

Merci à cecfollette67

Membre du site www.devenez-fonctionnaire.fr

Merci pour le partage et les futurs candidats

ÉTIQUETTE
D'IDENTIFICATION

À compléter par le candidat

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

Concours externe - interne - professionnel - ou examen professionnel

Rayer les mentions inutiles

Candidate des Finances

Sur l'emploi de : (IN)

Reuve n° : 1

Matr. : Questions au Cas pratique 102

Carrière Administrative

te : 23/10/2017

Nombre d'intercalaires supplémentaires : 1

À L'ATTENTION DU CANDIDAT

dehors de la zone d'identification rabattable, les copies doivent être
également 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.

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

s 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

travaux pris par la DGFIP
pour la sécurité de ses agents
et des données.

incidents, agressions
DGFIP (Direction Générale
qu'ils soient enquêteurs,
issie d'un Centre des Finances
pris différentes mesures
et d'accompagnement
risques et aux demandes
sur elle a également
sécurité et ses bases
C'est la législation sur l'information
sur ses données.

auton en matière de sécurité
DGFIP (I) et de ses bases
permettre de répondre aux
us par la DGFIP et ses agents

de Prévention de sécurité
DGFIP

d'Actions et une politique
protection de ses agents a
n partenariat avec différents
le et de protection des agents (B)

Question 1

Les mesures prises par la DGFIP pour assurer la sécurité de ses agents et des bases de données.

Face aux nombreuses incivilités, agressions contre les agents de la DGFIP (Direction Générale des Finances Publiques) qui ils soient enquêteurs, vérificateurs ou à la caisse d'un Centre des Finances Publiques. La DGFIP a pris différentes mesures préventives, de protection et d'accompagnement pour mieux répondre aux risques et aux demandes de ses agents. Par ailleurs, elle a également renforcé sa cybersécurité et ses bases de données par respect de la législation sur "l'information et les libertés" et sécuriser ses données.

La politique de prévention en matière de sécurité au travail au sein de la DGFIP (I) et de ses bases de données (II) doit permettre de répondre aux différents risques encourus par la DGFIP et ses agents.

I. La politique de Prévention de sécurité à la DGFIP

A l'été 2018, un plan d'Actions et une politique de prévention et de protection de ses agents a été mis en place (A) en partenariat avec différents acteurs de la sécurité et de protection des agents (B)

A. de PLAN d'urgence et de sécurité

Cette politique de prévention et de protection fait suite à de nombreux incidents subis par les agents de l'administration (effractions, insultes, vols, incendies, agressions).

Aussi, un plan d'urgence sécurité a été mis en place en 6 actions.

Dans un premier temps, pour respecter les agents de la DGFIP, une campagne de communication envers le public a été mise en place. Avec notamment l'affiche "ensemble, faisons le droit de la cartable et du respect". Avec également, rajout de mentions sur les sorties entrées, et le cisisme sur la charte du contribuable, les imprimés au droit de communication.

Dans un second temps, la DGFIP a décidé de diminuer les fonds au sein des CFIP (Centres des Finances Publiques) avec la possibilité de paiement par carte bancaire et la modification des dérogations de fonds.

Dans un troisième temps, a été décidé la mise en place d'un plan de sécurisation des bâtiments grâce à un diagnostic sécurité pour identifier les sites les plus exposés. Aussi, la Direction départementale à la sécurité avec les chefs de services ont pu mettre en place des règles de sécurité immobilière grâce à une analyse et en faisant des test-anti-agressions.

Dans, un quatrième temps, une politique de prévention en faveur des agents a été mise en place. Aussi, les agents ont été formés à la protection et sécurité en 2013, à la gestion des conflits. Par ailleurs, des guides de procédures ont été mis à jour pour être mieux adaptés aux crises. La Direction communique des fiches de sécurité aux agents et doit mettre à jour les fiches lors des périodes d'affluences.

Dans un cinquième temps, il a été consolidé l'accompagnement des agents face des incidents. Avec une prise en charge et un suivi personnalisé par l'Assistant au Réseau de prévention, avec l'aide d'une protection juridique et un protocole d'analyse après l'incident. Aussi un numéro d'urgence à la Direction a été mis en place sur les différents sites.

Enfin, une protection renforcée des agents a été mise en œuvre avec l'identification des risques psychosociaux, des vérifications, acquiescement. Cela pour avoir recours en cas de dossier sensible, public dangereux aux forces de Police ou judiciaires.

La sécurité des agents et également liée à la multiplication d'acteurs de prévention au sein de l'entreprise.

B. Les acteurs de la sécurité à la DDFIP

La mise en place de Télésurveillance, guichets sécurisés ou le contrôle d'accès ne suffit pas pour faire face à la sécurité au sein de la DDFIP.

De nombreux acteurs existent au sein de la DDFIP au autour de celle-ci.

C'est le cas de l'Assistant de prévention qui assiste conseil le DDFIP (Directeur des Finances Publiques) concernant les règles d'hygiène et sécurité au travail grâce au DUERP (Document unique évaluation des risques professionnels). Il collabore avec le Réseau de prévention, l'Inspecteur de sécurité au travail et CHSCT (Comité d'hygiène et sécurité du Travail) pour élaborer une politique de prévention, des actions préventives, le TRVS (Tableau de bord de veille sociale). Il sensibilise, informe les agents aux différents risques encourus. Au sein de chaque Direction ont été nommés en avril 2013 un Référent de protection juridique (RPJ).

permettant de savoir, accompagner les agents
agressés ou victimes. Il doit également informer
RH2B et le Directeur des mesures de prévention
prises suite à l'incident. Lors d'incident grave,
il met en place un suivi des risques, des actions
pénales avec l'agent.

Par ailleurs, il est en lien avec le délégué départemental
à la sécurité qui lui met en œuvre les règles de
sécurité de sa Direction en lien avec les chefs de
service et le DGFIP. Il propose et forme les
différents chefs de services notamment sur les transports
de fonds et le fonctionnement des alarmes.

Enfin, SPIB-2C, cellule à Bergu, s'occupe d'
un plan urgent sécurité avec la mise en place
de la télé-surveillance, l'auto-protection, la pose de
guichets sécurisés, la sécurisation de la partie
administrative par des codes d'accès.

Les divers risques psychosociaux, soit la
santé psychique au travail sont répertoriés grâce
à la fiche de prévention des risques remplie
par les agents, le DGFIP et le TBUS.
Grâce à ces outils, la DGFIP a pu mettre en place
des évolutions et aider les agents.

Aussi, la prévention passe par l'information et
la formation des agents (développement, évacuation,
risques psychosociaux).

La sécurité des agents n'est pas la seule qui
doit être vérifiée, celle des données informatiques
et également être importante.

II. La sécurité des bases de données au sein de la DGFIP

Face aux risques informatiques (A) la
contrôle interne et de traçabilité paraît également

nécessaire (B).

A. Les risques informatiques au sein de la DGFIP

Face aux données importantes et confidentielles que contient les différentes bases de données de la DGFIP, et aux nombreuses cyberattaques qu'elle doit faire face. Il est nécessaire que chaque agent, service sécurisé au mieux les informations professionnelles.

Par ailleurs, au regard des données à caractère professionnel et non personnelle, la CNIL (Commission nationale des informations et libertés) considère une divulgation d'information comme une infraction au sein de la législation d'informatique et de libertés.

Aussi, les agents doivent au mieux sécuriser leurs mots de passe en utilisant des majuscules, caractères spéciaux, chiffres et d'acronyms & caractères. Les mots de passe ne doivent pas être divulgués, ni à un collègue, ni à son bureau.

Par ailleurs, de nombreux clics sur des pièces jointes entraîne des virus qui peuvent bloquer les applications au sein d'une direction pendant plusieurs jours. Aussi, 15 000 postes doivent être réinstallés chaque année suite à l'infection d'un virus.

Enfin, les postes de travail sous Windows XP ont été progressivement supprimés d'accès à internet car la sécurité n'est pas optimale. En cas de doute, il existe une assistance téléphonique, qui n'a pas besoin du mot de passe pour accéder à distance et réparer les applications informatiques.

De plus, un contrôle interne et la traçabilité des informations est nécessaire.

Q2. D'après vous, quels sont les enjeux de la sécurité numérique en France et quels sont les principaux acteurs.

Le 16 octobre 2015, le Premier ministre Manuel Valls, a présenté la stratégie nationale par la sécurité du numérique.

Face au développement du Numérique, des réseaux sociaux, de la mondialisation, la politique de sécurité du numérique est une réponse de l'État aux dangers des cyberattaques dans un espace numérique mondial.

Les enjeux de la sécurité du Numérique en France (I) grâce à quelques acteurs (II) de la sécurité du numérique (II) qui y font face.

I. Les enjeux de la sécurité du Numérique.

La stratégie nationale par la sécurité du numérique du 16/10/2015 fait face à l'augmentation des utilisations des données numériques, des entreprises et métiers liés au numérique et des diverses menaces qui ont touchés ces dernières années et mais les particularités, entreprises privées et le secteur public. Aussi, 5 objectifs sont ressortis de cette stratégie.

Dans un premier temps, de garantir la souveraineté nationale en renforçant la sécurité et infrastructures critiques.

Dans un second temps apporter une réponse aux différentes cyberattaques contre l'ETAT, les entreprises et les particuliers. Avec un dispositif d'assistance aux victimes de malveillance.

Dans un troisième temps, sensibiliser, former à la cybersécurité notamment dès l'école et en entreprise. Des experts à la cybersécurité doivent apparaître.

Dans un quatrième temps, faire de la sécurité informatique un facteur de croissance économique. Pour ce faire, il faut encourager l'investissement, l'innovation aux entreprises offrant des produits et services de sécurité numérique.

Enfin, renforcer la coopération internationale et européenne en matière de cybersécurité. La France doit promouvoir cette stratégie de cybersécurité en soutenant les pays les moins développés notamment en Afrique.

L'ETAT a un rôle majeur, mais chaque citoyens, entreprises doit permettre de faire face aux risques liés à la sécurité informatique.

II. Les différents acteurs de la sécurité numérique en France

Hormis l'ETAT, d'autres acteurs contribuent à la sécurisation du numérique.

Aussi chaque ministère a la charge de sa sécurité et est assisté d'un haut fonctionnaire délégué à la Défense et à la Sécurité (HFDSS). Celui-ci anime et pilote la sécurité des systèmes d'information et des différents applications. Il a la charge de nommer un RSSI (Responsable

de sécurité des systèmes d'information) qui sera amenée à l'aider dans la sécurité. Par ailleurs les différents services contractuels disposent tous d'experts de haut-niveau dédiés à la sécurité informatique.

De surcroît, l'agence nationale de sécurité des systèmes de l'information (ANSSI) crée le 7/07/2009 assure la sécurité et la défense des systèmes d'information de l'ÉTAT et contribue à celle des opérateurs nationaux d'importance vitale (OIV).

Elle doit prévenir les menaces grâce à des mesures de protection, défendre les systèmes d'information grâce à la détection des incidents et fautes, en cas cyberattaques, et informer les différents publics avec la production des bonnes pratiques et des recommandations.

50 agents travaillent à l'ANSSI mais en cas d'attaque sont effectifs pourra être renforcé. Par ailleurs, en 2015, l'agence sera élargie avec un dispositif d'action territoriale au plus près des entreprises et collectivités territoriales.

Enfin, la CNIL a pour rôle de contrôler le droit à l'information et aux libertés.

Le but essentiel est d'avoir une bonne confiance dans le numérique permettant une stabilité de l'ÉTAT, un développement économique et une meilleure protection des citoyens face aux dangers du numérique.