

Sécurité : RSSI

Référence : **SECRSSI**

Durée : **5 jours (35 heures)**

Certification : **Aucune**

Connaissances préalables

- Des notions de base en sécurité appliquée aux systèmes d'information constituent un plus
- Expérience au sein d'une direction informatique en tant qu'informaticien ou bonne connaissance générale des systèmes d'information

Profil des stagiaires

- Directeurs des systèmes d'information ou auditeurs en systèmes d'information souhaitant connaître les contours de la fonction et les rôles du RSSI
- Ingénieurs en sécurité des systèmes d'information souhaitant rapidement acquérir toutes les compétences leur permettant d'évoluer vers la fonction de RSSI
- Nouveaux ou futurs RSSI souhaitant se remettre à niveau et échanger pratiques du métier avec d'autres RSSI
- RSSI expérimentés souhaitant se remettre à niveau et échanger sur les bonnes

Objectifs

- Les bases pour la mise en place d'une bonne gouvernance de la sécurité des systèmes d'information
- Les connaissances techniques de base indispensables à la fonction de RSSI
- Pourquoi et comment mettre en oeuvre un SMSI en s'appuyant sur la norme ISO27001
- Les méthodes d'appréciation des risques
- Les enjeux de la SSI au sein des organisations
- Les stratégies de prise de fonction et des retours d'expérience de RSSI

Certification préparée

- Aucune

Méthodes pédagogiques

- Mise à disposition d'un poste de travail par participant
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions

Formateur

- Consultant-Formateur expert Management de la sécurité

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. Introduction

- Accueil
- Présentation de la fonction de RSSI avec mise en perspective par rapport à tous les aspects de son à tous les aspects de son environnement
- Production, direction, métiers, conformité, juridique, etc.

2. Aspects organisationnels de la sécurité

- Panorama des référentiels du marché
- Politiques de sécurité
- Rédaction
- Politiques globales, sectorielles, géographiques
- Conformité
- Gouvernance de la sécurité
- Indicateurs sécurité
- Gestion des incidents
- Aspects techniques de la sécurité
- Sécurité du système d'exploitation
- Sécurité des applications (sessions, injections SQL, XSS)
- Sécurité réseau (routeurs, firewall)
- Sécurité du poste de travail

3. Systèmes de management de la sécurité de l'information (norme ISO)

- Bases sur les SMSI
- Panorama des normes type ISO27000
- Bases sur ISO 27001 et ISO 27002

4. Préparation à l'audit

- Formation et communication
- Audit à blanc
- Documents à préparer
- Considérations pratiques
- Réception des auditeurs (SoX, Cour des comptes, Commission bancaire...)

5. Gestion de risques

- Méthodologies d'appréciation des risques EBIOS / MEHARI / ISO27005
- Analyse - évaluation - traitement et acceptation des risques

6. Aspects juridiques de la SSI

- Informatique et libertés
- Communications électroniques
- Conservation des traces
- Contrôle des salariés
- Atteintes aux STAD
- Charte informatique
- Administrateurs

7. Acteurs du marché de la sécurité

- Gestion des relations avec les partenaires / Infogérance
- Prestataires en sécurité

8. Stratégies de prise de fonction du RSSI

- Rôles du RSSI
- Relations avec les métiers, la DSI, la DG, les opérationnels
- Retour d'expérience
- Témoignage d'un RSSI (selon les opportunités)
- Questions / Réponses avec les stagiaires

Notre référent handicap se tient à votre disposition au [01.71.19.70.30](tel:0171197030) ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.