



Institut Canadien de Développement International

Cybersécurité et protection des données à caractère personnel

Objectif Global

Renforcer la protection des systèmes d'information et des données à caractère personnel par une approche intégrée couvrant gouvernance, prévention, contrôle des accès, sécurité technique, gestion des incidents, continuité et conformité. La formation vise à permettre aux responsables non seulement de comprendre les menaces, mais surtout d'organiser des responsabilités et des contrôles proportionnés aux actifs critiques.

Contexte

La numérisation accroît la dépendance aux systèmes et la concentration de données sensibles. Les administrations sont exposées à l'hameçonnage, aux rançongiciels, aux compromissions de comptes, aux erreurs internes, aux fuites de données et aux interruptions de service. Les dispositifs purement techniques sont insuffisants lorsque les droits d'accès sont mal gérés, les sauvegardes non testées ou les responsabilités mal définies. La résilience exige une gouvernance qui articule prévention, détection, réaction, reprise et retour d'expérience.

Objectifs Spécifiques

- Identifier les actifs critiques, données sensibles, menaces et scénarios de risque prioritaires.
- Mettre en place une gouvernance cyber précisant rôles, responsabilités et niveaux d'escalade.
- Renforcer gestion des identités, habilitations, privilèges et séparation des fonctions.
- Organiser prévention, détection, journalisation, sauvegardes et continuité des services.
- Structurer réponse aux incidents, notification, conservation des preuves et retour d'expérience.
- Intégrer les exigences de confidentialité et de protection des données aux projets numériques.
- Piloter la sécurité par des indicateurs de risque, incidents, délais de correction et résilience.

Thèmes Abordés

Cartographie des actifs et risques cyber : Systèmes critiques, données sensibles, dépendances, menaces, vulnérabilités et hiérarchisation des scénarios selon impact et probabilité.

Identités, accès et privilèges : Cycle de vie des comptes, moindre privilège, authentification renforcée, revues d'accès et séparation des fonctions.

Prévention, détection et surveillance : Hygiène cyber, correctifs, configuration, sauvegardes, journalisation, alertes et détection de comportements anormaux.

Protection des données personnelles : Finalité, minimisation, conservation, accès, partage, traçabilité et intégration de la confidentialité dans les processus.

Gestion des incidents et continuité : Détection, escalade, confinement, reprise, communication, preuves et tests réguliers des plans de continuité.

Gouvernance et indicateurs de sécurité : Comité de sécurité, responsabilités métiers-DSI, registre des risques, suivi des incidents, délais de correction et exercices.

Étude de cas de crise cyber : Traitement d'un scénario de compromission avec décisions de confinement, continuité, notification, communication et amélioration post-incident.

Public Cible

Cette formation s'adresse aux administrations et entreprises publiques, directions des systèmes d'information, responsables cybersécurité et protection des données, auditeurs, contrôleurs internes, juristes, responsables des ressources humaines, gestionnaires de données et cadres responsables de services numériques critiques.

Nos formations sont sujettes à annulation lorsque le nombre de participants n'est pas suffisant.



ICDI

Institut Canadien de Développement International

Contact

Tél: +1-514-225-6800

info@consultants-icdi.com