Concours section : Examen professionnel d'ingénieur de l'agricu

Epreuve matière : iae - sujet n°2 (choix spécialité/domaine 1 - mise en valeur agr/rédaction d'une note au cho

16.75 / 20

Concours/Examen : examen professionnel IAE **Épreuve :** Admissibilité **N° sujet :** 2

Section-option/Spécialité/BAP/Domaine : mise en valeur agricole et industries agroalimentaires

CONSIGNES

- *Remplir soigneusement, sur CHAQUE feuille officielle, la zone d'identification en MAJUSCULES.*
- *Indiquer le n° du sujet quand l'épreuve comporte plusieurs sujets au choix.*
- *Ne pas signer la composition et ne pas y apporter de signe distinctif pouvant indiquer sa provenance.*
- *Numéroter chaque PAGE (cadre en bas à droite de la page) et placer les feuilles dans le bon sens et dans l'ordre.*
- *Rédiger avec un stylo à encre noire.*
- *N'effectuer aucun collage ou découpage de sujets ou de feuille officielle. Ne joindre aucun brouillon.*

Direction Departementale des Territoires

Departement D. Lieu ... le ...

Note à l'attention de Monsieur le Prefet

objet : continuité des fonctions numeriques dans le cadre du Plan de Continuité d'Activité (PCA)

Les attaques numériques sont de plus en plus fréquentes. Les services déconcentrés dont la DDT doivent assurer la continuité du service pour les usagers et la sécurisation des données.

Le Plan de continuité de l'activité permet de definir un ou des plans d'action en fonction des différents risques identifiés (voir I)

La DDT met en oeuvre un PCA (voir II) et plus précisemment un plan de continuité informatique tout en respectant le référentiel général de sécurité (RGS). Pour autant des pistes d'amelioration de la continuité du service pour l'usager et l'environnement numeriques sont relevées (voir III).

A 1/4..

Concours section : Examen professionnel d'ingénieur de l'agricu

Epreuve matière : iae - sujet n°2 (choix spécialité/domaine 1 - mise en valeur agr/rédaction d'une note au cho

16.75 / 20

I Le Plan de continuité d'activité (PCA)

1- Le PCA vise à prévoir une stratégie de protection et de prévention au sein d'une organisation dans le but d'assurer le maintien des activités opérationnelles essentielles et la planification de la reprise d'activités lors de risques altérant la continuité.

2. Le PCA est un document dans lequel sont identifiés / cartographiés les éléments suivants

- les besoins de l'organisation : services minimum requis, durée maximale d'indisponibilité, mode dégradé
- les risques prioritaires fréquences types gravité
- les activités essentielles
- les plus critiques
- la procédure de crise
- la communication
- la veille
- le retour à un fonctionnement normal

3- Le PCA est évolutif en fonctions des organisations, des risques nouveaux. Il repond à divers scénarios dans la perspective d'une forte réactivité lors de la confrontation au risque. Il doit faire l'objet d'amélioration continue.

2.1.4.

II Mise en œuvre du PCA en DDT.

1- Plan de continuité informatique PCI

La DDT utilise essentiellement des applicatifs WEB, des bases de données. Le risque de cyberattaques est largement identifié. C'est pourquoi, pour sécuriser les systèmes d'information, un plan de continuité de sécurité englobe un plan de continuité informatique. Celui-ci relève du domaine technique (sauvegarde de données, matériel, assistance ...) du plan humain (sensibilisation des agents, respects des consignes d'utilisation des postes informatique

2- Référentiel Général de sécurité (RGS)

Le RGS fixe les règles et les bonnes pratiques en matière de sécurité des systèmes d'information à destination des autorités administratives (services en ligne aux usagers). Une analyse systématique des risques permet d'adapter efficacement les mesures de sécurité mises en œuvre.

4 fonctions de sécurité de base : l'authentification, la signature électronique, la confidentialité et l'horodatage permettent aux usagers comme aux agents. de s'assurer de la sécurisation des données. Pour exemple l'espace TELEPAC applicatif permettant aux exploitants agricoles de réaliser leur déclarations PAC, ~~de~~ transmettre des données personnelles confidentielles aux agents DDT d'instruire les dossiers en modification en fonction de leur profil.

L'administration des habilitations de tel outils est très strict. et permet de mettre des profils consultatifs, actifs, de

regénérer les mots de passe des exploitants....

III Pistes d'amélioration / propositions

- Sensibilisation plus régulière des usagers et des agents (flyer, questions / réponses interactives ...) sur les risques
- Bonne pratiques et réflexes
- Faire des groupes de travail afin d'améliorer les plan de continuité d'activité (postes sensibles, actions sensibles)
- Renforcement des plans de communications internes et externes.
- Projet programme OSTHINEE = projet d'une offre de service cloud, service d'hébergement interministériel afin de rationnaliser les attaques = réflexion à mener : comment s'y inscrire ? valeurs ajoutées ?
- Communiquer auprès des agents des plans d'action en fonction des risques.

La cybercriminalité est croissante. A nous d'anticiper via des plans d'action toutes les attaques et de faire preuve de résilience pour permettre aux organisations de se maintenir en activité en période de crise.