

Programme de formation

CYBER : protéger sa collectivité au quotidien

Formation à destination des élus – Cyber Sécurité



1 jour – 7 heures

09h00 – 12h30

14h00 – 17h30



Dates

A définir



Modalité et lieu

Présentiel



Tarifs

400€ net de TVA / élu
(éligible dans le cadre du DIFE)

Face à des cybermenaces de plus en plus présentes, les élus ont un rôle clé pour protéger leur collectivité et garantir la continuité du service public. Grâce à des cas concrets et des mises en situation, cette formation vous donnera les clés pour anticiper les risques, prendre les bonnes décisions et agir avec confiance.

OBJECTIFS DE LA FORMATION

À l'issue de la formation, le stagiaire sera capable de :

- Distinguer les principaux types de risques cyber susceptibles d'affecter une collectivité.
- Identifier les impacts potentiels d'une cyberattaque sur les services publics et les usagers.
- Définir le rôle des élus dans la prévention et la gestion des risques numériques.
- Identifier les bonnes pratiques à promouvoir au sein de leur collectivité.
- Déterminer les actions prioritaires à mettre en œuvre lors d'une crise cyber.

PREREQUIS ET CONDITION D'ADMISSION

Recommandations : savoir utiliser à minima les outils de bureautique et l'outil informatique.

Prérequis matériel : avoir un ordinateur portable ou à défaut en faire part à l'organisme de formation

Public concerné : tout élu souhaitant être sensibilisé aux risques cyber.

CONTENU DE LA FORMATION

1. Comprendre les risques cyber pour les collectivités
 - Éléments de contexte.
 - Panorama des risques cyber.
 - Pourquoi les collectivités sont-elles des cibles potentielles ?



Effectif minimum - maximum :

5 - 15

Accueil des personnes en situation de handicap :

Une personne référente sur l'accueil de personne en situation de handicap est formée au sein de l'ARNia pour permettre un accompagnement bienveillant sur les parcours de formation. • Votre contact Laetitia TACHIN : ltachin@arnia-bfc.fr

CONTACT :

ARNia formation
formation@arnia-bfc.fr
0970 609 909

Dernière mise à jour le :
20/07/26

2. L'impact d'une cyberattaque
 - Conséquences opérationnelles
 - Conséquences financières
 - Conséquences sur les usagers
 - Conséquences sur les élus et la collectivité
3. Le rôle des élus dans la cybersécurité
 - La cybersécurité : un enjeu de gouvernance
 - Pourquoi le sujet dépasse la seule DSI.
 - Un risque qui peut affecter la continuité du service public.
 - Présentation de NIS2.
 - Les responsabilités des élus
 - Définition des orientations
 - Arbitrages budgétaires
 - Suivi des risques
 - Protection des données
 - Adapter l'approche selon la taille de la collectivité
4. Les bonnes pratiques
 - Les questions à poser régulièrement
 - Les fondamentaux
 - Sensibilisation des agents
 - Gestion des prestataires
 - Protection des données personnelles
5. Réagir face à une attaque – Atelier de mise en situation
 - Les premières heures d'une attaque
 - Organisation de la cellule de crise
 - Communication de crise
 - Les acteurs à mobiliser

METHODES PÉDAGOGIQUES ET MOYENS TECHNIQUES

Méthodes pédagogiques :

- Apports théoriques
- Exercices pratiques
- Échanges et partages d'expériences
- Démonstration d'exemple appliqué à des situations réelles
- Analyses de situations rencontrées par les stagiaires
- Exercices de réflexion individuels ou en groupes.

Moyens matériels :

- Pour les formations à distance avoir :
 - Un ordinateur
 - Une connexion internet
 - Un casque audio/micro (si possible)
 - Une webcam
- Pour les formations en présentiel, mise à disposition :
 - D'une salle disposant d'une connexion internet
 - D'un vidéoprojecteur
 - D'un paper board ou d'un tableau blanc.

LES INTERVENANTS

Nos intervenants sont des experts dans leurs domaines d'intervention. Leur expérience en conseil et formation auprès des apprenants est le fruit de plusieurs années d'exercice dans leurs domaines. Ils évoluent et adaptent leurs interventions en fonction des besoins des apprenants.

SUIVI ET EVALUATION

En amont de la formation :

- Évaluation individuelle de la candidature,
- Évaluation des attentes et des besoins des apprenants,
- Évaluation du niveau des stagiaires.

En fin de formation :

- Questionnaire d'évaluation des acquis,
- Évaluation de la satisfaction des stagiaires,
- Feuilles de présence signées des participants et du formateur par demi-journée.

Après la formation :

- Envoi d'une attestation individuelle de fin de formation,
- Envoi d'un questionnaire de satisfaction à froid.

ARNia FORMATION

Organisme de formation, Agence Régionale du Numérique et de l'intelligence artificielle

3 bis rue de Suzon – 21000 DIJON

Site web : arnia-bfc.fr



N° assistance : 0970 609 909



formation@arnia-bfc.fr

