

ÉTIQUETTE
D'IDENTIFICATION



À compléter par le candidat

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

Concours externe - interne - professionnel - ou examen professionnel ⁽¹⁾

Rayer les mentions inutiles

Normal FIP 2^{ème} classe

Pour l'emploi de : Contrôleur des FIP

Épreuve n° : 1

Matériau : Cas Pratique

Date : 23/10/2017

Nombre d'intercalaires supplémentaires : 0

À L'ATTENTION DU CANDIDAT

En dehors de la zone d'identification rabattable, les copies doivent être
entièrement 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
d'un 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
15,50

En 2012, pour répondre à
l'augmentation des incivilités et agressions
contre des agents de la DGFIP et aux
permanences sur les ressources de
exposées sur internet un plan
a été mis en place.

Quelles mesures prises pour assurer
la sécurité des agents mais aussi celles
des ?

En 2012, nous présenterons les actions
des agents, puis celles pour garantir
la sécurité.

En 2012, la DGFIP pour assurer la sécurité

un plan d'urgence sécurité autour

le schéma précisant les sanctions
à l'égard d'un agent, ainsi que la mention
contribuable ont permis de mener

la mise en œuvre du respect des personnels de
la DGFIP.

Les moyens de paiements permet
le guichet.

Le délégué départemental permet une
de sécurité immobilière, de procéder
à la mise en œuvre des tests

des agents de la DGFIP ont suivi
la mise en œuvre des agents en matière de protection

Question 1

Depuis 2012, pour répondre à l'augmentation des incivilités et agressions à l'encontre des agents de la DGFIP et aux attaques permanentes sur les ressources de la DGFIP exposées sur internet un plan d'action a été mis en place.

Quelles sont les mesures prises pour assurer la sécurité des agents mais aussi celles pour les bases de données ?

Dans un premier temps, nous présenterons les actions menées pour protéger les agents, puis celles pour garantir la confidentialité des données.

I. mesures prises par la DGFIP pour assurer la sécurité des agents.

En décembre 2012, un plan d'urgence sécurité autour de 6 axes a été exposé.

Une campagne d'affichage précisant les sanctions encourues en cas d'agression d'un agent, ainsi que la mention portée dans la charte du contribuable ont permis de mener une politique d'information sur le respect des personnels de la DGFIP.

la multiplication des moyens de paiements permet de limiter les risques au guichet.

la mise en place de délégué départemental permet une mise en œuvre des règles de sécurité immédiate, de procéder aux analyses de sites mais aussi de piloter les tests anti-agression.

En 2013, l'ensemble des agents de la DGFIP ont suivi une formation sur les droits des agents en matière de protection

et de sécurité. Ils ont également accès aux guides de procédures rénovés en cas de situation difficile.

L'accompagnement des personnels en cas d'incident est consolidé avec une prise en charge systématique et personnalisée. Le suivi de ses agents sera effectué par la collaboration des médecins de prévention, des assistants de prévention et des psychologues mais également avec le référent protection juridique des agents qui veillera à l'évolution du dossier sur le plan juridique.

Une meilleure identification des dossiers ou situations à risque permettra de mieux protéger le personnel de la DGFIP.

II. mesures prises par la DGFIP pour assurer la sécurité de ses bases de données

Plusieurs directives ont été instaurées pour garantir la confidentialité des données, tant en interne qu'à l'externe.

L'article 226-13 du code pénal précise que le manquement au secret professionnel est puni par 1 an d'emprisonnement et de 15 000 € d'amende. Par ailleurs, l'article 26 de la loi n° 83-634 du 13 juillet 1983 rappelle que les agents des finances publiques sont soumis à la discrétion professionnelle c'est à dire qu'ils ont l'obligation de taire les faits ou informations dont ils ont eu connaissance dans l'exercice de leurs fonctions.

Avec le développement des nouvelles technologies, la DGFIP est devenue une cible de choix. Pour contrer la plus part de ses attaques des pare-feux et antivirus ont été mis en place. D'autres outils sont développés pour assurer la sécurité des données comme la nouvelle utilisation des stockages en cloud, l'utilisation exclusive de la messagerie de la DGFIP, l'utilisation du logiciel Escalé pour les envois de

données sensibles. Il est également rappelé aux agents de sécuriser leurs ordinateurs en verrouillant leurs sessions de travail et de changer régulièrement leurs mots de passe robustes.

La DGFIP se modernise avec la dématérialisation et le prélèvement à source par contre cela entraîne une haute vigilance sur la sécurisation des données.

Question 2

La démocratisation d'Internet entraîne depuis quelques années des accidents de sécurité informatique.

Quels sont les enjeux de la sécurité numérique et quels en sont les principaux acteurs ?

Dans un premier temps nous verrons les 5 objectifs de la France en matière de sécurité numérique puis les acteurs concernés.

I. les 5 objectifs de la sécurité numérique

Depuis 2009 et la création de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), la France s'est dotée d'une sécurité et défense des systèmes d'informations.

La stratégie nationale est de garantir la souveraineté nationale par des mesures propres à renforcer la sécurité des infrastructures, apporter une réponse forte contre les actes de malveillance, sensibiliser et former à la cybersécurité mais également sur le plan international de faire de la sécurité numérique un vecteur de compétitivité et d'apporter un soutien aux pays émergents désireux de contribuer à la stabilité du cyberspace.

II les intervenants dans la sécurité numérique

Pour que le cyberspace demeure un espace de confiance, chaque entreprise et particulier doivent se doter de pare-feux et antivirus.

Depuis le décret n° 2009-834 du 17 juillet 2009, l'ANSSI assure une mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Le secrétaire général de la défense et de la sécurité nationale (SGDSN) assiste le chef du gouvernement dans ses responsabilités en matière de défense et de sécurité nationale. HADOPI permet une diminution des échanges de données non autorisés et non sécurisés.

Plusieurs ministères ont créés des fonctions d'administrateurs des données afin d'être plus proche des évolutions sur la réglementation des données personnelles, et de rester à l'écoute des innovations dans ce domaine.

Le numérique est un outil de plus en plus utilisé donc la sécurité du numérique est un atout à ne pas négliger. Les décideurs publics, privés et les citoyens doivent s'investir pour garantir un climat de confiance dans le cyberspace.

* Un Haut Fonctionnaire de défense et de sécurité (HFDS) est nommé par décret, sur proposition des ministres auprès desquels il est placé. Ses attributions sont fixées par le code de la défense. Il anime et coordonne la politique en matière de défense, de vigilance, de prévention de crise et de situation d'urgence. Il est également chargé de l'animation de la politique de sécurité des systèmes d'information et du contrôle de son application.

Un Fonctionnaire de Sécurité des systèmes d'information (FSSI) est nommé par l'HFDS pour l'assister dans ses missions.