ELABORER UN PLAN DE REPRISE APRES SINISTRE INFORMATIQUE - Durée 14h

OBJECTIFS

- Minimiser les temps d'arrêt des activités.
- Réduire les pertes financières liées aux sinistres informatiques.
- Protéger les applications critiques contre la perte de données.
- Reprendre rapidement les opérations après une interruption.
- Maintenir les accords de niveau de service établis.
- Offrir une tranquillité d'esprit aux équipes et aux employés.

PUBLIC CIBLE

- Toute entreprise souhaitant mettre en place un plan de repli efficace en cas de cyberattaque.

PRE-REQUIS

- Aucun

PROGRAMME

Sensibilisation et fondamentaux

- Présentation des attaques de cybersécurité.
- Le SMCA (Système de Management de la Continuité d'Activité, Norme ISO22301).
- Organisation en mode projet.
- Introduction à la gestion de crise et à la continuité d'activité.
- Statistiques sur les catastrophes et leurs impacts.

Analyse des risques et besoins

- Réalisation d'une analyse des risques et des besoins.
- Détermination du DMIA (Délai Maximal d'Interruption acceptable de l'Activité).
- Objectif de Reprise d'Activité (RTO) et Objectif de Perte de Données (RPO).
- Analyse des risques par site et par activité.

Mise en place d'un dispositif de gestion de crise

- Organisation des cellules de crise.
- Documentation : Plans de Gestion de Crise, de Communication et de Ressources Humaines.

Plan de continuité d'activité (PCA)

- Rôles des membres de la filière PCA.
- Site de repli et télétravail.
- Déclenchement du PCA.
- Travail sur des scénarios spécifiques.

S'assurer de l'efficacité du dispositif

- Plan d'Amélioration Continue (PAC).
- Gouvernance de la continuité d'activité.
- Audit et contrôles.

Conclusion

La formation « Élaborer un Plan de Reprise après Sinistre Informatique » est une opportunité indispensable pour les entreprises souhaitant se prémunir efficacement contre les cyberattaques et assurer la pérennité de leurs activités. Grâce à des méthodes pédagogiques interactives et des outils adaptés, les participants acquerront des compétences pratiques et stratégiques pour anticiper, gérer et surmonter les crises informatiques.

MOYENS TECHNIQUES ET HUMAINS :

- Intervenant : Formateur Professionnel
- Mobilisation des outils et auxiliaires utiles : paperboard, vidéoprojecteur…
- Possibilité de mettre à disposition des PC portables pour les stagiaires

METHODES PEDAGOGIQUES MOBILISEES :

- Alternance de méthodes affirmatives, interrogatives et actives
- Ressources de type formatives, évaluatives, de synthèses, de soutien, de mémorisation…
- Utilisation de Padlet

MODALITES D'EVALUATION :

- Des acquis
  - Fiche de renseignements en amont et questions
  - Evaluations formatives réalisées à l'aide de grilles critériées ;
  - Attestation de fin de formation mentionnant l'atteinte des objectifs de la formation
  - Evaluation différée
- Evaluation satisfaction
- Rédaction d'un bilan d'action remis au commanditaire en cas de formation intra-entreprise