FORMATION

SETYM Canada International
85, SAINTE-CATHERINE OUEST, 10E ÉTAGE
MONTRÉAL, QUÉBEC, CANADA H2X 3P4
+1 (514) 939-2200 | SETYM@SETYM.COM
setym.com

NOUVEAU

Gestion des risques des systèmes d'information

L'information est un actif fondamental et sa sécurité est devenue un enjeu majeur pour tout organisme. La gestion des risques des systèmes d'information joue un rôle essentiel dans la préservation de l'intégrité, de la confidentialité et de la disponibilité des données. Elle vise à identifier, évaluer et atténuer les menaces potentielles qui pèsent sur les systèmes d'information, tout en garantissant une continuité opérationnelle efficace.

Basé sur les normes ISO 27000 (normes sur les systèmes de management de la sécurité de l'information) et la méthode MEHARI (Méthode Harmonisée d'Analyse des Risques), ce séminaire a pour objectif de donner aux participants une connaissance approfondie de la gestion des risques des systèmes d'information, des outils et des techniques pour identifier, évaluer, contrôler et atténuer ces risques.

OBJECTIFS PRATIQUES

- **Maîtriser** la gouvernance de la sécurité de l'information.
- **Comprendre** les référentiels internationaux et les normes ISO 27000.
- **Apprendre** à cartographier des risques, des systèmes d'information.
- **Approfondir** vos connaissances du processus d'identification, d'évaluation, de contrôle et traitement des risques.
- **Acquérir** une maîtrise complète du cycle de gestion des risques en utilisant la méthodologie et les outils de MEHARI.

CLIENTÈLE CIBLE :

- Responsables de la sécurité du système information
- Responsables des risques, responsables qualité
- Directeurs, cadres ou responsables informatique, Responsables RH, Auditeurs internes et externes
- Chefs de projet intégrant des contraintes de sécurité
- Ingénieurs ou correspondants sécurité.

DURÉE : 2 semaines

THÈMES ET CONTENUS

- **Fondamentaux de la sécurité des systèmes d'information :** Définitions, concepts-clés, cadres de référence et normes. Actifs informationnels : actifs processus/information et actifs support. Critères DIC (Disponibilité, Intégrité, Confidentialité). Composantes du risque : vulnérabilités et menaces. Types de risques : accident, erreur, malveillance.
- **Normes internationales ISO 27000 et SMSI :** Système de management de la sécurité de l'information. Exigences en matière de sécurité de l'information (ISO 27001). Guide des bonnes pratiques (ISO 27002). Méthode MEHARI : démarche, référentiels et outils.
- **Cartographie des risques des systèmes d'informations :** Identification des actifs informatiques. Évaluation des menaces et des vulnérabilités. Analyse des chaînes de causalité, impacts et probabilités. Élaboration et gestion d'une cartographie des risques. Repères et tendances en matière de sinistres informatiques.
- **Conception des services de sécurité optimaux :** Sécurité physique : accès, locaux, archive. Sécurité des infrastructures, systèmes et des réseaux. Sécurité de l'exploitation, des applicatifs et des données. Sécurité des projets.
- **Audit de la sécurité des systèmes d'informations :** Objectifs. Méthodologies et techniques d'audit. Normes ISO 19011 et ISO 27005. Sensibilisation à la sécurité. Surveillance et évaluation continue des risques des systèmes d'information.
- **Gestion de la continuité des activités et reprise après sinistre :** Couverture des risques et stratégie de continuité. Plan de continuité d'activité et plan de secours informatique. PSI, organisation et procédures. Démarche d'élaboration.
- **Gouvernance et politique de sécurité :** COBIT, cadre de gouvernance et directives. Politique et charte de sécurité. Mise en œuvre de l'organisation et supervision de la sécurité. Conformité et cadre réglementaire. Indicateurs et mesures d'efficacité (ISO 27004).
- **Atelier pratique avec MEHARI :** Référentiels MEHARI. Apprentissage de l'outil MEHARI. Questionnaires d'audit. Exercice de simulation.