SECURITE DES SI : Devenir RSSI

49 heures
MG802

Objectifs pédagogiques

- Identifier toutes les facettes du métier de Responsable de la Sécurité du SI, son rôle et ses responsabilités
- Savoir construire une politique de sécurité efficace et gérer les risques du SI
- Avoir une vue d'ensemble des mesures techniques de protection des SI
- Disposer d'une méthodologie pour assurer la mise en oeuvre et le suivi de la sécurité
- Savoir quelles sont les bonnes pratiques pour construire son plan d'action et définir ses indicateurs

Public(s)

- Responsables métiers ou informatiques souhaitant évoluer vers le métier de RSSI
- RSSI opérationnels souhaitant appréhender les nouvelles missions du RSSI

Pré-requis

Bonne culture générale sur les infrastructures IT

Modalités pédagogiques

- Un tour d'horizon exhaustif des différents aspects de la mission de RSSI.
- Une approche méthodologique participative permettant des échanges entre les participants et le formateur sur des retours d'expériences concrets : le formateur accompagne des RSSI depuis plusieurs années dans l'accomplissement de leurs missions.
- Le support de formation est utilisé pour présenter les éléments théoriques et les applications pratiques dans le domaine de la sécurité des SI. Il est adapté au contexte actuel et aux obligations réglementaires en vigueur.
- Des documents annexes illustrent les cas concrets abordés durant la formation.

Moyens et supports pédagogiques

Les plus de cette formation Devenir Responsable de la Sécurité du Système d'Information
Un tour d'horizon exhaustif des différents aspects de la mission de RSSI.
Une approche méthodologique participative permettant des échanges entre les participants et le formateur sur des retours d'expériences concrets : le formateur accompagne des RSSI depuis plusieurs années dans l'accomplissement de leurs missions.
Le support de formation est utilisé pour présenter les éléments théoriques et les applications pratiques dans le domaine de la sécurité des SI. Il est adapté au contexte actuel et aux obligations réglementaires en vigueur.
Des documents annexes illustrent les cas concrets abordés durant la formation.

Modalités d'évaluation et de suivi

Évaluation en cours et fin de formation
Cette formation ne fait pas l'objet d'un contrôle des acquis via une certification

Formateur

Programme

1ERE PARTIE : LE MÉTIER DE RSSI, SON RÔLE, SES RESPONSABILITÉS, SON PÉRIMÈTRE D'ACTION ET SES MÉTHODES DE TRAVAIL (3 JOURS)

INTRODUCTION : QUELS SONT LES ENJEUX DE LA SSI ?
Quelques définitions, périmètres et terminologies de base
Les enjeux de la sécurité de l'information
La nature des menaces et des risques

LES MISSIONS DU RSSI
Conseiller la Direction Générale par rapport aux obligations légales et les risques SSI
Formaliser une stratégie et définir un plan d'actions
Définir un référentiel SSI
Participer à la mise en en place de la gouvernance
Conseiller et assister la maîtrise d'ouvrage pour la gestion des risques
Conseiller, assister et contrôler la maîtrise d'oeuvre pour le traitement des risques
Former, sensibiliser
Réaliser une veille proactive
Auditer et réaliser des contrôles de conformité et mesurer l'efficacité

LES OBLIGATIONS LÉGALES ET LES EXIGENCES SSI
Responsabilités civile délictuelle et contractuelle

Les obligations légales
PPST : Protection des informations relatives au potentiel technique de la nation
Les respect de la vie privée / Secret des correspondances
GDPR : General Data Protection Regulation
Loi pour une république numérique
SOX : Sarbanes Oaxley
LSF : La Loi de Sécurité Financière
LCEN : Loi Confiance dans l'Economie Numérique
LSQ : Loi Sécurité Quotidienne / Loi Godfrain
CPI : Code de la Propriété Intellectuelle
La directive "Network and Information Security"
LMP : Loi de Programmation Militaire

IDENTIFICATION DES AUTORITÉS COMPÉTENTES ET RÉFÉRENTIELS
ANSSI, PSSI x, RGS
Agence Française de la santé numérique
PCI DSS

LES CONTRATS

LA GOUVERNANCE DE LA SSI
Niveaux de maturité SSI et types d'organisation
Le comité de pilotage, arbitrage, suivi et homologation
Voie hiérarchique et voie fonctionnelle
Les articulations avec les autres filières (hiérarchique, sécurité des installations, gestion de crises, ...)
La notification d'incidents, la gestion d'alerte

FORMALISATION D'UNE STRATÉGIE SSI
Adjonction d'outils et bonnes pratiques
Orientée enjeux
Orientée SMSI
Les étapes de la formalisation d'une feuille de route
LA GESTION DES RISQUES
La norme ISO 31000
La norme ISO 27005 : l'assistance à la maîtrise d'ouvrage pour l'évaluation des besoins et événements redoutés, l'assistance à la maîtrise d'oeuvre pour le traitement des risques, le conseil pour la validation ou l'homologation
Études de cas
La norme ISO 27002
La norme ISO 27001

LA DÉFINITION D'UN RÉFÉRENTIEL SSI
Lettre d'engagement de la direction
Lettre de nomination du RSSI
La politique générale de protection de l'information
Comment construire la politique sécurité système d'information ?
Chartes
Guides et procédures

MISE EN OEUVRE D'UNE MÉTHODE D'INTÉGRATION SSI DANS LES PROJETS
EBIOS
Adaptée

2ÈME PARTIE : DE LA THÉORIE À LA PRATIQUE (3 JOURS)

L'ÉTAT DE L'ART DES SOLUTIONS TECHNIQUE DE SÉCURITÉ DU SI
La sécurité des accès : filtrages, authentifications, habilitations, détections, journalisations
La sécurité des échanges : chiffrements symétriques et asymétriques, infrastructure à gestion de clés publiques (PKI), les déclinaisons
La sécurité des serveurs : durcissement, hébergement
La sécurité des postes de travail sédentaires et mobiles
La sécurité des applications

LES ARCHITECTURES SSI
Périphériques
En profondeur

INTRODUCTION AUX PLANS DE CONTINUITÉ DES ACTIVITÉS ET PLANS DE SECOURS
Fondamentaux de la continuité des activités
Le modèle du BCI et de la norme ISO 22301
Les différents plans : PCA, PCO, PSI, PGC, PCOM...
Les phases d'un projet de PCA
LA PRISE EN COMPTE DU FACTEUR HUMAIN
Sensibilisation
Formation
Communication

LA VEILLE JURIDIQUE ET TECHNIQUE SSI

CONTRÔLE ET AUDIT
Définition des indicateurs de contrôle
Les tests intrusifs
Formalisation et mise à jour des tableaux de bord

CONSEILS GÉNÉRAUX POUR RÉUSSIR DANS SON MÉTIER DE RSSI
Les freins et les difficultés rencontrés par les RSSI (retour d'expérience)
La bonne appropriation et la bonne communication du rôle du RSSI
Les erreurs à ne pas commettre, les conseils d'accompagnement au changement