Formation Sécurité des Systèmes d'Information, synthèse

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Avec l'explosion du digital qui a multiplié les opportunités de développement, le management de la sécurité des Systèmes d'Information est devenu un enjeu majeur pour toutes les entreprises. Ce séminaire très riche vous présentera l'ensemble des actions et des solutions permettant d'assurer la sécurité de votre SI : de l'analyse des risques à la mise en oeuvre optimale de solutions de sécurité. Vous verrez également les thématiques assurantielles et juridiques intimement liées à l'application d'une politique de sécurité.

Référence	SSI
Durée	3 jours (21h)
Tarif	2 790 €HT
Repas	repas inclus

Objectifs

| 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

Public

| ingénieurs prenant les fonctions de RSSI
| directeurs ou responsables informatiques
| ingénieurs ou correspondants sécurité
| chefs de projet intégrant des contraintes de sécurité

Prérequis

| aucune connaissance particulière

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 4 au 6 juin 2024
du 9 au 11 septembre 2024
du 17 au 19 décembre 2024

PARIS

du 28 au 30 mai 2024
du 15 au 17 octobre 2024
du 10 au 12 décembre 2024

VOIR TOUTES LES DATES

Programme de la formation

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.

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.
| 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.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.