Διασφάλιση της Ποιότητας στις Υπηρεσίες Πληροφόρησης

Τμήμα Αρχειονομίας – Βιβλιοθηκονομίας
Ιόνιο Πανεπιστήμιο

Πέτρος Κωσταγιόλας
λέκτορας, Ιόνιο Πανεπιστήμιο
pkostagiolas@ionio.gr
(26610-87402 & 6944 456336)

Κέρκυρα
Ακαδημαϊκό Έτος 2012-2013

Χρηματοδότηση

Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Ιόνιο Πανεπιστήμιο**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Άδειες Χρήσης

Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons

Η πληροφορία σε κίνδυνο…

- Σήμερα, οργανώσεις, εταιρίες ακόμη και η ανθρώπινη μεμονωμένη παρουσία αντιμετωπίζουν ένα ευρύ φάσμα απειλών ασφάλειας. Είτε από:
  - ❖την αποτυχία εξοπλισμού
  - ❖την απάτη
  - ❖το βανδαλισμό
  - ❖την κλοπή
  - ❖τη δολιοφθορά
  - ❖τις φυσικές καταστροφές (πλημμύρα, πυκαγιά, κτλ)
  - ❖την τρομοκρατία σε πολλές χώρες

Ασφάλεια Δεδομένων: Σκοπιμότητα – rationale

Οι υπηρεσίες πληροφόρησης όπως και άλλοι οργανισμοί που διαχειρίζονται «ευαίσθητα» δεδομένα, οφείλουν να αναπτύσσουν μηχανισμούς για την ασφαλή διακίνηση της ηλεκτρονικής πληροφορίας μεταξύ δικτύων υπολογιστικών συστημάτων.

- Διαστάσεις Ασφάλειας Δεδομένων για τις Υπηρεσίες Πληροφόρησης:
  - Ο ρόλος της διοίκησης για την εφαρμογή Νόμων & διατάξεων
  - Δίδεται η απαραίτητη προσοχή και δεσμεύονται οι απαραίτητοι πόροι για αυτό τον σκοπό;
  - Υπάρχει κοινά αποδεκτός και αποτελεσματικός τρόπος για την διαχείριση και την ασφάλεια δεδομένων;
- **Διαστάσεις Μηχανισμών Διαχείρισης Ασφάλειας Δεδομένων:**
  - **Νομικό & Κανονιστικό υπόβαθρο (Legal & Data Protection Act & European Directives, 95/46/EC)**
  - **Πρότυπα Ασφάλειας Δεδομένων** (εφαρμογή του BS 7799)
- **Το Διεθνές Πρότυπο 27001:2005**

BS 7799, ISO/IEC 17799, ISO/IEC 27001

- **1995**: το Βρετανικό Ινστιτούτο Προτύπων (British Standards Institute, BSI) εκδίδει το πρότυπο BS 7799 Part 1. Συντάχθηκε από την Κυβερνητική Υπηρεσία Εμπορίου και Βιομηχανίας της Μεγάλης Βρετανίας
- **2000**: υιοθετήθηκε από τον Διεθνή οργανισμό Πιστοποίησης (International Organization for Standardization, ISO), ως ISO/IEC 17799 "Information Technology - Code of practice for information security management
- **2005**: αναθεωρήθηκε
- **Ιούλιος του 2007**: μετονομάστηκε σε ISO/IEC 27002.

Περιγραφή των προτύπων (1/2)

Το πρότυπο BS7799, περιλαμβάνει δύο μέρη

- BS7799-1:1999 Part1. Code of practice for Information Security Management (Κώδικας πρακτικής για τη διαχείριση ασφάλειας πληροφοριών)
- και BS 7799-2:1999 Part 2. Specification for Information Security Management Systems (Προδιαγραφή για τα συστήματα διαχείρισης ασφάλειας πληροφοριών).

Περιγραφή των προτύπων (2/2)

- Τα δύο πρότυπα της σειράς BS7799 είναι συμπληρωματικά.
- Το πρότυπο ISO/IEC 17799:2000 έχει την μορφή κατευθυντήριων οδηγιών και συστάσεων για την ανάπτυξη ολοκληρωμένων Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών.
- Το πρότυπο BS 7799-2:2002 περιλαμβάνει τις απαιτήσεις και προδιαγραφές των Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών. Παρέχει μια δομημένη προσέγγιση στην ανάπτυξη ενός πλαισίου διαχείρισης της ασφάλειας πληροφοριών και καταγράφει 10 σημεία ελέγχου (controls) με στόχο τον εντοπισμό, την διαχείριση και την ελαχιστοποίηση των κινδύνων στους οποίους εκτίθεται η πληροφορία του οργανισμού.
- Από τα δύο πρότυπα της σειράς BS7799, μόνον το πρότυπο BS 7799-2:2002 μπορεί να πιστοποιηθεί.

Διαδικασία εφαρμογής

Για την ανάπτυξη και εφαρμογή Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) σε έναν οργανισμό, σύμφωνα με τις απαιτήσεις του προτύπου BS7799-2:2002, απαιτούνται οι εξής γενικές ομάδες ενεργειών:

- Καθορισμός της γενικής στρατηγικής του οργανισμού και ανάπτυξη και συγγραφή της Πολιτικής Ασφάλειας
- Εντοπισμός των κρίσιμων στοιχείων πληροφοριών του οργανισμού (informationassets) που θα πρέπει να προστατευθούν
- Εκτίμηση των διαφόρων κινδύνων (risk assessment) που απειλούν τα παραπάνω στοιχεία πληροφοριών.
- Ανάπτυξη του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
- Εκπαίδευση του προσωπικού που κατέχει τις θέσεις-κλειδιά για την λειτουργία του συστήματος.
- Εφαρμογή του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών στον οργανισμό

Διεθνή πρότυπα Ασφάλειας Δεδομένων (BS 7799:2006): Σύνοψη Περιεχομένου

Ο Βρετανικός Οργανισμός Τυποποίησης (British Standards) εξέδωσε ένα γενικό πρότυπο που είναι διεθνώς αποδεκτό (BS 7799), όπως και ειδικό κώδικα ασφαλούς διαχείρισης της πληροφορίας (Code of Practice for Information Security Management).

- Διακριτές ενότητες-βήματα για την ανάπτυξη πολιτικής για την ασφάλεια δεδομένων:
  - Καθορισμός Πολιτικής για την Ασφάλεια Δεδομένων ***(Information Security Policy, ISP)***
  - Καθορισμός Σημείων Επιθεώρησης **(Targets of Evaluation, TOE)**
  - Καθορισμός Σημείων Ασφάλειας **(Security Targets, ST)**
  - Επιθεώρηση **(Evaluation)**
  - Πιστοποίηση **(Certification)**

Το Βρετανικό Πρότυπο BS 7799:2006

BS 7799-3:2006

BRITISH STANDARD

Information security management systems –

Part 3: Guidelines for information security risk management

ICS 35.020; 35.040

Το Διεθνές Πρότυπο ISO 27001:2005

BS ISO/IEC 27001:2005

INTERNATIONAL STANDARD

ISO/IEC 27001

First edition
2005-10-15

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Επισκόπηση θεμάτων Περιβαλλοντικής Διαχείρισης

- Βασικές έννοιες για την Προστασία του Περιβάλλοντος
- Πράσινες Βιβλιοθήκες
- Ανακύκλωση στις υπηρεσίες πληροφόρησης
- Εξοικονόμηση Ενέργειας στις Υπηρεσίες Πληροφόρησης
- Συμπεράσματα

Σύστημα Περιβαλλοντικής Διαχείρισης

Είναι μια μεθοδολογία συστηματοποίησης των διεργασιών μιας επιχείρησης με σκοπό τη βελτίωση των περιβαλλοντικών και οικονομικών της επιδόσεων

Πλεονεκτήματα από την ανάπτυξη ενός ΣΠΔ:

- Βελτίωση περιβαλλοντικών επιδόσεων
- Μείωση αποβλήτων και προστασία της ανθρώπινης υγείας
- Μείωση δαπανών (οικονομικά οφέλη)
- Βέλτιστη χρήση πόρων και εξοικονόμηση ενέργειας
- Βελτίωση της οργάνωσης της επιχείρησης
- Αποδοχή από τους υπεύθυνους και το κοινό
- Βελτίωση της δημόσιας εικόνας

Πράσινες Βιβλιοθήκες

- www.greenlibraries.org
  - ιστοσελίδα αφιερωμένη στις λεγόμενες «Πράσινες Βιβλιοθήκες» ➔βιβλιοθήκες που χρησιμοποιούν πρακτικές φιλικές προς το περιβάλλον και ευνοούν την αειφόρο ανάπτυξη
  - Κατάλογο των «Πράσινων βιβλιοθηκών» των Ηνωμένων Πολιτειών και του Καναδά
  - Λίστα *πράσινων πηγών*

Πράσινες Βιβλιοθήκες

- *Rosemary Garfoot Public Library*
  - Στο κεντρικό αναγνωστήριο έχει τοποθετηθεί μία σειρά από παράθυρα που κοιτάνε στο βορρά, σχεδιασμένα να συλλαμβάνουν το φως της ημέρας, αλλά και να κρατούν τη ζέστη μακριά.
  - Ο χώρος δροσίζεται με ανεμιστήρες οροφής, αποφεύγοντας την χρήση των air conditioners
  - Αισθητήρες φωτός και κίνησης ελέγχουν τον φωτισμό
  - Αναφορά στην ενεργειακή κατανάλωση του κτιρίου εμφανίζεται σε πραγματικό χρόνο στον ιστότοπο: www.scls.lib.wi.us/csp/
  - Η βιβλιοθήκη διαθέτει συλλογή με τεκμήρια που αφορούν το περιβάλλον τόσο για τους ενήλικες όσο και για τα παιδιά

Ανακύκλωση χαρτιού

<u>Λόγοι ανάπτυξης προγράμματος ανακύκλωσης:</u>

- Διατήρηση φυσικών πόρων (δάση)
- Μείωση κατανάλωσης πολύτιμων πρώτων υλών
- Εξοικονόμηση ενέργειας
- Μείωση απορριμμάτων
- Μείωση κόστους συλλογής και διάθεσης απορριμμάτων

Εξοικονόμηση Ενέργειας στις Υπηρεσίες Πληροφόρησης

- Αξιοποίηση του υπάρχοντος εξοπλισμού με τη χρήση ενέργειας στη μέγιστη απόδοση
  - Επαναρρύθμιση των συστημάτων ελέγχου,όπως:
    - Ρύθμιση θερμοστάτη σε λογική θερμοκρασία
    - Συχνή εξαέρωση των καλοριφέρ
  - Επισκευή διαρροών
  - Επαναπρογραμματισμός καταναλώσεων, (ενεργειακός έλεγχος στο κτίριο της βιβλιοθήκης)
  - Εξοικονόμηση χαρτιού
  - Κλείσιμο διακοπτών όταν δεν λειτουργούν
  - Εξοπλισμός γραφείου (υπολογιστές, φωτοτυπικά, εκτυπωτές) με τη μεγαλύτερη ενεργειακή αποδοτικότητα
  - Συντήρηση του καυστήρα/λέβητα
  - Μόνωση
  - Ανακύκλωση

Σύνοψη ISO 14000/ISO 14001:2004

Η ανάπτυξη συστήματος περιβαλλοντικής διαχείρισης πέραν των γενικών στοιχείων που αναλύονται στην συνέχεια αφορά και στην διαμόρφωση μιας νέας κουλτούρας για την ενίσχυση της ψηφιοποίησης της πληροφορίας (το μεγαλύτερο μέρος των βιβλιοθηκών στον τρίτο κόσμο βασίζονται στο χαρτί, ενώ στην Ευρώπη είναι μικτές) και στην ανακύκλωση.

- **Η διαμόρφωση της Περιβαλλοντικής Πολιτικής.**
- **Η διεξαγωγή Περιβαλλοντικής Ανάλυσης των συνιστωσών προστασίας του περιβάλλοντος.**
- **Η θέσπιση Περιβαλλοντικών Στόχων και Προγράμματος.**
- **Ο σχεδιασμός Συστήματος Περιβαλλοντικής Διαχείρισης.**
- **Η διεξαγωγή αυτοτελώς ή μέσω τρίτων Περιβαλλοντικών Ελέγχων.**
- **Περιβαλλοντική Δήλωση.**

Το Διεθνές Πρότυπο ISO 14001:2004

INTERNATIONAL STANDARD

ISO 14001

Second edition
2004-11-15

Environmental management systems — Requirements with guidance for use

Systèmes de management environnemental — Exigences et lignes directrices pour son utilisation

Σύνοψη BSI OHSAS 18001:1999

- Απαίτηση για καθιέρωση Πολιτικής όσον αφορά την Υγεία και Ασφάλεια της Εργασίας
- Ανάγκη αναγνώρισης της ταυτότητας των κινδύνων στον χώρο της βιβλιοθήκης
- Εντοπισμός και ικανοποίηση ισχύουσας Νομοθεσίας *(μεταξύ άλλων, άρθρα 7 & 8 του Π.Δ. 17/96)*
- Καθιέρωση στόχων για τη βελτίωση της ασφάλειας και της υγείας της εργασίας
- Σχεδιασμός Προγραμμάτων διαχείρισης των κινδύνων που εντοπίζονται στον εργασιακό χώρο
- Εκπαίδευση και εγρήγορση προσωπικού σε θέματα υγείας και ασφάλειας της εργασίας
- Σχεδιασμός προγραμμάτων για απόκριση σε έκτακτες ανάγκες
- Απαιτήσεις για παρακολούθηση και μέτρηση της αποδοτικότητας του συστήματος
- Απαιτήσεις για πραγματοποίηση Επιθεωρήσεων
- Ανασκόπηση του Συστήματος, σε τακτά χρονικά διαστήματα, από τη Διοίκηση

Το πρότυπο OHSAS 18001:1999

Contents

Εκτίμηση Επαγγελματικού Κινδύνου