SECURITE DES SI | Maîtriser l'analyse des risques du SI Mettre en oeuvre une politique d'analyse de risques

14 heures
MG803

Objectifs pédagogiques

Appréhender les concepts fondamentaux de l'analyse de risques SSI
Savoir identifier les enjeux pour l'entreprise
Disposer d'une démarche complète pour mener à bien un projet d'analyse de risques
Découvrir les méthodes d'analyse et les solutions logicielles disponibles pour maîtriser les risques du SI

Public(s)

Appréhender les concepts fondamentaux de l'analyse de risques SSI
Savoir identifier les enjeux pour l'entreprise
Disposer d'une démarche complète pour mener à bien un projet d'analyse de risques
Découvrir les méthodes d'analyse et les solutions logicielles disponibles pour maîtriser les risques du SI

Pré-requis

Aucun

Modalités pédagogiques

Alternance théorie et pratique

Moyens et supports pédagogiques

Support(s) de formation par apprenant

Modalités d'évaluation et de suivi

Cette formation ne fait pas l'objet d'une évaluation des acquis.
Cette formation ne fait pas l'objet d'un contrôle des acquis via une certification

Formateur

Programme

Les concepts généraux de la gestion des risques
- Définition du risque et des typologies de menaces
- Modèle général de gestion des risques

Les acteurs impliqués dans la cartographie des risques
- La gouvernance à prévoir, les acteurs, leurs rôles et responsabilités
- La voie hiérarchique et les voies fonctionnelles
- Identification des risques juridiques : métier, civil, pénal, réglementaire, contractuel
- Identification des risques accidentels
- Identification des risques d'erreurs
- Identification des risques liés à la malveillance (cybercriminelle, concurrentielle, ludique, idéologique et stratégique) : les caractéristiques de compétence, temps, moyen, connaissance au préalable sur la cible, ...

Présentation de la norme ISO 31000
- Objectifs de la norme

Présentation de la norme ISO 27005
- Objectifs de la norme
- Présentation du contenu de la norme
- Démarche générale de l'analyse des risques
- Démarche d'appréciation et d'analyse des risques
- Classification
- Les pièges à éviter
- Présentation des référentiels d'analyse des menaces, des enjeux et des contraintes : la granularité et les domaines d'analyse
- Présentation des référentiels de vulnérabilité proposés par la norme
- Présentation des métriques d'appréciation des risques : les approches possibles
- La stratégie de traitement des risques, les objectifs et l'acceptation des risques selon la norme
- Les processus de communication et de surveillance des risques
- Les validations EIVP
- Les homologations RGS, PSSIx

La norme ISO 29134
- Objectifs de la norme
- Présentation du contenu de la norme
- Démarche générale de l'analyse des risques
- Démarche d'appréciation et d'analyse des risques
- Les validations AIPD

Les homologations RGS, PSSIx

- Objectifs
- Présentation du RGS
- Démarche d'homologation...

Études de cas

La prise en compte native des risques SSI dans les projets

- L'approche en V
- L'approche Agile
- EBIOS
- EBIOS RM
- MEHARI
- Adaptée
- La déclinaison Privacy by design du RGPD

Études de cas

La définition et la mise en oeuvre du Plan de Prévention des Risques (PPR)

- Notions principales et objectifs du PPR
- Le processus d'élaboration du PPR
- La définition des objectifs et des priorités de mise en oeuvre
- Introduction à la norme ISO 27002
- Le cas du Cloud ISO 27018
- Les relations avec les PCA et la norme 22301
- Les relations avec la gestion de crise

Les conseils de mise en oeuvre d'une gestion structurée des risques

- La gouvernance
- La mise en oeuvre du système de management de gestion des risques
- Le maintien en condition opérationnelle

La prise en compte du facteur humain dans la gestion du risque SI

- Direction générale
- Encadrement
- Acteurs DSI
- Représentant de la MOA
- Les utilisateurs
- Les solutions
- Études de cas

Les principes généraux relatifs aux systèmes de management de la sécurité

- Le système de management ISO 31000
- Présentation générale du modèle PDCA ISO 27001