

ÉTIQUETTE
D'IDENTIFICATION

À compléter par le candidat

Abatte le cache qu'en présence d'un membre de la commission de surveillance

Merci à Solken10972

Membre du site www.devenez-fonctionnaire.fr

Merci pour le partage et les futurs candidats

Concours externe - interne - professionnel - ou examen professionnel (*)

Rayer les mentions inutiles

Pour l'emploi de : Contrôleur des finances publiques

Preuve n° : 1

Matière : Questions cas pratique

Date : 23/10/2017

Nombre d'intercalaires supplémentaires :

À L'ATTENTION DU CANDIDAT

En dehors de la zone d'identification rabattable, les copies doivent être totalement anonymes et ne comporter aucun élément d'identification tel que nom, prénom, signature, paraphe, localisation, initiale, numéro, ou toute autre indication même fictive étrangère au traitement du sujet.

Il est demandé aux candidats d'écrire et de souligner si nécessaire au stylo bille, plume ou feutre, de couleur noire ou bleue uniquement. Toute autre couleur pourrait être considérée comme un signe distinctif par le jury, auquel cas la note de zéro serait attribuée. De même, l'utilisation du crayon surligneur est interdite.

Les étiquettes d'identification codes à barres, destinées à permettre à l'administration d'identifier votre copie, ne doivent être détachées et collées dans les deux cadres prévus à cet effet qu'en présence d'un membre de la commission de surveillance.

NOTE / 20
16,00

1 : Vous présenterez les mesures de la DGFiP pour assurer la sécurité des agents et de ses bases de données.

Le constat d'une recrudescence de litiges et des agressions de tout ordre à l'égard des agents (Prévention des risques sociaux (RPS)) des finances, la protection et la sécurité ont été au cœur des préoccupations de

Une action a été mise en place en collaboration avec différentes instances compétentes et se situe autour de 6 axes et vise la mise en œuvre de prévention et de protection et compte de la sécurité des agents, des bases de données.

agents :

circule autour de mesures cohérentes :

- d'une politique d'information : communication, respect des personnels, action (affichage d'une affiche choisie de la courtoisie et du respect).

- de paiement au guichet pour limiter le paiement par carte bancaire privilégiée.

- un plan de sécurisation renforcée : renforcement de la protection structurelle, des agents de protection et d'alerte.

Question 1 : Vous présenterez les mesures prises par la DGFiP pour assurer la sécurité de ses agents et de ses bases de données.

Face au constat d'une recrudescence des incivilités et des agressions de toute nature à l'égard des agents (Prévention des risques psycho-sociaux (RPS)) des finances publiques, la protection et la sécurité ont été placées au cœur des préoccupations de la DGFiP.

Pour ce faire un plan d'action a été mis en place en concertation avec les différentes instances compétentes.

Ce plan d'action s'articule autour de 6 axes et vise à conduire une politique de prévention et de protection plus rigoureuse en tenant compte de la sécurité des agents bien sûr mais aussi des bases de données.

A) La Protection des agents :

Cette protection s'articule autour de mesures complémentaires et cohérentes :

- 1) Par la mise en place d'une politique d'information : rappel des règles de civisme, respect des personnels, campagne de communication (affichage d'une affiche « ensemble, faisons le choix de la courtoisie et du respect »).
- 2) Evolution des moyens de paiement au guichet pour limiter les risques (Paiement par carte bancaire privilégié)
- 3) Mise en place d'un plan de sécurisation renforcée des bâtiments : - Renforcement de la protection structurelle et des équipements de protection et d'alerte des postes les plus sensibles.

- Identification annuel des sites les plus exposés par le biais d'un diagnostic.

- Assistanat des chefs de services par le délégué départemental dans la mise en œuvre des règles de sécurité immobilière.

4) Permettre aux agents de gérer au mieux les situations difficiles en renforçant la politique de prévention par le biais de formation sur les droits des agents en matière de protection et de sécurité (droit à la protection, droit de retrait, discrimination).

Ces premières formations seront complétées par des formations adaptées à chaque mission. (concerneront les agents mais aussi les responsables de prévention et de gestion de relations conflictuelles.) mais aussi par la mise à jour des guides de procédure et le renforcement lors des périodes d'affluences des dispositifs organisationnels de l'accueil.

5) Consolider l'accompagnement des personnels en cas d'incident : * Prise en charge personnalisée, systématique de tout incident.

* Nomination d'un référent « protection juridique des agents ».

* Accompagnement des agents victimes par la formalisation de points d'étape réguliers en lien avec les différents interlocuteurs (médecin de prévention, assistants de prévention et psychologues).

* Création d'un numéro d'urgence afin d'alerter rapidement la direction en cas d'incident grave.

6) Une protection renforcée des personnels : ce qui permettra une meilleure identification des dossiers à risque.

En tout état de cause, l'agent DGFIP sera accompagné au plus près dans sa démarche en l'assurant du soutien de la DGFIP dans la démarche et les conseils.

B) La Protection des bases de données :

La confidentialité des données constitue un enjeu majeur en matière de sécurité.

Dans cette perspective tous les agents doivent être sensibilisés à cette problématique et à l'obligation de secret professionnel qui la sous-tend.

C'est pourquoi, il apparaît nécessaire de rappeler certains principes et règles de prudence : (Messagerie Ulysse)

- La sécurité des bases de données passe d'abord par le choix d'un mot robuste et sûr. Pour cela, celui-ci doit être choisi avec rigueur en tenant compte de plusieurs facteurs et chacun doit acquiescer le réflexe de le protéger.

- * Le mot de passe ne doit avoir aucun lien avec l'utilisateur (nom, date de naissance.....)

- * Il doit être obligatoirement changé à la 1^{ère} connexion.

- * Il ne doit pas être transmis à quelconque ni par messagerie électronique.

- * A sa création éviter les mots contenus dans le dictionnaire,

- * S'astreindre de toute mémorisation informatique.

- * Être saisi à l'abri des regards indiscrets

- * Favoriser l'outil Escalier pour tout envoi volumineux de fichiers tant en interne qu'en externe.

- * Séparer la vie professionnelle de la vie privée, ce qui implique des mots de passe différents.

- * En cas d'absence prolongée de son poste de travail ne pas oublier de verrouiller son ordinateur.

Malgré toutes ces mesures, si votre mot de passe est compromis, une seule solution s'offre à vous :

changer celui-ci ou ceux-ci et prévenir immédiatement l'équipe d'assistance téléphonique.

Question 2 : D'après vous, quels sont les enjeux de la sécurité numérique en France, et quels en sont les principaux acteurs ?

A) La sécurité du numérique en France passe par la dotation de celle-ci d'une stratégie nationale destinée à accompagner la transition numérique de la société française.

Cette nouvelle stratégie a pour ambition de répondre aux nouveaux enjeux nés des évolutions des usages numériques et des menaces qui y sont liés.

Cette stratégie s'articule autour de 5 objectifs ou enjeux :

1. Garantir le maintien de la souveraineté nationale par des mesures propres à renforcer la sécurité des infrastructures critiques ;

2. Apporter une réponse forte contre les actes de cybermalveillance affectant les systèmes d'information de l'Etat, des entreprises et des particuliers ;

3. Sensibiliser et former à la cybersécurité ;

4. Faire de la sécurité numérique un vecteur de compétitivité et renforcer la voix de la France à l'international par le soutien à une autonomie stratégique européenne.

5 - Favoriser l'appui aux pays émergents désireux de contribuer à la stabilité du cyberspace.

Cette stratégie est un engagement de l'Etat au bénéfice de la sécurité des systèmes d'information.

Son rôle est d'apporter une réponse collective et coordonnée vers la confiance numérique propice à la stabilité de l'Etat, au développement économique et à la protection des citoyens.

B) Afin de mener à bien la sécurité du numérique en France 3 acteurs sont à mettre en œuvre :

1 - L'expert de haut niveau du "Cap Numérique" dont le rôle est d'apporter une expertise dans le domaine des données numériques. Il a un rôle de veille, de proposition et de réflexion en lien avec le service des ressources humaines et du service des systèmes d'information afin de diffuser la "culture de la donnée" au sein de la DGFiP, en particulier de son encadrement.

2 - Le Haut fonctionnaire de défense et de sécurité (HFD S) qui conseille et assiste pour les questions relatives aux mesures de défense et de sécurité nationale. En liaison permanente avec le Secrétaire général de la défense et de la sécurité nationale (SGDSN) il anime et coordonne la politique en matière de défense, de vigilance, de prévention de crise et de situation d'urgence.

Il mène également des actions de sensibilisation et de formation au sein des ministères.

3 - L'agence nationale de la sécurité des systèmes d'information (ANSSI). Son rôle est d'assurer la sécurité et la défense des systèmes d'information de l'Etat

et de contribuer à celle des opérateurs nationaux d'importance vitale (O.I.V).

Elle a une compétence nationale et est rattachée au secrétaire général de la défense et de la sécurité nationale (SGDSN).

Les 3 missions majeures de l'ANSSI sont de :

Prévenir	Défendre	Informer
<u>Mission 1</u>	<u>Mission 2</u>	<u>Mission 3</u>
En anticipant les modes d'attaques par les pentests et en définissant les mesures de protection. Mais également en labellisant des produits et services informatiques de confiance.	En détectant les failles des systèmes d'information ainsi que les incidents et réagir au plus tôt en cas de cyberattaque, en apportant son assistance technique et son expertise.	En sensibilisant les différents publics sur la nécessité d'une protection des environnements numériques et en promouvant les bonnes pratiques de cybersécurité et en émettant des recommandations techniques.

En contribuant à la promotion de technologies, de systèmes et de savoir-faire nationaux auprès des administrations, des acteurs économiques et du grand public, l'ANSSI participe à la protection et à la défense du potentiel économique de la Nation.