# Fiche Technique:Audit Cybersécurité au Togo

## Objectifs de la formation

- Diagnostiquer les vulnérabilités techniques, organisationnelles et humaines.
- Évaluer la conformité aux normes nationales et internationales.
- Établir un plan d’action priorisé pour renforcer la sécurité.
- Diminuer les risques d’incidents cybernétiques.
- Optimiser les ressources investies en cybersécurité.
- Fournir un support décisionnel aux dirigeants.

## Population cible

- Entreprises et organisations de toutes tailles et secteurs.
- Directions générales, responsables informatiques et RSSI.
- Équipes réseaux, infrastructures IT et décideurs en risques/conformité.
- Sociétés industrielles dans zones économiques spéciales.
- Entreprises de transport/logistique au port autonome de Lomé.
- Institutions financières et administrations publiques togolaises.

## Durée de la formation

| Étape | Activités principales | Durée estimée |
|---|---|---|
| Étape 1 | Diagnostic initial et collecte de données | 1 semaine |
| Étape 2 | Analyse documentaire et réglementaire | 1 à 2 semaines |
| Étape 3 | Rédaction des recommandations et plan d’action | 1 semaine |
| Étape 4 | Suivi et accompagnement post-audit | 2 à 4 semaines |

## Programme de la formation

### Étape 1 : Diagnostic initial

- Collecte d’informations sur infrastructures, politiques et pratiques.
- Entretiens avec responsables clés.

### Étape 2 : Analyse documentaire et réglementaire

- Examen des procédures, plans continuité, rapports d’audit.
- Évaluation conformité aux lois nationales et RGPD.

### Étape 3 : Recommandations et plan d’action

- Formulation de recommandations adaptées au contexte local.
- Plan d’action avec calendrier et chiffrage estimatif.

### Étape 4 : Suivi et accompagnement

- Accompagnement personnalisé pour mise en œuvre des mesures.
- Suivi régulier et reporting.

> La formation offre une expertise pratique pour diagnostiquer, planifier et sécuriser efficacement les systèmes d’information en environnement togolais.

---