FICHE THEMATIQUE N°33

Numérique et Cybersécurité

Gestion et protection des données (RGPD, sauvegardes, PCA/PRA, IA)

Conformité au RGPD (Règlement Général sur la Protection des Données)

Pour la gestion et protection des données (RGPD, sauvegardes, PCA/PRA, IA), en se basant sur les bonnes pratiques de l'ISO/IEC 27001, voici une démarche structurée :

Identification des Données Personnelles : Cartographier les données personnelles collectées, traitées, et stockées par l'entreprise. Veiller à ce que chaque type de donnée soit bien justifié et traité de manière légale.

Bases Légales de Traitement : S'assurer que chaque traitement a une base légale conforme au RGPD, comme le consentement, l'obligation légale, ou l'intérêt légitime.

Droits des Personnes : Mettre en place des procédures pour répondre aux demandes des individus concernant leurs droits (accès, rectification, suppression, etc.). S'assurer que ces demandes peuvent être traitées rapidement.

Sauvegardes et Protection des Données

Sauvegardes Régulières : Mettre en place un système de sauvegarde régulier des données critiques. Ces sauvegardes doivent être protégées et chiffrées pour empêcher l'accès non autorisé.
Réplication Géographique : Prévoir des sauvegardes dans des localisations différentes pour se protéger contre les catastrophes locales.

Test des Sauvegardes : Effectuer des tests réguliers des restaurations pour vérifier que les sauvegardes sont valides et peuvent être récupérées en cas d'incident.

Plan de Continuité d'Activité (PCA) et Plan de Reprise d'Activité (PRA)

PCA : Développer un plan qui garantit que les processus critiques de l'entreprise peuvent continuer pendant un incident. Cela inclut des moyens de contournement, des ressources minimales nécessaires, et des rôles et responsabilités clairs.

PRA : Élaborer un plan de reprise d'activité qui définit comment rétablir les systèmes à leur état normal après un incident. Assurer une procédure de récupération des données basée sur les sauvegardes. Simulations et Tests : Organiser régulièrement des tests des PCA/PRA pour vérifier leur efficacité. Cela inclut des simulations de scénarios, tels que des cyberattaques ou des pannes complètes des systèmes.

Protection des Données dans les Projets d'IA

Minimisation des Données : Limiter la collecte des données aux éléments nécessaires pour l'entraînement et l'utilisation de l'IA.

Anonymisation et Pseudonymisation : Anonymiser les données personnelles utilisées dans les projets d'IA, afin de minimiser les risques de réidentification.

Éthique et Biais : S'assurer que les algorithmes d'IA ne contiennent pas de biais injustes ou discriminatoires. Cela inclut des tests réguliers et des validations des modèles IA.

Contrôles de Sécurité

Chiffrement des Données : Les données personnelles doivent être chiffrées, qu'elles soient en transit ou stockées. Cela permet de minimiser les risques d'accès non autorisé.

Contrôles d'Accès : Définir des politiques strictes de contrôle d'accès aux données, basées sur le besoin de connaître. Cela inclut la gestion des droits d'accès des employés.

Surveillance et Audit

Surveillance des Incidents : Mettre en place un processus de surveillance des incidents liés aux données, en particulier en cas de violation de données personnelles, pour se conformer aux obligations de notification.

Audit Régulier : Effectuer des audits réguliers sur la gestion des données et les plans de continuité pour garantir que les politiques sont respectées et restent à jour.

Ces actions, basées sur l'ISO/IEC 27001, visent à assurer la sécurité et la protection des données tout en garantissant la conformité aux régulations comme le RGPD, la résilience opérationnelle grâce aux plans PCA/PRA, et une approche éthique et responsable des projets d'IA.