VISIO - Fondamentaux de la cybersécurité pour les collectivités territoriales

TOO141FCSC

En Visio-conférence, de 9h00 à 17h00

A distance - Synchrone

Inscrivez-vous au moins 3 mois avant le début du stage pour bénéficier d'un tarif préférentiel
Délai d'accès : Inscription jusqu'à la veille du démarrage de la session
Contactez Gaëlle (01 53 39 14 18,gaelle.ducher@adiaj.org) ou Julien (01 53 39 14 24, julien.laudat@adiaj.org) pour réaliser cette formation en INTRA

Objectifs

- Comprendre les enjeux de la cybersécurité dans le contexte des collectivités territoriales
- Découvrir les menaces spécifiques et les moyens de protection adapté
- Mettre en place des stratégies pour sécuriser les systèmes d'information locaux

Public Visé

Responsables de services, DSI (Directeurs des Systèmes d'Information), agents en charge de la gestion numérique des collectivités territoriales

Pré Requis

Avoir des connaissance en informatique ou justifier d'une expérience suffisante

Objectifs pédagogiques

Comprendre les enjeux de la cybersécurité dans le contexte des collectivités territoriales
Découvrir les menaces spécifiques et les moyens de protection adaptés
Mettre en place des stratégies pour sécuriser les systèmes d'information locaux

Méthodes et moyens pédagogiques

- Apports de connaissances théoriques
- Atelier pratique
- Echanges autour des questions/réponses
- Support documentaire via PADLET (présentation, fiches outils, guide pratique pour établir une politique de cybersécurité dans une collectivité, liste des outils et solutions de cybersécurité recommandés pour les collectivités, documentation sur les normes et réglementations applicables (ISO, RGPD))
- Encadrement assuré par l'ADIAJ Formation et/ou le formateur

Déroulement pédagogique et prérequis techniques de la classe virtuelle, à distance

- Chaque jour est séquencé en 4 séquences d'1h30. Pause de 15 à 30 minutes le matin et l'après-midi. Pause méridienne d'une heure.
- Chaque stagiaire sera invité à rejoindre une salle digitale, via un lien d'accès, un ID de réunion communiqué par mail, au minimum 15 minutes avant le début de la session, pour permettre de paramétrer sereinement sa connexion.
- Chaque stagiaire reste maître de sa connexion visuelle (caméra) et sonore (son), pour permettre de suivre en toute autonomie et dans le respect de tous.
- Matériel nécessaire : un ordinateur par stagiaire, une connexion internet, un navigateur compatible, une webcam et un micro.

Qualification Intervenant.e.s

Formatrice experte en intelligence artificielle, numérique et

Parcours pédagogique

Matinée (3h30)

• 9h00 – 9h30 : Introduction et enjeux
Présentation des objectifs de la formation.
Introduction aux enjeux spécifiques :
Pourquoi les collectivités territoriales sont une cible privilégiée ?
Impacts des cyberattaques.
Cas réel : Présentation d'une cyberattaque subie par une collectivité (exemple d'un ransomware ou d'une fuite de données).

• 9h30 – 10h30 : Comprendre les cybermenaces
Les principales menaces :
Ransomware (rançongiciels).
Phishing (hameçonnage).
Attaques par déni de service (DDoS).
Intrusions réseau et vols de données.
Les acteurs derrière les attaques :
Hackers, cybercriminels, insiders (agents internes malveillants).
Atelier pratique : Analyser des exemples d'attaques ciblant des collectivités.

• 10h30 – 10h45 : Pause

• 10h45 – 12h15 : Les bases de la protection
Stratégies de défense :
Importance des mises à jour régulières des logiciels et systèmes.
Gestion des mots de passe (création et rotation).
Gestion des accès (principe du moindre privilège).
Présentation des outils de protection :
Antivirus et pare-feu.
Systèmes de détection des intrusions (IDS).
Outils de sauvegarde et de récupération.
Atelier pratique : Élaborer une liste d'actions prioritaires pour sécuriser les données et systèmes de la collectivité.

• 12h15 – 12h30 : Synthèse de la matinée
Récapitulatif des menaces et des premières mesures de protection.
Introduction au volet organisationnel de l'après-midi.

• 12h30 – 13h30 : Pause déjeuner

Après-midi (3h30)

• 13h30 – 14h30 : Mettre en place une stratégie de cybersécurité

cybersécurité

Éléments d'une stratégie efficace :
Réalisation d'un audit de sécurité (évaluation des vulnérabilités).
Élaboration d'une politique de cybersécurité (charte, procédures).
Formation continue des agents.
Présentation des normes et cadres :
ISO 27001 (gestion de la sécurité de l'information).
Obligations liées au RGPD.
Atelier collaboratif : Élaborer les grandes lignes d'une politique de cybersécurité adaptée à une collectivité.

• **14h30 – 15h30 : Gestion des incidents et résilience**
Réagir face à un incident :
Détection, alerte, confinement, et récupération.
Communication de crise (interne et externe).
Plan de continuité d'activité (PCA) et plan de reprise après sinistre (PRS).
Étude de cas : Simulation d'un incident dans une collectivité
Les participants jouent le rôle de différents acteurs pour gérer une crise cyber (par exemple, une attaque par ransomware).

• **15h30 – 15h45 : Pause**

• **15h45 – 16h45 : Sensibilisation et culture de cybersécurité**
Sensibiliser les agents :
Formation régulière sur les menaces émergentes.
Mise en place de tests internes (ex. simulation d'e-mails de phishing).
Collaborer avec des partenaires :
Rôle de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).
Collaboration avec des prestataires externes.
Quiz de révision interactif : Questions clés sur les points abordés.

• **16h45 – 17h00 : Conclusion et évaluation**
Synthèse des apprentissages.
Questionnaire d'évaluation de la formation.
Remise d'un guide pratique pour sécuriser les collectivités (check-list, ressources externes, outils).

Initiez-vous à la cybersécurité avec ADIAJ. Maîtrisez les fondamentaux pour mieux protéger votre collectivité territoriale des cybermenaces.

Méthodes et modalités d'évaluation

Chaque stagiaire est invité à émarger sur EasySign, grâce à un mail d'invitation. L'émargement est obligatoire. L'équipe de l'ADIAJ est à votre disposition pour toute aide technique.
Modalités d'évaluation : Chaque stagiaire est invité par mail à compléter :
- Avant la formation : un questionnaire de positionnement via EvalOne, afin que chacun puisse nous faire remonter ses attentes.
- Après la formation : une Evaluation de la satisfaction des stagiaires via EvalOne.
Attestations de la formation : Certificat de réalisation à l'employeur et Attestation de fin de formation à l'apprenant.

Modalités d'Accessibilité

ADIAJ Formation est en capacité d'accueillir ou réorienter toute personne en situation de handicap. Pour assurer un suivi optimal, merci de nous contacter.
Référent handicap : Volodia TOURTCHINE - 01 53 39 14 17 - volodia.tourtchine@adiaj.org

Durée

7.00 Heures
1 Jour

Effectif

De 3 à 14 Personnes

Tarifs (net de taxes)

Inter (Par personne) :	**680.00**
Inter Adhérent (Par personne) :	**640.00**

Contactez-nous !

Gaëlle DUCHER
Responsable Ingénierie Formation
Tél. : 0153391418
Mail : gaelle.ducher@adiaj.org

ADIAJ Formation - Numéro de déclaration d'activité (ne vaut pas agrément de l'état) : 11.75.18.99.575

Association pour le Developpement de l'Information Administrative & Juridique
3, Rue Henri Poincaré - 75 020 PARIS - Tél.:01.53.39.14.14 - Contact mail :adiaj@adiaj.org - www.adiaj.org
N° Siret 380 426 353 00039 - N° APE 8559A