβασης;
- Προστατεύονται επαρκώς ευαίσθητες και εμπιστευτικές πληροφορίες;
- Χρησιμοποιείται λογισμικό προστασίας συστημάτων και πληροφοριών;
- Έχουν απαγορευτεί συγκεκριμένες ιστοσελίδες κατά την πλοήγηση στο διαδίκτυο;
- Λαμβάνονται αρχεία **back up**; Με ποια συχνότητα;
- Ποιος είναι υπεύθυνος για τη λήψη αρχείων back up; Τι άλλα καθήκοντα έχει;
- Που φυλάσσονται τα αρχεία back up;
- Ποιος έχει πρόσβαση στα αρχεία back up; Τι είδους πρόσβαση έχει;
- Ελέγχονται τα αρχεία back up για τη λειτουργία τους;
- Υφίσταται πλάνο εναλλακτικής λειτουργίας σε περίπτωση κατάρρευσης των συστημάτων;
- Έχουν ληφθεί **μέτρα ασφαλείας** στο δωμάτιο των υπολογιστών;
- Υπάρχει συναγερμός του οποίου η χρήση ελέγχεται ανά τακτά χρονικά διαστήματα;
- Υπάρχουν ανιχνευτές καπνού και πυρός;
- Πραγματοποιούνται ασκήσεις πυρκαγιάς;
- Υπάρχουν εμφανή σημεία εξόδου ή εξόδων κινδύνου;
- Ο εξοπλισμός δοκιμάζεται ανά τακτά χρονικά διαστήματα ή ελέγχεται η ημερομηνία λήξης του;
- Υπάρχει μηχανισμός ο οποίος απομονώνει αυτόματα την παροχή ρεύματος πριν την εφαρμογή του συστήματος αντιμετώπισης πυρκαγιάς;
- Έχει ληφθεί υπόψη πέρα από την περίπτωση της πυρκαγιάς σενάριο φθοράς λόγω κακοκαιρίας;
- Έχει τεθεί σε ισχύ μηχανισμός εξισσορόπησης της παροχής ρεύματος είτε αυτή αυξηθεί είτε σημειώσει πτώση (UPS);
- Έχει ληφθεί μέριμνα για τη χρήση γεννήτριας στην περίπτωση πτώσης της παροχής ρεύματος;
- Γνωστοποιούνται στη διοίκηση της εταιρείας τα αποτελέσματα των δοκιμών;
- Έχει ληφθεί μέριμνα για εναλλακτική παροχή air-condition;

- Έχουν τεθεί σε ισχύ **ασφαλιστικές δικλείδες** στην εισαγωγή και εξαγωγή δεδομένων;
- Είναι επαρκής και σαφής ο **διαχωρισμός των καθηκόντων** μεταξύ των χρηστών;
- Παράγει το σύστημα αναφορές για τις περιπτώσεις εισαγωγής των χρηστών σε μη εξουσιοδοτημένα πεδία;
- Παράγει το σύστημα αναφορές για τις περιπτώσεις εισαγωγής των χρηστών σε πεδία (exception reports) ώστε να είναι δυνατός ο εντοπισμός των σχετικών εξουσιοδοτήσεων;
- Η πρόσβαση σε συγκεκριμένα πεδία περιορίζεται με τη λήξη του ωραρίου;
- Έχει συσταθεί και εγκριθεί από τη διοίκηση **πλάνο παρακολούθησης εργασιών** των χρηστών;
- Παράγονται από το σύστημα αναφορές των εργασιών των χρηστών;
- Επισκοπούνται οι αναφορές των εργασιών των χρηστών;
- Έχουν συσταθεί και εγκριθεί από τη διοίκηση διαδικασίες ασφαλείας του δωματίου των υπολογιστών;
- Είναι επαρκής η ασφάλεια του δωματίου των υπολογιστών;
- Η πρόσβαση στο δωμάτιο των υπολογιστών είναι περιορισμένη στους απολύτως απαραίτητους υπαλλήλους;
- Έχουν συσταθεί και εγκριθεί από τη διοίκηση διαδικασίες σχετικά με την εισαγωγή δεδομένων στο σύστημα και την πρόσβαση των χρηστών στα απολύτως απαραίτητα πεδία;
- Υπάρχει media library;
- Έχουν συνταχθεί και εγκριθεί από τη διοίκηση διαδικασίες για τη βιβλιοθήκη;
- Η βιβλιοθήκη βρίσκεται σε ξεχωριστό σημείο από το δωμάτιο των υπολογιστών;
- Η πρόσβαση στη βιβλιοθήκη έχει περιοριστεί στους απολύτως απαραίτητους και εξουσιοδοτημένους υπαλλήλους;
- Έχουν ληφθεί μέτρα ασφαλείας στη βιβλιοθήκη όπως απαγόρευση καπνίσματος, ανανέωση αέρα, ανιχνευτής πυρός, σύστημα συναγερμού σε περίπτωση φωτιάς;
- Τα **ευαίσθητα αρχεία** είναι **κλειδωμένα**;
- Παρακολουθούνται οι ποσότητες των δίσκων και προγραμμάτων που εισέρχονται

στη βιβλιοθήκη;

- Είναι σαφής και επαρκής ο διαχωρισμός των καθηκόντων μεταξύ των προγραμματιστών, χρηστών, υπευθύνου ασφαλείας των πληροφοριακών συστημάτων;
- Ο **υπεύθυνος ασφαλείας** είναι ανεξάρτητος από το υπόλοιπο τμήμα;
- Είναι σαφής και επαρκής ο διαχωρισμός των καθηκόντων μεταξύ των database administrator και υπευθύνου ασφαλείας των πληροφοριακών συστημάτων;
- Κατά την εσωτερική ανάπτυξη προγραμμάτων είναι διαχωρισμένα η ανάπτυξη και προγραμματισμός από το τρέξιμο των προγραμμάτων;
- Είναι σαφώς και επαρκώς διαχωρισμένες οι δικλείδες εισαγωγής και εξαγωγής δεδομένων;
- Είναι σαφώς και επαρκώς διαχωρισμένες οι δικλείδες της βιβλιοθήκης και άλλων δραστηριοτήτων;
- Είναι σαφώς και επαρκώς διαχωρισμένες οι δικλείδες των προγραμμάτων και άλλων δραστηριοτήτων;
- Έχει απαγορευθεί στους προγραμματιστές η χρήση του συστήματος;
- Έχει απαγορευθεί στους χρήστες ο προγραμματισμός;
- Εκτελούνται οι εργασίες βάσει του εγχειριδίου διαδικασιών;
- Ο **database administrator** βρίσκεται σε ξεχωριστό χώρο από τους χρήστες;
- Η έκδοση των media από τη βιβλιοθήκη ελέγχεται επαρκώς;
- Τηρούνται αρχεία σχετικά με την έκδοση και επιστροφή των media στη βιβλιοθήκη;
- Τα ευαίσθητα αρχεία τηρούνται εις διπλούν;
- Μετά την κωδικοποίηση των προγραμμάτων, πραγματοποιείται δοκιμή τους από ανεξάρτητο προγραμματιστή;
- Αποτυπώνεται η δοκιμή του προγράμματος;
- Υπάρχουν αντίγραφα των προγραμμάτων και της αποτύπωσης τους εάν αυτό καταστεί αναγκαίο;
- Κατά την παραίτηση ή απόλυση του υπαλλήλου, εξασφαλίζεται ότι ο υπάλληλος δεν

έχει πρόσβαση σε κανενός είδους σύστημα της εταιρείας;

- Έχει ληφθεί πρόνοια για την κάλυψη κύριων θέσεων από προσωπικό ασφαλείας σε περίπτωση ανάγκης;
- Έχει συσταθεί και εγκριθεί από τη διοίκηση πλάνο συντήρησης εξοπλισμού;
- Επισκοπείται το πλάνο συντήρησης;
- Τηρούνται στατιστικά δεδομένα σχετικά με τις φθορές του εξοπλισμού;
- Έχει γνωστοποιηθεί στους υπαλλήλους το **πλάνο εναλλακτικό λειτουργίας**;
- Γνωρίζουν όλοι οι υπάλληλοι τα καθήκοντα τους σε περίπτωση ολικής / μερικής καταστροφής και εφαρμογής του πλάνου εναλλακτικής λειτουργίας;
- Συμμετέχουν οι υπάλληλοι των τμημάτων στην ανάπτυξη του εναλλακτικού πλάνου λειτουργίας;
- Έχει υπογραφεί συμβόλαιο με ασφαλιστική εταιρεία με σκοπό την ασφαλιστική κάλυψη του εξοπλισμού των ηλεκτρονικών συστημάτων;
- Βάσει ποιων παραμέτρων επιλέγεται η ασφαλιστική εταιρεία, βάσει τιμής ή προσφερόμενων υπηρεσιών;
- Η ασφαλιστική κάλυψη κρίνεται επαρκής ή όχι;
- Υπήρξε περίπτωση όπου χρειάστηκε η εταιρεία να αποζημιωθεί από την ασφαλιστική;
- Εάν ναι, ο χρόνος αποζημίωσης κρίνεται ικανοποιητικός;
- Έχει συνταχθεί πρόγραμμα αξιολόγησης της ασφαλιστικής εταιρείας;
- Παρακολουθούνται τα νέα ασφαλιστικά προϊόντα με σκοπό την επιλογή νέων που ταιριάζουν περισσότερο στις ανάγκες της εταιρείας;
- Έχει οριστεί **υπεύθυνος διαχείρισης κινδύνων** των **πληροφοριακών συστημάτων** (security officer);
- Ο υπεύθυνος διαχείρισης κινδύνων είναι ανεξάρτητος από το τμήμα πληροφορικής;
- Έχει λάβει ο υπεύθυνος διαχείρισης κινδύνων υπόψη του εάν όχι όλους τους περισσότερους κινδύνους που σχετίζονται με την ασφάλεια των πληροφοριακών συστημάτων;

- Ποια είναι τα τυπικά προσόντα του υπευθύνου διαχείρισης κινδύνων;
- Έχει προσληφθεί ο υπεύθυνος διαχείρισης κινδύνων με απόφαση του διοικητικού συμβουλίου;

- **Ερώτημα κατανόησης: Κατανόηση περιβάλλοντος και λειτουργίας**

Πληροφορείστε από τις απαντήσεις σε ερωτηματολόγιο πληροφορικής, ότι δεν υφίσταται καθορισμένη πολιτική αναφορικά με τα πεδία πρόσβασης των χρηστών στο λογιστήριο. Ποιοι πιθανοί κίνδυνοι ελλοχεύουν;

Προτεινόμενη απάντηση: παρατίθενται πιθανοί κίνδυνοι:

- *Μη εξουσιοδοτημένη πρόσβαση των χρηστών σε σχετικά πεδία.*
- *Πρόσβαση των χρηστών σε πληροφόρηση που δεν είναι απαραίτητη για την εκτέλεση των καθηκόντων τους.*
- *Πιθανή αλλοίωση δεδομένων του συστήματος.*
- *Πιθανός ανεπαρκής διαχωρισμός καθηκόντων μεταξύ των στελεχών του λογιστηρίου.*

9.3 Πρόγραμμα ελέγχου – γενικά

Το πρόγραμμα ελέγχου, ως εργαλείο του Εσωτερικού Ελεγκτή για την άσκηση των καθηκόντων του, έπεται πάντα της συνέντευξης με τον ελεγχόμενο και περιλαμβάνει τα βήματα σε σειρά που θα ακολουθήσει ο Εσωτερικός Ελεγκτής, με βάση τη ροή των εργασιών της περιοχής που επισκοπείται και ελέγχεται.

Η ανάπτυξη του προγράμματος ελέγχου βασίζεται στους στόχους του οργανισμού, στις διαδικασίες του, καθώς και στις αποφάσεις της Διοίκησης, που θα πρέπει να γνωρίζει ο Εσωτερικός Ελεγκτής. Θα πρέπει να έχει την ανάλογη δομή και βήματα, ώστε η εφαρμογή του να προσδίδει στον Εσωτερικό Ελεγκτή, την εξασφάλιση ότι έχει ελεγχθεί αν όχι όλο, το μεγαλύτερο μέρος των δραστηριοτήτων, καθώς επίσης και το ότι τα συμπεράσματα στα οποία θα καταλήξει, θα τον βοηθούν να σχηματίσει εικόνα για το αν οι εντοπισμένοι κίνδυνοι αντιμετωπίζονται επαρκώς.

Το παρακάτω γενικό πρόγραμμα ελέγχου, παραθέτει τα βήματα που θα ακολουθήσει ο Εσωτερικός Ελεγκτής. Τα βήματα ελέγχου εκτιμάται ότι ακολουθούνται γενικότερα σε κάθε περίπτωση ελέγχου.

9.4. Πρόγραμμα ελέγχου Συστημάτων και Διεύθυνσης Πληροφορικής

Τι πρέπει να εξασφαλιστεί από τον έλεγχο των συστημάτων πληροφορικής; Να εξασφαλιστούν τα παρακάτω:

- Να εξασφαλιστεί ότι η υπάρχουσα οργανωτική διάρθρωση της μηχανογραφικής υπηρεσίας είναι αποτελεσματική.
- Να εξασφαλιστεί ότι ο έλεγχος του τμήματος μηχανογράφησης διενεργείται από τα αρμόδια άτομα αποτελεσματικά και αποδοτικά.
- Να εξασφαλιστεί η ομαλή και απρόσκοπτη λειτουργία των συστημάτων και των δεδομένων και ότι διασφαλίζεται η πρόσβαση σε αυτά μόνο σε εξουσιοδοτημένους χρήστες.
- Να εξασφαλιστεί η ορθή και απρόσκοπτη χρήση του μηχανογραφικού προγράμματος.

Βήματα ελέγχου

Διαχωρισμός καθηκόντων

- Αξιολόγησε τις λειτουργικές ευθύνες των στελεχών της διεύθυνσης πληροφορικής, με σκοπό την **επάρκεια** του **διαχωρισμού καθηκόντων**. Γενικά, οι παρακάτω λειτουργίες θα πρέπει να πραγματοποιούνται από διαφορετικά στελέχη:
  - Ανάπτυξη εφαρμογής και χρήστης εφαρμογής.
  - Διαχείριση ασφάλειας πληροφοριακών συστημάτων και χρήστες πληροφοριακών συστημάτων.
  - Υπεύθυνος πληροφοριακών συστημάτων, υπεύθυνος ασφάλειας πληροφοριακών συστημάτων.

Οργάνωση μηχανογράφησης

- Κατέγραψε την οργανωτική δομή του Τμήματος / διεύθυνσης Μηχανογράφησης.
- Εξέτασε ποιες είναι οι υποχρεώσεις του κάθε εργαζόμενου στο τμήμα. Εξέτασε εάν υφίστανται λεπτομερείς περιγραφές θέσεων των εργαζομένων του τμήματος.
- Εξέτασε αν υπήρξαν αλλαγές στη δομή του τμήματος ή στις αρμοδιότητες του προσωπικού κατά το τελευταίο έτος.
- Εξέτασε σε ποια διεύθυνση υπάγεται το τμήμα μηχανογράφησης.
- Εξέτασε σε ποιας βαθμίδας στέλεχος αναφέρεται ο Προϊστάμενος του τμήματος.
- Έλεγξε εάν υφίστανται σημεία μέτρησης απόδοσης στα οποία να αναφέρεται η Διεύθυνση του τμήματος.

- Εξέτασε εάν τα προαναφερθέντα σημεία απόδοσης εξετάζονται από την κατάλληλη Διεύθυνση.
- Εξέτασε αν εφαρμόζεται κάποια τυπική μεθοδολογία ανάπτυξης συστημάτων.
- Εξέτασε αν έχει καθιερωθεί από τη Διοίκηση τυπική διαδικασία ελέγχου του καθημερινού συστήματος συντήρησης.
- Εξέτασε αν υφίσταται **διαδικασία ασφάλειας** των **μηχανογραφικών συστημάτων** και αν το προσωπικό είναι ενήμερο σχετικά με αυτή τη διαδικασία.
- Εξέτασε εάν ο οργανισμός έχει διασφαλίσει την συνέχεια των εταιρικών εργασιών.

Ασφάλεια πληροφοριακών συστημάτων

- Εξέτασε αν υφίσταται σχετική λίστα εντός του μηχανογραφικού προγράμματος όπου καθορίζονται τα **δικαιώματα πρόσβασης** όλου του προσωπικού.
- Εξέτασε αν οι διάφορες λειτουργίες και προσβάσεις στα μηχανογραφικά συστήματα καταχωρούνται και εξετάζονται βάσει σχετικών μητρώων που μπορούν να εκτυπωθούν από το μηχανογραφικό πρόγραμμα (logs).
- Εξέτασε αν έχει προκύψει κατά το παρελθόν, θέμα σχετικό με την ασφάλεια των συστημάτων ή δεδομένων και με ποιο τρόπο τελικά διευθετήθηκε.
- Επέλεξε δείγμα χρηστών συστημάτων και έλεγξε τα παρακάτω:
  - Αν έχουν **ξεχωριστά ID** και **κωδικούς πρόσβασης**.
  - Ποιά ήταν η τελευταία φορά που τροποποιήθηκε ο κωδικός πρόσβασης.
  - Αν υφίσταται λίστα που καθορίζει τα δικαιώματα πρόσβασης του προσωπικού, εάν υπάρχουν σε αυτή οι χρήστες που έχουμε επιλέξει σαν δείγμα και εάν και κατά πόσο σχετίζονται τα δικαιώματα πρόσβασης που έχουν με τις αρμοδιότητές τους.
  - Επέλεξε δείγμα ατόμων που η πρόσληψη τους πραγματοποιήθηκε πρόσφατα και έλεγξε αν υφίστανται στη λίστα δικαιωμάτων πρόσβασης και αν έχουν ξεχωριστά ID και κωδικούς πρόσβασης.
  - Επέλεξε δείγμα ατόμων που αποχώρησαν πρόσφατα από τον οργανισμό και έλεγξε κατά πόσο έχουν διαγραφεί από το σύστημα.
  - Έλεγξε εάν **λαμβάνονται** σε καθημερινή βάση **back ups** των συστημάτων, των servers και των δεδομένων που αποτελούν περιουσιακά στοιχεία του οργανισμού.
  - Επιβεβαίωσε ότι έχουν καθορισθεί επίπεδα πρόσβασης για κάθε χρήστη, με χρήση κωδικού πρόσβασης και ταυτότητας για κάθε χρήστη.
  - Εξέτασε την **εμπιστευτικότητα** των **κωδικών πρόσβασης**, την συχνότητα αλλαγής τους και το πόσο δυνατοί είναι οι κωδικοί πρόσβασης.

Σημείωση: κάθε κωδικός πρόσβασης θα πρέπει να αποτελείται από συνδυασμό γραμμάτων, αριθμών και συμβόλων, καθώς επίσης να επικαιροποιείται κάθε δύο μήνες.

- Έλεγξε αν μπλοκάρεται η πρόσβαση του χρήστη αυτόματα, μετά από συγκεκριμένο αριθμό μη επιτυχών προσπαθειών εισόδου στο σύστημα.
- Αξιολόγησε εάν τα δεδομένα επίπεδα πρόσβασης, εξασφαλίζουν ένα επαρκές επίπεδο διαχωρισμού καθηκόντων.
- Επιβεβαίωσε ότι για αλλαγές στα δικαιώματα πρόσβασης των χρηστών, υφίστανται **γραπτές εγκρίσεις** από τη Γενική Διεύθυνση, οι οποίες προωθούνται στη διεύθυνση πληροφορικής.
- Επιβεβαίωσε το ότι η δυνατότητα τροποποιήσεων των κυρίως αρχείων πελατών, προϊόντων, τιμοκαταλόγων, περιορίζεται στο προσωπικό της διεύθυνσης πληροφορικής.
- Επιβεβαίωσε ότι **δικλείδες ασφαλείας** όπως κλείδωμα πώλησης σε πελάτες που έχουν ανεξόφλητα υπόλοιπα, είναι σε ισχύ και δε μπορούν να προσπεραστούν από τους χρήστες.
- Επιβεβαίωσε την ύπαρξη τελευταίας έκδοσης λογισμικού προστασίας από ιούς, η οποία είναι εγκατεστημένη στους υπολογιστές των χρηστών.
- Εξέτασε αν υφίστανται πυροσβεστήρες κοντά σε servers.
- Εξέτασε αν η **πρόσβαση** στο δωμάτιο υπολογιστών και στους servers, **περιορίζεται** μόνο σε εξουσιοδοτημένα στελέχη.
- Επιβεβαίωσε την ύπαρξη εξοπλισμού UPS, με σκοπό την εξασφάλιση της ύπαρξης ρεύματος για ορισμένο χρονικό διάστημα, σε περίπτωση διακοπής.

Στοιχεία μηχανογραφικού προγράμματος

- Κατέγραψε ποια είναι τα σημαντικότερα πεδία χρήσης του προγράμματος (π.χ. λογιστήριο, τμήμα προμηθειών κλπ.).
- Κατέγραψε ποια έκδοση του προγράμματος χρησιμοποιείται.
- Κατέγραψε ποιες εφαρμογές του προγράμματος χρησιμοποιούνται και ποιος είναι ο βαθμός χρήσης τους.
- Εξέτασε αν το πρόγραμμα χρησιμοποιείται σε όλες τις εταιρικές διαδικασίες / κύκλους ελέγχου.
- Κατέγραψε τη μέθοδο μέσω της οποίας διασφαλίζεται το σύστημα δεδομένων του προγράμματος.
- Κατέγραψε πόσοι είναι οι ενεργοί χρήστες του προγράμματος.

Λήψη αρχείων back-up

- Επισκόπησε την πολιτική λήψης back-up, ως προς την συχνότητα λήψης.
- Επισκόπησε τις κασέτες με τα ληφθέντα αρχεία back-up ως προς τις ημερομηνίες λήψης των αρχείων και της ασφάλειας ως προς τον **περιορισμό πρόσβασης** σε αυτά.
- Που φυλάσσονται τα αρχεία back – up, σε χρηματοκιβώτιο, σε τραπεζική θυρίδα;
- Εξέτασε τα αρχεία back – up ως προς τη λειτουργία τους.

Σημείωση: δεν αρκεί να λαμβάνονται αρχεία back – up. Θα πρέπει σε τακτά χρονικά διαστήματα να επιβεβαιώνεται, ότι τα αρχεία λειτουργούν.

Πλάνο εναλλακτικής λειτουργίας

- Εξέτασε αν ο οργανισμός διαθέτει **πλάνο εναλλακτικής λειτουργίας**, προκειμένου να εξασφαλίσει ότι το σύστημα μπορεί να επανέρθει σε λειτουργία σε εύλογο χρονικό διάστημα, σε περίπτωση κρίσης.
- Επιβεβαίωσε ότι στο πλάνο εναλλακτικής λειτουργίας έχουν ιεραρχηθεί και συμπεριληφθεί, οι σημαντικές περιοχές / περιοχές υψηλής σημασίας και τα σημαντικά συστήματα τα οποία θα πρέπει να λειτουργήσουν άμεσα μετά την κρίση.
- Επιβεβαίωσε ότι το πλάνο εναλλακτικής λειτουργίας φέρει **έγκριση** της Γενικής Διεύθυνσης ή και Διοικητικού Συμβουλίου.
- Επισκόπησε τις αναφορές αποτελεσμάτων των δοκιμών του πλάνου εναλλακτικής λειτουργίας (αν δοκιμάζεται). Εντόπισε τα αδύναμα σημεία που προκύπτουν από τις δοκιμές και έλεγξε για τις διορθωτικές ενέργειες.

- **Ερώτημα κατανόησης: Έλεγχος πληροφοριακών συστημάτων**

Που θα επικεντρωθούν οι Εσωτερικοί Ελεγκτές, κατά τον έλεγχο των πληροφοριακών συστημάτων;

Προτεινόμενη απάντηση: Ένας έλεγχος στα πληροφοριακά συστήματα είναι ουσιαστικά ένας έλεγχος επί των δικλείδων που το σύστημα ενσωματώνει. Σε ολοένα αυξανόμενο βαθμό στους σύγχρονους οργανισμούς, τα ψηφιακά πληροφοριακά συστήματα καθίστανται ζωτικής σημασίας για τη λειτουργία του. Συνεπώς οι δικλείδες που αυτά ενσωματώνουν είναι από τις πιο σημαντικές που υπάρχουν στους οργανισμούς. Οι Εσωτερικοί Ελεγκτές θα επικεντρωθούν στα εξής:

- *Διαχείριση λειτουργικού συστήματος,*
- *Διαχείριση βάσεων δεδομένων,*
- *Διαχείριση ανάπτυξης συστημάτων,*

- *Διαχείριση προβλημάτων,*
- *Διαχείριση ελλείψεων στα συστήματα,*
- *Διαχείριση δικτύου,*
- *Διαχείριση υποδομής,*
- *Διαχείριση προσβάσεων,*
- *Διαχείριση λειτουργικού συστήματος.*

Περιεχόμενα ερωτημάτων / παραδειγμάτων κεφαλαίου

- Ερώτημα κατανόησης: Κατανόηση περιβάλλοντος και λειτουργίας
- Παράδειγμα κατανόησης: Έλεγχος πληροφοριακών συστημάτων