Ageris group

Formation SSI : Prise en compte native de la sécurité informatique dans les projets

PLUS D'INFOS

- Contactez-nous

CONTACT REFERENT

- Commercial@ageris-group.com
- +33 3 87 62 06 00

MODALITES D'ACCES

- Accessible à distance
- Accessible en présentiel

DELAI D'ACCES

- La durée estimée entre la demande du stagiaire et le début de la formation est de 7 jours (peut être raccourci pour le mode distanciel)

ACCESSIBILITE AUX PERSONNES EN SITUATION D'HANDICAP

- Accessible à distance pour les personnes à mobilité réduite
- Pour connaître l'accessibilité aux salles de formation, vous pouvez nous joindre au +33 3 87 62 06 00

REFERENCE

- SSIPROJETS

TARIF

- Sur devis

DUREE DE LA FORMATION

- 2 jours, 14 heures

DATES DES SESSIONS

- Voir site internet

FINANCEMENT

- OPCO

FORMULE INTRA-ENTREPRISE

Formulaire : soumettez votre projet

METHODES

- Cours théorique
- Exemples concrets
- Evaluation des compétences par un quizz en cours et en fin de formation
- Support de cours remis au stagiaire en fin de formation

PRESENTATION DE LA FORMATION

Aujourd'hui, la sécurité des SI nécessite une implication et une adhésion forte de tous et plus particulièrement des directions métiers.
Seule l'intégration native de la SSI pourra permettre une sécurité conforme aux obligations légales et adaptées aux besoins et aux risques des directions métiers.
L'intégration native de la sécurité dans les projets est devenue obligatoire.
Cette formation a pour objectif de donner les éléments méthodologiques et techniques nécessaires pour améliorer la qualité du dialogue entre les maitrises d'ouvrage, les directions ou comités d'homologations, les RSSI et les maitrises d'œuvre en charge du projet.

OBJECTIFS DE CETTE FORMATION

- Comprendre comment améliorer la qualité du dialogue sécurité entre la maîtrise d'ouvrage et le chef de projet informatique en charge du projet
- Être en mesure de concevoir des architectures de systèmes d'information en adéquation avec les exigences règlementaires et les besoins métiers
- Savoir identifier les risques, concevoir et mettre en œuvre les dispositifs de sécurité afin de les réduire
- Pouvoir constituer un dossier d'homologation/validation du projet.

PUBLIC

Chefs de projet Informatique, Chefs de projet métier, Représentants de la maitrise d'ouvrage, Responsables sécurité des systèmes d'information, Directeur des systèmes d'information, Responsable des risques opérationnels, Maîtres d'œuvre.

PREREQUIS

Aucun prérequis n'est nécessaire.

PROGRAMME DETAILLE

1. L'identification des acteurs SSI dans le projet

- Le responsable des traitements
- Les directions métiers
- Les maitrises d'ouvrage
- Les maitres d'œuvre
- Le gestionnaire de risques ou le RSSI
- Le DPO
- Les sous-traitants

2. Rappel rapide sur les obligations légales par la Maîtrise d'ouvrage

- Les exigences liées au RGPD
- Les exigences liées au RGS
- Les exigences liées aux différents codes (santé, sécurité sociale, protection des mineurs, …)
- Les exigences SOX, Solvency II, Bâle, …
- Les exigences LPM

3. L'approche normative et méthodologique

- ISO 31000
- ISO 27005

Formation SSI : Prise en compte native de la sécurité informatique dans les projets

- Outil distanciel : Teams

POUR ALLER PLUS LOIN

- SSI – Devenir Responsable de la Sécurité des Systèmes d'Information (RSSI)
- SSI – Maîtriser l'analyse des risques du système d'information

PLUS D'INFOS

- Contactez-nous

- ISO 29134
- ISO 22301

4. L'approche méthodologique de la gestion des risques

- MEHARI
- EBIOS
- EBIOS RM
- "Adaptée"

5. L'intégration dans la gestion de projets

- En V
- En mode Agile

6. La formalisation des besoins de sécurité DICP

- Les liens entre informations, processus et ressources
- La formalisation des besoins DICP par les impacts
- Les pièges à éviter
- La consolidation dans les processus puis dans les ressources
- Le cas de la classification intrinsèque de la ressource
- Les cas particuliers de la confidentialité et les profils d'habilitation
- Les cas particuliers de la disponibilité et les paramètres RTO / RPO
- Les cas particuliers des besoins d'authentification (réciprocité, forces et non rejeu, …)
- La gestion des habilitations (le moindre privilège et la séparation des pouvoirs)
- Etudes de cas

7. L'identification des menaces et la gestion des risques

- Modélisation des risques, menaces, et vulnérabilités
- Cartographie et identification des niveaux de risques
- Les méthodes de traitement
- La réduction des risques par l'application des politiques institutionnelles, déclinées de l'ISO 27002 (PSSI E, PSSI MCAS, PGSSI- S, les règles d'hygiène ANSSI, …)
- L'évitement
- Le transfert
- L'acceptation
- L'identification des risques résiduels
- Comment monter son dossier de validation/homologation ?
- Le cas des AIPD pour la « security by design »
- Etudes de cas

8. La gestion de l'externalisation

- Les PAS
- Etudes de cas

9. Conclusion

10. Confidentialité des études et développements

11. La sécurité de la mise en production des SI

12. La sécurité de la maintenance des SI

Formation SSI : Prise en compte native de la sécurité informatique dans les projets

13. La documentation sécurisée des SI

- Etudes de cas

14. Conclusion

MODALITES D'EVALUATION

Validation des connaissances et compétences par un quizz à la fin de chaque chapitre.