PCIE Passeport de Compétences Informatique Européen

ECDL European Computer Driving Licence

Sécurité des TI

Syllabus Version 1.0

VF 1.4 mars 2017

Le Syllabus : Référentiel de connaissances du PCIE

1. Introduction

Le Passeport de Compétences Informatique Européen est administré à travers le monde par la Fondation ECDL. Le Syllabus du PCIE est le Référentiel des connaissances nécessaires à l'obtention de la certification.
Le Syllabus ECDL est une description standard et identique dans tous les pays. Il a été réalisé par le groupe de travail SQA (Syllabus, Question Test Base, Automation) et par le Comité Technique de la Fondation ECDL qui comprennent près de 450 experts.

Les connaissances décrites dans le Syllabus ne font pas référence à un matériel ou à un logiciel donné, elles en sont indépendantes. Seules les instances nationales, qui déclinent les tests sur des systèmes existants, font appel à des logiciels ou matériels identifiés. Certains pays possèdent des versions multiples du PCIE pour différentes marques de systèmes et de logiciels bureautiques.

2. Le Passeport de Compétences Informatique Européen

Le « Passeport de Compétences Informatique Européen » (PCIE), ou « European Computer Driving Licence » (ECDL) ou « International Computer Driving Licence » (ICDL) en anglais, est un certificat qui indique que son détenteur a passé avec succès un test qui mélange l'évaluation des compétences théoriques et pratiques sur une thématique donnée.

2.1 Quels en sont les bénéfices?

Les bénéfices de l'utilisation du PCIE sont multiples et originaux par rapport à d'autres produits d'évaluation de compétences concurrents.
D'une part, l'approche délibérément orientée vers l'utilisateur de la bureautique donne au PCIE un aspect convivial et non contraignant qui pourra être mis à son profit. Il ne s'agit pas de faire une évaluation scolaire ou théorique des compétences, mais de faire s'approprier par l'utilisateur le concept d'auto-évaluation selon ses propres besoins. Le rôle du test étant ainsi perçu plus au bénéfice de son utilisateur qu'à son détriment. De plus, l'absence de contrainte ou de sanction négative augmente l'acceptabilité et surtout la motivation du candidat pour l'adopter à son profit.

D'autre part, le caractère européen et la notion de standard augmente la crédibilité du PCIE qui est ressentie par le candidat comme une valorisation des enseignements ou des acquis. On peut résumer comme suit les avantages du PCIE selon les angles d'approche des acteurs concernés.

Pour le collaborateur :

- Il incite à une meilleure connaissance de son environnement informatique.
- Il permet de se mesurer de son propre gré, sans contrainte et dans la durée, à un standard.
- Il fournit une preuve, incontestable et mondialement reconnue, de ses compétences.

Pour les personnes en recherche d'emploi :

- Il démontre sur le marché de l'emploi l'expérience acquise sur le terrain ou par des formations.
- Il fait un bilan des connaissances avant de suivre une reconversion ou pour obtenir un stage de formation d'un niveau adapté.

Pour l'étudiant :

- Il valide la qualité des enseignements et des connaissances acquises.
- Il facilite la recherche d'un stage ou d'un premier emploi.

Pour la Direction des Ressources Humaines :

- Il offre un outil motivant et non contraignant dans l'évaluation des compétences de tous les collaborateurs : cadres, techniciens, agents, ouvriers.
- Il permet d'optimiser et d'adapter à l'individu les formations futures.
- Il peut valider les acquis après formation.
- Il incite à l'auto-formation et l'auto-évaluation.
- Il entraîne un accroissement général des compétences de l'entreprise.

Pour la Direction Informatique :

- Il rapproche le collaborateur des préoccupations de la DI.
- Il réduit les recours à la hot line interne ou externe (50% du coût réel du PC sont dus à une mauvaise utilisation ou des erreurs d'organisation).

Pour l'Organisme de formation :

- Il atteste le niveau des formations par un certificat validé et mondialement reconnu.
- Il fidélise les personnes formées.
- Il encourage à un développement des formations dans tous les domaines importants de la bureautique.

2.2 Les objectifs du PCIE

Les objectifs du PCIE sont multiples :

- Elever le niveau global des compétences d'une population dans la pratique de l'ordinateur.
- Accroître le niveau de productivité de tous les collaborateurs dans leur travail quotidien.
- Inciter à une meilleure utilisation des investissements dans les technologies de l'information : à l'école, à la maison, dans l'entreprise.
- S'assurer que les utilisateurs comprennent les bonnes pratiques et les problèmes de qualité et d'organisation dans l'utilisation de l'ordinateur individuel.
- Permettre à tous les utilisateurs d'applications bureautiques de posséder une preuve de leur maîtrise et de leur compétence.
- Optimiser les plans de formation professionnelle en bureautique.

Outre ses caractéristiques uniques et son approche délibérément orientée vers l'utilisateur, le PCIE apporte sa contribution à l'autonomie et à la mobilité du travailleur Européen.

Les technologies de l'information sont les clés de la production et de la recherche de l'information. Le PCIE contribue à ce mouvement des entreprises et des collaborateurs vers une meilleure utilisation de ces technologies.

2.3 Les modules du PCIE

La certification PCIE est constituée de plusieurs modules portant sur différentes thématiques de l'utilisation de l'outil informatique. Il est possible pour chaque candidat de passer un ou plusieurs modules parmi les suivants :

PCIE Syll.vers.1 - Module de Base - Les Essentiels de l'Ordinateur
PCIE Syll.vers.1 - Module de Base - Les Essentiels du Web
PCIE Syll.vers.5 - Module de Base - Traitement de Texte
PCIE Syll.vers.5 - Module de Base - Tableur
PCIE Syll.vers.5 - Module Standard - Base de Données Utilisateur
PCIE Syll.vers.5 - Module Standard - Présentation
PCIE Syll.vers.1 - Module Standard - CAO 2D
PCIE Syll.vers.2 - Module Standard - Edition Image
PCIE Syll.vers.2 - Module Standard - Edition Site Web
PCIE Syll.vers.1 - Module Standard - Gestion de Projets
PCIE Syll.vers.1 - Module Standard - Travail Collaboratif en Ligne
PCIE Syll.vers.1 - Module Standard - Sécurité des TI
PCIE Syll.vers.1 - Module Avancé - Traitement de texte
PCIE Syll.vers.1 - Module Avancé - Tableur
PCIE Syll.vers.1 - Module Avancé - Base de Données
PCIE Syll.vers.1 - Module Avancé - Présentation

3. Le passage du Passeport de Compétences Informatique Européen

3.1 La Carte PCIE

La Carte PCIE représente un identifiant unique et international rattaché à un candidat PCIE, et valable à vie. La Carte PCIE enregistre au fur et à mesure les modules réussis qui sont ensuite portés sur le certificat PCIE qui pourra être montré lors d'entretiens ou de demandes de formation.

Le candidat au PCIE peut :

- choisir son centre PCIE accrédité en fonction de sa situation. Ce peut être son entreprise, son organisme de formation, son école, etc.
- passer les modules au moment opportun, par exemple selon une programmation au sein de l'entreprise, ou en début ou en fin de formation professionnelle.
- repasser les modules qui ont posé problème plus tard après une mise à jour des connaissances.

La Carte PCIE est créée dès que le candidat s'inscrit auprès d'un centre d'examen PCIE. Elle est virtuelle, c'est-à-dire administrée via Internet par le Centre en charge du candidat. Elle est mise à jour automatiquement chaque fois qu'un test est passé. Le centre pourra à tout moment imprimer le certificat du candidat, et en particulier si le candidat quitte le centre.

3.2 Validité de la Carte et du Certificat PCIE

Les tests du PCIE peuvent être passés à tout moment après l'acquisition de la Carte PCIE. Les tests peuvent être passés dans n'importe quel centre habilité. La Carte PCIE est strictement personnelle, non transférable dès le moment qu'un nom de candidat lui a été assigné et qu'un test a été passé, quelles qu'en soient les raisons.
La durée de validité d'un module inscrit sur un certificat PCIE est de trois ans.

4. Organisation du Syllabus

4.1 Catégories

Chaque module est décrit par une séquence de Catégories. Une Catégorie rassemble un domaine de compétences ou de connaissances liées à une partie significative du module. Les résultats des tests sous forme graphique font référence aux Catégories.

4.2 Sous-catégories

Chaque catégorie contient des sous-catégories. Une sous-catégorie précise les sous domaines de compétences à maîtriser dans une Catégorie donnée.
Une sous-catégorie est définie par un ou plusieurs items (ou éléments individuels de compétences).

4.3 Items - Eléments individuels de compétences

Ce sont les lignes qui décrivent les points de compétences ou de connaissances demandées par le PCIE.
Dans le texte du Syllabus, chaque item reçoit, avant sa définition textuelle, un chiffre entre 1 et 3 : ce chiffre indique le niveau de complexité des questions pouvant être posées sur cet item.

- Les items de niveau 1 seront testés avec des questions faciles ou très faciles, à la portée de toute personne ayant une connaissance élémentaire des Technologies de l'information et des applications.

  Elles servent à vérifier le fondement des connaissances et des compétences basiques des candidats, et aussi à déstresser les candidats et les encourager. En gros, un candidat de niveau PCIE devrait avoir 90% de bonnes réponses à ces questions.
- Aux items de niveau 2 correspondront des questions qui nécessitent d'avoir reçu une formation de base ou bien d'avoir une certaine expérience pratique ou basée sur une bonne appréciation générale des problèmes, avec l'item en question. Un candidat ayant le niveau PCIE devrait avoir environ 60% de réponses correctes à ces questions.
- Les items de niveau 3 correspondent à des compétences plus avancées, sans qu'elles relèvent d'une expertise poussée sur l'item. Un candidat devrait avoir 40% de bonnes réponses pour ces questions.

4.4 Explications supplémentaires sur les niveaux donnés aux items du Syllabus

1. La difficulté donnée aux items dans le Syllabus est une bonne indication du niveau qui est demandé dans les contenus de formation : cela signifie qu'il n'est pas besoin de couvrir l'ensemble d'une fonctionnalité, y compris ses aspects complexes, pour apporter la connaissance nécessaire à un item de niveau 1 ou 2.

2. La difficulté donnée aux items dans le Syllabus est aussi une bonne indication de la "complexité apparente" de l'item par rapport à une utilisation quotidienne.

- Certaines fonctionnalités sont bien connues par certains et moins par d'autres.
- Elles font l'objet de formations qui peuvent être spécifiques, ou plus générales.
- Elles sont utilisées tous les jours par certains et moins souvent par d'autres.
- Elles sont élémentaires pour certains et assez compliquées pour d'autres.

On trouvera donc, pour certaines catégories ou sous catégories, des items de niveau 2 ou 3, alors que la formation les couvre très bien ou même de manière supérieure au Syllabus. Cela tient au niveau de compétences de bases que le PCIE veut tester, et l'utilisation globale qui en est faite par les utilisateurs.

4.5 Composition d'un test en termes de complexité

Le nombre de questions des différents niveaux dans chaque test est variable, mais pour un test de 36 questions il se situe aux alentours de 20 questions de niveau 1, 10 questions de niveau 2 et 6 questions de niveau 3.
Dans la suite les temps indiqués sont relatifs au passage avec le système automatisé.

5. Un système adapté pour les personnes handicapées

Bien que les informations figurant dans ce référentiel soient relatifs au passage de l'examen PCIE avec le système automatisé, il existe 2 systèmes adaptés pour les personnes handicapées.

5.1 Système automatisé adapté

Chaque centre d'examen PCIE utilisant le système de test automatisé PCIE peut à tout moment faire la demande d'activation du tiers-temps supplémentaire à l'attention des personnes handicapées. Le temps du test passe alors de 35 min à 47 min.
Cette option est exclusivement réservée aux personnes handicapées, et fait l'objet d'un processus de vérification auprès des centres qui l'utilisent.

5.2 Système manuel adapté

Certains centres d'examen spécialisés disposent également d'un processus d'évaluation et de certification de compétences appelé système manuel. Ce processus implique qu'une personne physique habilitée (formateur, examinateur) évalue les compétences du candidat en temps réel en lui soumettant un certain nombre d'exercices et de tâches à accomplir. L'examinateur suit un processus strict d'évaluation, équivalant au système automatisé mais permettant plus de souplesse afin de s'adapter au handicap du candidat.

5.3 Référentiel et Certificats pour personnes handicapées

Le référentiel PCIE utilisé est identique quel que soit le système d'évaluation utilisé. Il n'est fait d'aucune mention du système d'évaluation utilisé sur le certificat PCIE.

Introduction

Sécurité des TI

CCe module expose les concepts essentiels et les techniques à maîtriser pour comprendre les principaux éléments qui assurent une sécurité dans l'utilisation des TIC (Technologies de l'Information et de la Communication) au quotidien. Ceci passe notamment par la maîtrise des techniques et applications appropriées pour conserver une connexion sécurisée au réseau, pour utiliser Internet en toute sécurité et pour manipuler les données et les informations de manière adaptée.

Objectifs du module

Les candidats qui réussiront ce module seront capables de :

- comprendre les concepts clés relatifs à l'importance d'assurer la sécurité des informations et des données, d'assurer leur sécurité physique, d'éviter le vol de données personnelles et de protéger leur vie privée,
- protéger un ordinateur, un dispositif numérique mobile, un réseau contre les logiciels malveillants (malware) et les accès non-autorisés,
- connaître les différents types de réseaux, de connexions et les composants spécifiques tels que le pare-feu (firewall) qui peuvent poser problème lors des connexions,
- naviguer sur le World Wide Web et communiquer en toute sécurité sur Internet,
- comprendre les problèmes de sécurité liés à la communication, notamment en matière de courrier électronique et de messagerie instantanée (MI – IM/Instant messaging),
- sauvegarder et restaurer des données de manière appropriée et sécurisée, entreposer ses données et ses dispositifs numériques mobiles en toute sécurité.

Test et Evaluation du module « Sécurité des TI »

Temps alloué : 35 minutes.

Nombre de questions : 36.

Barre de succès : 75% de bonnes réponses.

Beaucoup de questions demandent une réflexion sur les objets présents dans l'écran, et permettent un autoapprentissage des bonnes pratiques ou des fonctions usuelles du domaine couvert.

Quelques conseils pour réaliser son test avec le maximum de chances de succès :

- Bien prendre son temps à chaque question : la lire deux fois posément et complètement.
- Ne jamais répondre trop vite (bien qu'il n'y ait jamais de piège dans les questions).
- Pour les questions QCM : lire complètement les réponses, et travailler par élimination.
- Pour les questions à zones sensibles : examiner l'image en détail, utiliser les éléments de la question.
- Analyser et retenir le sens des questions et des réponses quand il s'agit de bonnes pratiques ou de règles de productivité.

Catégorie	Domaine	Réf.	Dif.	Connaissances requises
1. Concepts de sécurité	1.1 Menaces sur les données	1.1.1		Faire la différence entre les données et les informations
		1.1.2		Comprendre le terme : cybercriminalité
		1.1.3		Comprendre la différence entre hacker (hacking), cracker (cracking) et pirater dans un but éthique (ethical hacking)
		1.1.4		Connaître les menaces majeures pour la sécurité des données comme : les incendies, les inondations, les guerres, les tremblements de terre
		1.1.5		Connaître les menaces pour la sécurité des données causées par : les employés, le fournisseur d'accès, les personnes externes
	1.2 Valeur de l'information	1.2.1		Comprendre pourquoi il est important de protéger les informations personnelles, notamment : pour éviter le vol d'identité, pour éviter les fraudes
		1.2.2		Comprendre pourquoi il est important de protéger des données commerciales sensibles, notamment : pour éviter le vol ou le détournement d'informations sur les clients, pour éviter le vol de données financières
		1.2.3		Identifier les mesures à prendre pour empêcher les accès non-autorisés aux données comme : le cryptage des données, l'utilisation de mots de passe
		1.2.4		Comprendre les caractéristiques de base de la sécurisation de l'information comme : la confidentialité, l'intégrité, la disponibilité des données
		1.2.5		Identifier les principales règles de protection, de conservation et de contrôle des données / données privées en vigueur dans votre pays
		1.2.6		Comprendre l'importance de créer et d'adopter des directives (lignes de conduite / guidelines) et des réglementations (policies) en matière d'utilisation des TIC
	1.3 Sécurité personnelle	1.3.1		Comprendre le terme : ingénierie sociale (social engineering) et ses implications comme : la collecte d'informations, la fraude, l'accès au système informatique

Catégorie	Domaine	Réf.	Dif.	Connaissances requises
		1.3.2		Identifier les méthodes employées pour l'ingénierie sociale comme : les appels téléphoniques, l'hameçonnage, l'espionnage par-dessus l'épaule (shoulder surfing)
		1.3.3		Comprendre le terme : vol d'identité et ses implications dans les domaines : personnels, financiers, des affaires, légaux
		1.3.4		Identifier les méthodes de vol d'identité comme : escroquerie exploitant d'anciens matériels et / ou informations (information diving), escroquerie à la carte de paiement (skimming), escroquerie par abus de confiance (pretexting)
	1.4 Sécurité des fichiers	1.4.1		Comprendre les effets de l'activation / la désactivation des macros dans les options de sécurité des applications
		1.4.2		Utiliser un mot de passe pour les fichiers comme : les documents, les fichiers compressés, les classeurs / feuilles de calculs
		1.4.3		Comprendre les avantages et les limites du cryptage des données
2. Logiciels malveillants	2.1 Définition et fonctionnement	2.1.1		Comprendre le terme : logiciel malveillant (malware)
		2.1.2		Reconnaître les différentes techniques adoptées par les logiciels malveillants pour rester masqués comme : le cheval de Troie (Trojan), le logiciel malveillant furtif (rootkit) et la porte dérobée (backdoor)
	2.2 Types	2.2.1		Reconnaître les différents types d'infections produits par les logiciels malveillants et comprendre comment ils agissent, notamment : les virus, les vers informatiques
		2.2.2		Reconnaître les types de vols de données, les bénéfices produits par l'emploi de logiciels malveillants de vol de données et comprendre comment ils fonctionnent notamment : le logiciel publicitaire (adware), le logiciel espion (spyware), la machine zombie (botnet), l'enregistreur de frappe (keystroke logging) et le composeur de numéros téléphoniques (dialler)

Catégorie	Domaine	Réf.	Dif.	Connaissances requises
	2.3 Protection	2.3.1		Comprendre comment fonctionne un logiciel anti-virus et identifier ses limites
		2.3.2		Analyser/scanner des lecteurs, dossiers, fichiers spécifiques avec un logiciel anti-virus. Planifier les analyses en utilisant un logiciel anti-virus
		2.3.3		Comprendre le terme : quarantaine et l'effet d'une quarantaine sur des fichiers infectés ou suspects
		2.3.4		Comprendre l'importance de télécharger et d'installer régulièrement les mises-à-jour des logiciels anti-virus et les nouvelles signatures de virus reconnues par votre anti-virus
3. Sécurité réseau	3.1 Réseaux	3.1.1		Comprendre le terme : réseau et reconnaître les principaux types de réseaux comme : réseau local (Local Area Network (LAN)), réseau étendu (Wide Area Network (WAN)), réseau privé virtuel (Virtual Private Network (VPN))
		3.1.2		Comprendre le rôle de l'administrateur réseau dans la gestion des comptes utilisateurs, des droits d'accès, des autorisations et des espaces disques alloués aux utilisateurs
		3.1.3		Comprendre l'utilité et les limites d'un pare-feu (firewall)
	3.2 Connexions réseaux	3.2.1		Connaître les différentes façons de se connecter à un réseau comme : par câble, sans-fil (wireless)
		3.2.2		Comprendre que le fait de se connecter à un réseau peut entraîner des problèmes de sécurité comme : apparition de logiciels malveillants, accès non autorisés aux données privées, failles de protection des données personnelles
	3.3 Sécurité en environnement sans fil	3.3.1		Connaître l'importance d'imposer la saisie d'un mot de passe pour protéger l'accès à un réseau sans fil
		3.3.2		Connaître les différents types de sécurisation d'un réseau sans fil comme : Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Media Access Control (MAC)

Catégorie	Domaine	Réf.	Dif.	Connaissances requises
		3.3.3		Être conscient que l'utilisation d'un réseau sans fil non-protégé peut permettre l'espionnage de vos données personnelles
		3.3.4		Se connecter à un réseau sans fil protégé / non-protégé
	3.4 Contrôle d'accès	3.4.1		Comprendre l'utilité d'un compte utilisateur pour se connecter à un réseau et l'importance de toujours passer par la saisie d'un nom d'utilisateur et d'un mot de passe pour accéder au réseau
		3.4.2		Connaître les bonnes pratiques en matière de mot de passe comme : ne pas le partager avec d'autres utilisateurs, le changer régulièrement, le choisir de longueur suffisante, y mélanger des caractères très variés (lettres, chiffres et caractères spéciaux)
		3.4.3		Connaître les principales possibilités de contrôle d'accès biométrique comme : lecteur d'empreintes digitales, scanner rétinien
4. Utilisation sécurisée du Web	4.1 Navigation Web	4.1.1		Savoir que certaines activités en ligne (achats, transactions bancaires) ne devraient être effectuées que sur des pages Web sécurisées
		4.1.2		Reconnaître un site Web sécurisé : https, symbole de cadenas
		4.1.3		Etre conscient des risques de redirection vers des sites malveillants (pharming)
		4.1.4		Comprendre le terme : certificat numérique. Mettre en fonction un certificat numérique
		4.1.5		Comprendre le terme : mot de passe à usage unique
		4.1.6		Choisir les réglages appropriés pour activer, désactiver la fonction de remplissage automatique de formulaire / de sauvegarde automatique des données de formulaire lors du remplissage d'un formulaire sur le Web
		4.1.7		Comprendre le terme : mouchard électronique (cookie)
		4.1.8		Choisir les réglages appropriés pour autoriser, bloquer les mouchards électroniques (cookies)

Catégorie	Domaine	Réf.	Dif.	Connaissances requises
		4.1.9		Supprimer les données personnelles dans un navigateur comme : l'historique de navigation, les fichiers Internet temporaires, les mots de passe, les mouchards électroniques (cookies), les données de remplissage automatique de formulaires Web
		4.1.10		Comprendre le but, la fonction et les types de logiciels de contrôle de contenus comme : les logiciels de filtrage Web, les logiciels de contrôle parental
	4.2 Réseaux sociaux	4.2.1		Comprendre l'importance de ne pas diffuser d'informations confidentielles sur des sites de réseaux sociaux
		4.2.2		Etre attentif à l'importance d'appliquer les bons réglages de confidentialité pour les comptes de réseaux sociaux
		4.2.3		Comprendre les risques potentiels lors de l'utilisation des réseaux sociaux comme : le harcèlement par le Web (cyberbullying), la manipulation psychologique (grooming), les informations trompeuses / dangereuses, les identités falsifiées, les liens ou messages frauduleux
5. Communications	5.1 E-Mail	5.1.1		Comprendre le rôle du cryptage, décryptage d'un e-mail
		5.1.2		Comprendre le terme : signature numérique
		5.1.3		Créer et ajouter / importer un certificat numérique
		5.1.4		Être conscient de la possibilité de recevoir des e-mails frauduleux et non-sollicités
		5.1.5		Comprendre le terme : hameçonnage (phishing). Identifier les principales caractéristiques d'hameçonnage comme : utiliser le nom d'entreprises connues, de personnes connues, proposer des liens Internet falsifiés
		5.1.6		Etre conscient du risque d'infecter l'ordinateur par des logiciels malveillants en ouvrant une pièce jointe (contenant une macro ou un fichier exécutable)

Catégorie	Domaine	Réf.	Dif.	Connaissances requises
	5.2 Messagerie instantanée (MI/IM)	5.2.1		Comprendre le terme : messagerie instantanée (MI/IM) et ses utilisations possibles
		5.2.2		Comprendre les failles de sécurité liées aux messageries instantanées comme : les logiciels malveillants (malware), les portes dérobées (backdoor access), les accès non-autorisés aux fichiers
		5.2.3		Connaître les méthodes pour assurer la confidentialité lors de l'utilisation des messageries instantanées comme : le cryptage, ne pas diffuser d'informations importantes, limiter le partage des fichiers
6. Gestion de la sécurité des données	6.1 Sécuriser et sauvegarder les données	6.1.1		Connaître les méthodes pour s'assurer de la sécurité physique des dispositifs numériques mobiles comme : gérer efficacement les emplacements et les caractéristiques des appareils, utiliser un câble de verrouillage, limiter les accès aux appareils
		6.1.2		Connaître l'importance de maîtriser la procédure de sauvegarde (backup) en cas de perte de fichiers, de données comptables, d'historique de navigation et de signets
		6.1.3		Identifier les paramètres d'une procédure de sauvegarde comme : régularité/fréquence, planification des tâches de sauvegarde, emplacement de stockage de la sauvegarde
		6.1.4		Sauvegarder des données
		6.1.5		Restaurer et valider la restauration de données en provenance d'une sauvegarde
	6.2 Destruction sécurisée	6.2.1		Comprendre l'importance de pouvoir détruire de manière définitive des données qui se trouvent dans un lecteur ou dans un dispositif numérique mobile
		6.2.2		Faire la distinction entre un effacement et une totale destruction (définitive) de données

Catégorie	Domaine	Réf.	Dif.	Connaissances requises
		6.2.3		Identifier les méthodes habituelles de suppression définitive de données comme : utiliser un logiciel de suppression de données (shredding), détruire le lecteur/support, démagnétiser le support de données, utiliser un utilitaire de destruction de données