Fiche Technique:Audit Cybersécurité en Mauritanie

Objectifs de la formation

- Diagnostiquer les vulnérabilités techniques, humaines et organisationnelles.
- Évaluer la conformité aux normes internationales et locales.
- Définir un plan d'action priorisé pour maîtriser les risques.
- Réduire le risque d'incidents de sécurité.
- Renforcer la résilience opérationnelle des systèmes d’information.
- Fournir des recommandations adaptées au contexte mauritanien.

Population cible

- Entreprises industrielles, financières et commerciales.
- Administrations publiques et organismes de régulation.
- Directions générales, responsables informatiques et RSSI.
- Responsables risques, conformité et équipes infrastructures critiques.
- Sociétés des zones industrielles de Nouadhibou, Nouakchott et portuaire.

Durée de la formation

Phase	Objectifs	Durée indicative
Diagnostic initial	Collecte d’information et état des lieux	1 semaine
Analyse documentaire	Examen des politiques et conformité	1 à 2 semaines
Recommandations	Plan d’action priorisé et recommandations	1 semaine
Suivi et accompagnement	Mise en œuvre et reporting	Variable selon besoins

> La durée totale varie entre 3 et 6 semaines selon taille, complexité et objectifs. Formats sur site, à distance ou hybrides.

Programme de la formation

Étape 1 : Diagnostic initial

- Collecte des informations et état des protections.
- Analyse des incidents passés et processus en place.

Étape 2 : Analyse documentaire et réglementaire

- Revue des politiques, procédures, contrats fournisseurs.
- Vérification de conformité aux normes (ISO 27001, RGPD, etc.).

Étape 3 : Recommandations et plan d’action

- Formulation de recommandations hiérarchisées.
- Élaboration d’un plan d’amélioration adapté.

Étape 4 : Suivi et accompagnement

- Assistance à la mise en œuvre des recommandations.
- Formation des équipes et reporting adapté.
