Formation Devenir Responsable de la Sécurité du Système d'Information

Appréhendez toutes les dimensions du métier

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

Tout le monde s'accorde à dire qu'une des pires choses qui puisse aujourd'hui arriver à une organisation (entreprise, administration, agence gouvernementale,...) est une cyber attaque entrainant une paralysie partielle ou totale de son activité ! Et ce sans même parler de vol de données qui, au-delà des conséquences immédiates de l'attaque en termes d'activité, entacherait durablement la réputation de l'organisation victime. On comprend dès lors pourquoi la protection de l'information et la sécurité des systèmes d'information revêt aujourd'hui une telle importance que les professionnels qui en ont la responsabilité sont de plus en plus impliqués dans les processus de gouvernance des organisations qui les emploient. Pour mener à bien leur mission, ils ne doivent donc plus seulement être « bon » techniquement, ils doivent également savoir construire et mettre en oeuvre des politiques de sécurité efficaces.

Référence	MGR802
Durée	7 jours (49h)
Tarif	5 090 €HT

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 10 au 25 juin 2025
du 25 août au 10 septembre 2025
du 29 sept. au 15 octobre 2025
du 17 nov. au 10 décembre 2025

VOIR TOUTES LES DATES

Objectifs

| 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
| Connaître les bonnes pratiques pour construire son plan d'action et définir ses indicateurs

Public

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

Prérequis

| Bonne culture générale sur les infrastructures IT

Programme de la formation

1ÈRE PARTIE : LE MÉTIER DE RSSI, SON RÔLE, SES RESPONSABILITÉS, SON PÉRIMÈTRE D'ACTION ET SES MÉTHODES DE TRAVAIL (4 jours)

Introduction : Quels sont les enjeux de la SSI ?

| Quelques définitions, périmètres et terminologies de base
| Enjeux, menaces et 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 et la maîtrise d'oeuvre
| 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
| Les lois LSF, LCEN et LSQ
| 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
| CNIL

Les contrats
| 6.1)

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
| La notification d'incidents, la gestion d'alerte

Formalisation d'une stratégie SSI
| Adjonction d'outils et bonnes pratiques
| Orientée enjeux ou orientée SMSI
| Les étapes de la formalisation d'une feuille de route

La gestion des risques
| La norme ISO 31000
| La norme ISO 27005
| 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, filtrages applicatifs (WAF, CASF), authentifications, habilitations, détections d'intrusion, journalisations, supervision
| La sécurité des échanges
| 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
| 17.1)

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

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.