Sécurité des systèmes d'information, synthèse

-Réference: **PL-35** -Durée: **3 Jours (21 Heures)**

Les objectifs de la formation

- Aucune connaissance particulière

A qui s'adesse cette formation ?

POUR QUI :

- Maîtriser le processus de gestion des risques de sécurité de l'information Utiliser les référentiels et les normes associées Connaître le cadre juridique Définir et piloter la mise en oeuvre de solutions

Programme

- **Introduction à la gestion des risques**
  - La définition du risque et ses caractéristiques : potentialité, impact, gravité.
  - Les différents types de risques : accident, erreur, malveillance.
  - La classification DIC : Disponibilité, Intégrité et Confidentialité d'une information.
  - Les contre-mesures en gestion des risques : prévention, protection, report de risque, externalisation.
- **RSSI : chef d'orchestre de la sécurité**
  - Quels sont le rôle et les responsabilités du Responsable Sécurité SI ? Vers une organisation de la sécurité, le rôle des "Assets Owners".
  - Gestion optimale des moyens et des ressources alloués.
  - Le Risk Manager dans l'entreprise ; son rôle par rapport au Responsable Sécurité SI.
- **Les cadres normatifs et réglementaires**
  - Les réglementations SOX, COSO, COBIT.
  - Pour qui ? Pour quoi ? Vers la gouvernance du système d'information.
  - Les liens avec ITIL et CMMI.
  - La norme ISO 27001 dans une démarche système de management de la sécurité de l'information.
  - Les liens avec ISO 15408 : critères communs, ITSEC, TCSEC.
  - Les atouts de la certification ISO 27001 pour les organisations.

Programme

- **Le processus d'analyse des risques**
  - Identification et classification des risques.
  - Risques opérationnels, physiques, logiques.
  - Comment constituer sa propre base de connaissances des menaces et vulnérabilités ? Utiliser les méthodes et référentiels : EBIOS/FEROS, MEHARI.
  - La démarche d'analyse de risques dans le cadre de l'ISO 27001, l'approche PDCA (Plan, Do, Check, Act).
  - Le standard ISO 27005 et les évolutions des méthodes françaises.
  - De l'appréciation des risques au plan de traitement des risques : les bonnes pratiques.
- **Les audits de sécurité et le plan de sensibilisation**
  - Processus continu et complet.
  - Les catégories d'audits, de l'audit organisationnel au test d'intrusion.
  - Les bonnes pratiques de la norme 19011 appliquées à la sécurité.
  - Comment créer son programme d'audit interne ? Comment qualifier ses auditeurs ? Apports comparés, démarche récursive, les implications humaines.
  - Sensibilisation à la sécurité : qui ? quoi ? comment ? Définitions de Morale/Déontologie/Ethique.
  - La charte de sécurité, son existence légale, son contenu, sa validation.
- **Le coût de la sécurité et les plans de secours**
  - Les budgets sécurité.
  - La définition du Return On Security Investment (ROSI).
  - Les techniques d'évaluation des coûts, les différentes méthodes de calcul, le Total Cost of Ownership (TCO).
  - La notion anglo-saxonne du "Payback Period".
  - La couverture des risques et la stratégie de continuité.
  - Plans de secours, de continuité, de reprise et de gestion de crise, PCA/PRA, PSI, RTO/RPO.
  - Développer un plan de continuité, l'insérer dans une démarche qualité.
- **Concevoir des solutions optimales**
  - Démarche de sélection des solutions de sécurisation adaptées pour chaque action.
  - Définition d'une architecture cible.
  - La norme ISO 1540 comme critère de choix.
  - Choisir entre IDS et IPS, le contrôle de contenu comme nécessité.
  - Comment déployer un projet PKI ? Les pièges à éviter.

Programme

- Les techniques d'authentification, vers des projets SSO, fédération d'identité.
- La démarche sécurité dans les projets SI, le cycle PDCA idéal.

- **Supervision de la sécurité**
  - Gestion des risques : constats, certitudes.
  - Indicateurs et tableaux de bord clés, vers une démarche ISO et PDCA.
  - Externalisation : intérêts et limites.

- **Les atteintes juridiques au Système de Traitement Automatique des Données**
  - Rappel, définition du Système de Traitement Automatique des Données (STAD).
  - Types d'atteintes, contexte européen, la loi LCEN.
  - Quels risques juridiques pour l'entreprise, ses dirigeants, le RSSI ?

- **Recommandations pour une sécurisation "légale" du SI**
  - La protection des données à caractère personnel, sanctions prévues en cas de non-respect.
  - De l'usage de la biométrie en France.
  - La cybersurveillance des salariés : limites et contraintes légales.
  - Le droit des salariés et les sanctions encourues par l'employeur.

(+212) 5 22 27 99 01 (+212) 6 60 10 42 56 Contact@skills-group.com

Nous sommes à votre disposition :
De Lun - Ven 09h00-18h00 et Sam 09H00 – 13H00

Angle bd Abdelmoumen et rue Soumaya, Résidence Shehrazade 3, 7éme étage N° 30
Casablanca 20340, Maroc