Les fondamentaux de la sécurité des SI
assurer et améliorer la sécurité de votre SI

Séminaire de 3 jours - 21h
Réf : FTS - Prix 2024 : 2 890€ HT

Avec l'explosion d'Internet qui a multiplié les opportunités de développement, la sécurité des systèmes d'information est devenue un enjeu majeur pour toutes les entreprises. Cette formation très riche vous présentera l'ensemble des actions et des solutions permettant d'assurer et améliorer la sécurité de votre SI. Vous verrez ce qu'est une analyse des risques, comment mettre en œuvre des solutions de sécurité ainsi que les thématiques assurantielles et juridiques intimement liées à l'application d'une politique de sécurité.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Comprendre le processus de gestion des risques des SI

Connaître les référentiels et les normes associées

Apprendre le cadre juridique

Savoir piloter la mise en œuvre de solutions

LE PROGRAMME

dernière mise à jour : 11/2019

1) La gestion des risques et les objectifs de sécurité

- 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.

2) Le métier du RSSI

- Quels sont le rôle et les responsabilités du Responsable Sécurité SI ?
- Vers une organisation de la sécurité, le rôle des "Assets Owners".
- Comment mettre en place une gestion optimale des moyens et des ressources alloués.
- Le Risk Manager dans l'entreprise, son rôle par rapport au Responsable Sécurité SI.

3) Les normes et les réglementations

- 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.

4) L'analyse des risques informatiques

- Comment mettre en place une démarche d'identification et de classification des risques.
- Risques opérationnels, physiques, logiques.
- Comment constituer sa propre base de connaissances des menaces et vulnérabilités ?

PARTICIPANTS

Toutes les personnes souhaitant apprendre les fondamentaux de la sécurité des SI.

PRÉREQUIS

Avoir suivi la formation "Introduction à la sécurité informatique".

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Méthodes et référentiels : EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)/FEROS, MEHARI.
- La démarche d'analyse de risques dans le cadre de l'ISO 27001, l'approche PDCA (Plan, Do, Check, Act).
- Quels sont les apports du standard ISO 27005 et les évolutions des méthodes françaises.
- De l'appréciation des risques au plan de traitement des risques : les bonnes pratiques.

5) Le processus d'un audit de sécurité

- 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.

6) Le plan de secours et le coût de la sécurité

- La couverture des risques et la stratégie de continuité.
- L'importance des 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.
- Comment définir les budgets sécurité.
- La définition du Return On Security Investment (ROSI).
- Quelles sont les techniques d'évaluation des coûts, les différentes méthodes de calcul, le Total Cost of Ownership (TCO).
- La notion anglo-saxonne du "Payback Period".

7) Les solutions et les architectures de sécurité

- Démarche de sélection des solutions de sécurisation adaptées pour chaque action.
- Définition d'une architecture cible.
- La norme ISO 15408 comme critère de choix.
- Choisir entre IDS et IPS, le contrôle de contenu comme nécessité.
- Comment déployer un projet PKI ? Les pièges à éviter.
- Les techniques d'authentification, vers des projets SSO, fédération d'identité.
- La démarche sécurité dans les projets SI, le cycle PDCA idéal.

8) La supervision de la sécurité

- Comment mettre en place une démarche de gestion des risques : constats, certitudes...
- Quels sont les indicateurs et les tableaux de bord clés. Aller vers une démarche ISO et PDCA.
- Externalisation : quels sont les intérêts et quelles sont les limites ?

9) Les aspects juridiques

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

10) Les bonnes pratiques

- 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.

LES DATES

CLASSE À DISTANCE
2024 : 18 juin, 01 oct., 26 nov.

PARIS
2024 : 11 juin, 24 sept., 19 nov.