SÉCURITÉ DES SI - Prendre en compte la SSI dans les projets

14 heures
SECU004

Objectifs pédagogiques
Aujourd'hui, la sécurité des SI nécessite une implication et une adhésion forte de tous et plus particulièrement des directions métiers, afin qu'elles ressentent les règles de sécurité comme des exigences appropriées à leurs contextes règlementaires et opérationnels, et non plus comme des contraintes. 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

Public(s)
Responsables sécurité des systèmes d'information, Directeurs des systèmes d'information, Responsables des risques opérationnels, Maîtres d'œuvre.

Pré-requis
Aucun

Modalités pédagogiques
Session sur demande

Moyens et supports pédagogiques
Support(s) de formation par alternant

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

- De l'adjonction d'outils extérieurs SSI à l'intégration native SSI
- L'identification des acteurs liées à la démarche et leurs responsabilités
- L'identification des obligations légales par la Maîtrise d'ouvrage
- La protection des données à caractère personnel
- 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
- L'approche méthodologique
- ISO 27005 - EBIOS - « Adaptée »
- 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 forte (réciprocité, force et non rejeu, …) - La gestion des habilitations (le moindre privilège et la séparation des pouvoirs)
- L'identification des menaces et 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 et comment remplir et faire remplir le PAS
- L'acceptation
- L'identification des risques résiduels
- Comment monter son dossier de validation/homologation ?
- Le cas des EIVP pour la « security by design »
- Sécurité des études et des développements de SI
- Confidentialité des études et développements.
- La sécurité de la mise en production des SI
- La sécurité de la maintenance des SI
- La documentation sécurisée des SI
- Etudes de cas