Programme Régional UEMOA
Système de suivi de la pêche continentale

Stratégies

de Gestion des données

et de

Valorisation des données (SIRP)

1. Stratégie de gestion des données

Objectif général: Assurer la sécurité et la pérennité des données du suivi PC, tout en permettant leur exploitation.

- (1) Assurer la sécurité physique des B.D. dans le court et long-terme
- (2) Assurer le maintien de l'intégrité du contenu électronique des B.D. tout en assurant la sécurité physique et la possibilité d'usage des données
- (3) Assurer la sécurité sur le plan « humain » et institutionnel dans le long terme

Ce sont des questions de « moyens » et des questions de « bonnes pratiques »

Rappels préalables du contexte

- La B.D. utilisée pour la saisie des fiches collectées sur une macro-strate donnée est unique.
- Mais: des fiches venant de plusieurs macro-strates peuvent être saisies dans une seule base située sur un seul poste.
- Conséquence: 1 à 6 (?) B.D. actives « en saisie » dans un pays donné, sur 1 à 6 (?) machines PC dédiées.

(1) Assurer la sécurité physique des B.D. dans le court et long-terme

Contraintes:

Les BD actives en saisie sont des bases Access© installées sur des PC « fragiles » (problèmes de disques, virus..) dans un environnement imparfait (coupures de courant, vols, voire incendies etc..)

Solutions:

(1a) Protéger les postes de saisie (MaJ des antivirus, onduleur)

(1b) Faite en sorte que les postes de saisie soient dédiés à la saisie (pour éviter trop de passages avec risques de contamination)

(1) Assurer la sécurité physique des B.D. dans le court et moyen-terme

Solutions (suite) :

(1c) Effectuer des copies de sauvegarde de la B.D. régulièrement:
- soit sur un PC différent (possible mais déconseillé),
- soit sur une clé USB (possible mais déconseillé)
- ou (mieux) sur un disque dur de sauvegarde dédié (conseillé, car localisé et peut être stocké dans un autre local)
- ou encore: graver les copies de sauvegarde sur des CD.

(1d) Conserver le support des copies de sauvegarde dans un lieu différent, bien identifié et connu par au moins deux personnes de l'équipe.

2. Assurer le maintien de l'intégrité du contenu électronique des B.D.

- Eviter de saisir les fiches d'enquête venant d'une macrostrate donnée sur plusieurs postes (et donc dans plusieurs bases de saisie actives) : organisation de la saisie.
- Eviter une multiplication non maîtrisée des copies des bases et des versions, supprimer les vieilles copies de sauvegarde qui ont été remplacées par des copies de sauvegarde plus récente.
- Distinguer dans le vocabulaire l'outil base de données, d'un côté, et les bases de données créées avec du contenu, de l'autre.
- Eviter que d'éventuelles modifications inopportunes faites sur les données de la B.D. ne reviennent contaminer la B.D. active source.

Solutions (bonnes pratiques):

La base source originelle active « en saisie » utilisée pour une macrostrate doit toujours être localisée sur un PC précis et identifiée (par un préfixe « EnSais- ») et par un morceau de nom des macro-strates dont elle contient les données.

Convenir d'une norme pour nommer les bases et leurs copies

Les sauvegardes de sécurité doivent être identifiées en tant que sauvegarde en ajoutant dans leur nom un préfixe ou un suffixe « Sauv- » dans leur nom, ainsi que la date de leur sauvegarde. Elles ne doivent jamais faire l'objet de modification après leur sauvegarde, puisqu'elles sont destinées à pouvoir être utilisées. (Elles sont « archivées »).

Solutions (bonnes pratiques - suite):

Les copies de base de données faites pour être utilisées pour extraction doivent être identifiés en tant que telles.

Les copies de B.D. éventuellement transmises à des tiers (étudiants, doctorants ..) pour des objectifs d'analyses statistiques originales doivent être identifiées avec un préfixe ou un suffixe dans leur nom (ex.: « Cop-pr-rech- » et la date de la création de la copie dans leur nom.

Elles ne doivent jamais revenir dans la zone de saisie.

(3) Assurer la sécurité sur le plan « humain » et institutionnel dans le long terme

Les problèmes et les risques dus à l'instabilité des équipes ou au changement des mandats des services administratifs sont nombreux.

Voici quelques « bonnes pratiques » pour les limiter et pour prendre en compte cet aspect délicat:

- Bien identifier l'équipe (les personnes) qui interviennent dans la saisie, la gestion, l'archivage des données, avec leurs responsabilités respectives.
- Toujours faire intervenir deux personnes sur les opérations délicates (création des copies de sauvegarde et des copies pour extraction et reporting). Ces personnes doivent obligatoirement partager leurs informations et s'informer de leurs actions. Elles doivent respecter les mêmes normes.
- Donner un statut « reconnu » à la base de données dans le dispositif administratif de l'Etat. Les bases ne doivent pas être considérées comme « personnelles ».
- Créer une B.D. unique concaténée (agrégée) par année, dont une copie est envoyée à l'UEMOA.