Plan de gestion des risques des actifs informatiques – CFA Numérique

KOUASSI GLOHNDY JEAN-MARIE

Sommaire

1. Introduction

Le présent plan vise à identifier, évaluer et gérer les risques liés aux actifs informatiques du CFA Numérique. L'objectif est de minimiser les impacts négatifs sur la continuité des activités et la sécurité des informations.

2. Identification des risques

Cinq risques spécifiques ont été identifiés concernant la gestion des actifs informatiques :

1. Perte de données – Risque de suppression accidentelle ou de corruption des données importantes.
2. Vol ou perte d'équipements – Ordinateurs portables, serveurs ou autres équipements sensibles.
3. Non-conformité des licences – Utilisation de logiciels sans licence ou licences expirées.
4. Cyberattaques – Malware, ransomware ou phishing ciblant les actifs numériques.
5. Défaillance matérielle – Pannes de serveurs, disques durs ou équipements critiques.

3. Évaluation des risques

Risque	Probabilité	Impact	Justification
VPerte de données	Moyenne	Élevé	Les données sont cruciales pour les formations et la gestion administrative.
Vol ou perte d'équipements	Moyenne	Élevé	Les équipements contiennent des informations sensibles et des logiciels coûteux.
Non-conformité des licences	Faible	Moyen	Peut entraîner des sanctions légales et des coûts supplémentaires.
Cyberattaques	Moyenne	Élevé	Risque de compromission des données et interruption des services.
Défaillance matérielle	Moyenne	Moyen	Peut entraîner des pertes de données et des arrêts temporaires d'activité.

4. Mesures de prévention et de mitigation

Risque	Mesures de prévention
Perte de données	Sauvegardes régulières, solutions de stockage cloud sécurisées, plans de restauration d'urgence.
Vol ou perte d'équipements	Inventaire régulier, systèmes de suivi des équipements, chiffrement des données sensibles.
Non-conformité des licences	Audit régulier des logiciels, suivi des renouvellements de licences, formation du personnel.
Cyberattaques	Antivirus et pare-feu à jour, sensibilisation du personnel, tests de vulnérabilité, mises à jour régulières des systèmes.
Défaillance matérielle	Maintenance préventive, redondance des serveurs, contrats de support avec fournisseurs.

5. Matrice des risques

Risque	Probabilité	Impact	Niveau de risque	Recommandation
Perte de données	Moyenne	Élevé	Élevé	Implémenter des sauvegardes automatisées et régulières
Vol ou perte d'équipements	Moyenne	Élevé	Élevé	Installer un suivi des actifs et chiffrer les données
Non-conformité des licences	Faible	Moyen	Moyen	Mettre en place un suivi rigoureux des licences
Cyberattaques	Moyenne	Élevé	Élevé	Sensibiliser les utilisateurs et mettre à jour les systèmes
Défaillance matérielle	Moyenne	Moyen	Moyen	Prévoir des redondances et maintenance régulière

6. Conclusion

La gestion proactive des risques informatiques permet de sécuriser les actifs de l'entreprise, de réduire les pertes potentielles et d'assurer la continuité des activités. La mise en place de mesures de prévention et de suivi constant est essentielle pour protéger les ressources numériques du CFA Numérique.