GHDE Formation

Référentiel de certification et d'évaluation

Maîtriser les Concepts de la CyberSécurité

Sujet du document	Référentiel de certification			**Version**	V1.0
Description brève	Ce document décrit en détail le référentiel de la certification *Maîtriser les concepts de la cybersécurité*.				
Propriétaire	*GH Digital Evolution*	**Rôle**	Organisme certificateur et organisme de formation	**Date**	*29/04/2025*
Vérifié par					
Approuvé par					

Historique du document référentiel

Version	Date	Statut	Auteur	Description
V0.1	*11/03/2025*	*Draft*	*GH Digital Evolution*	*Initialisation du document*
V0.2	*20/03/2025*	*Draft*	*GH Digital Evolution*	*Fin de l'élaboration de la partie de présentation de la certification*
V0.3	*20/03/2025*	*Draft*	*GH Digital Evolution*	*Début de la rédaction du référentiel de compétences et dévaluation.*
V0.4	*26/03/2025*	*Draft*	*GH Digital Evolution*	*Fin de la rédaction du référentiel de compétence et dévaluation.*
V0.5	*03/04/2025*	*Draft*	*GH Digital Evolution*	*Changement du titre de la certification.*
V1.0	*29/04/2025*	*Publication*	*GH Digital Evolution*	*Publication de la version 1 du document*

Sommaire

1- Introduction

À l'ère du numérique, la **cybersécurité** est devenue un **enjeu majeur** pour les entreprises. Face à la multiplication des cybermenaces, il est essentiel de renforcer la protection des systèmes et des données afin de prévenir les risques d'attaques.

Les organisations manipulent quotidiennement des **informations sensibles**, qu'il s'agisse de données personnelles, de secrets industriels ou d'actifs stratégiques. Une faille de sécurité peut entraîner des conséquences désastreuses, pertes financières, atteinte à la réputation, sanctions juridiques, voire mise en danger de vies humaines. Assurer la confidentialité, l'intégrité et la disponibilité des données est donc **crucial** pour garantir la confiance des clients et des partenaires.

Dans un monde où les logiciels et les infrastructures numériques sont omniprésents, **toute organisation impliquée dans leur développement se doit d'intégrer la cybersécurité au cœur de ses processus**. Cela implique une parfaite maîtrise des concepts fondamentaux et des meilleures pratiques en matière de sécurité, indispensables pour évoluer dans un environnement numérique fiable et conforme aux exigences réglementaires actuelles.

C'est dans cette optique que cette **certification a été conçue**. Elle vise à doter les professionnels des **compétences essentielles** pour comprendre, analyser et mettre en œuvre des solutions de cybersécurité efficaces, garantissant ainsi une protection optimale des systèmes et des données.

2- À propos du certificateur

Ce référentiel, dédié à la certification « **Maîtriser les concepts de la cybersécurité** », a été élaboré par **GH Digital Evolution**, organisme de formation opérant sous le nom commercial **GHDE Formation**.

GHDE Formation est spécialisé dans les domaines du **génie logiciel** et de la **cybersécurité**. L'ensemble du contenu de ce référentiel a été conçu par son équipe d'experts, composée de professionnels issus du génie logiciel, de la cybersécurité et de l'ingénierie pédagogique.

Afin de garantir un référentiel en phase avec les **exigences du marché**, ces experts conjuguent leurs activités pédagogiques avec une expérience concrète en entreprise. Cette double approche permet d'assurer une formation alignée sur les besoins réels du tissu industriel et les évolutions constantes du secteur.

3- Présentation de la certification

Le tableau ci-dessous représente les caractéristiques principales de la certification :

Maîtriser les concepts de la cybersécurité				
	*Référence interne*	**GHDEF-CERT-01**	*Difficulté*	*Moyenne*
	Organisme	*GH Digital Evolution*	*Durée*	*90 minutes*
	Prérequis	*Aucun*		
	Validation	*Obtenir 80% de bonnes réponses*		
	Langue	*Français*		
	Modalité	*QCM – 80 questions*		
	Site web	https://ghdeformation.fr/nos-certifications/		

3.1- Les objectifs et le contexte de la certification

La certification ***Maîtriser les concepts de la cybersécurité*** vise à former des professionnels de l'IT (**I**nformation **T**echnology en anglais – **T**echnologie de l'**I**nformation) capables de choisir, développer, et mettre en œuvre des solutions de cybersécurité au sein d'un environnement logiciel.

Le monde du **digital** est extrêmement **vaste** et en constante évolution. Il englobe une multitude de domaines comme les réseaux de communication, la mise en place d'infrastructures matérielles, le DevOps ou encore, le développement logiciel. En matière de développement logiciel, on peut même distinguer la programmation pour les applications web, pour les applications embarquées ou pour des applications de type client lourd.

Les **cybermenaces** peuvent se manifester à **tous les niveaux** de cet écosystème numérique. Que ce soit par des attaques visant les réseaux, des logiciels malveillants infiltrant les infrastructures ou des tentatives de phishing ciblant les utilisateurs. Les risques sont omniprésents.

Pour lutter efficacement contre ces menaces, il est nécessaire que **tous les acteurs du logiciel** sachent les reconnaître les cybermenaces et leurs impacts, comprendre comment elles fonctionnent et choisir la solution de sécurité la plus adaptée.

3.2- Les Profiles concernés par la certification

La certification « *Maîtriser les concepts de la cybersécurité* » est adaptée à plusieurs métiers du secteur de l'IT et de la cybersécurité. Voici quelques exemples de profils qui peuvent en bénéficier :

1- *Développeur logiciel / Ingénieur logiciel*

Les développeurs qui souhaitent intégrer des pratiques de cybersécurité dans le développement d'applications et de logiciels, en particulier dans la gestion des vulnérabilités et l'intégration de mesures de sécurité dans le code.

2- *Ingénieur sécurité informatique*

Les professionnels en charge de la protection des infrastructures informatiques, du réseau et des systèmes, qui doivent comprendre les menaces liées aux logiciels et aux environnements numériques pour implémenter des solutions de cybersécurité adaptées.

3- *Architecte logiciel / Architecte sécurité*

Ceux qui conçoivent des systèmes logiciels et des architectures d'infrastructure et qui doivent prendre en compte les problématiques de sécurité tout au long du cycle de vie des projets logiciels.

4- *Responsable cybersécurité (CISO)*

Les responsables de la cybersécurité dans les entreprises ou les organisations, qui doivent comprendre les risques liés aux environnements logiciels et mettre en place des politiques et des stratégies de sécurité adaptées.

5- *Analyste en cybersécurité / Consultant en cybersécurité*

Les analystes et consultants en cybersécurité, qui évaluent les risques, détectent les vulnérabilités et recommandent des solutions pour renforcer la sécurité des systèmes logiciels contre les cybermenaces.

6- *Administrateur systèmes et réseaux*

Les administrateurs responsables de la gestion des systèmes informatiques et des réseaux, qui doivent avoir une bonne compréhension de la cybersécurité afin de protéger les infrastructures contre les attaques et les menaces ciblant les applications.

7- *Consultant en transformation numérique*

Ceux qui accompagnent les entreprises dans leur transformation numérique, en veillant à ce que les nouvelles technologies et les systèmes logiciels déployés respectent les normes et principes de sécurité.

Cette certification permet à ces professionnels d'acquérir une expertise spécifique et de renforcer leur capacité à intégrer des solutions de cybersécurité efficaces dans les environnements logiciels. Elle est également idéale pour toute personne souhaitant évoluer vers des postes à responsabilité en cybersécurité ou dans les domaines techniques du développement et de la gestion des systèmes d'information.

3.3- Les compétences attestées par la certification

La certification « *Maîtriser les concepts de la cybersécurité* » permet d'attester de la maîtrise des compétences essentielles en cybersécurité. Ces compétences constituent la base pour protéger efficacement les systèmes d'information et les données sensibles. Les compétences couvertes par cette certification incluent :

1- Comprendre la cybersécurité pour renforcer la défense contre les cybermenaces en analysant son écosystème.

2- Identifier et évaluer les menaces et vulnérabilités afin de renforcer la sécurité informatique en se basant sur une analyse de risques.

3- Comprendre les réglementations et les normes en cybersécurité pour assurer la conformité du système d'information en analysant leurs exigences.

4- Sécuriser les données et les communications afin de protéger les informations en mettant en place les principaux mécanismes de protection.

5- Utiliser efficacement les outils de sécurité pour protéger les systèmes et les données en configurant, surveillant et exploitant leurs fonctionnalités.

6- Détecter et gérer les incidents de sécurité pour assurer la protection des systèmes d'information en analysant les menaces.

7- Implémenter les bonnes pratiques en cybersécurité afin d'augmenter le niveau général de la sécurité en adoptant les méthodes appropriées.

8- Réduire les risques liés à l'utilisation des outils numériques en mettant en place des politiques de sécurité.

3.4- Les prérequis demandés par la certification

La certification « *Maîtriser les concepts de la cybersécurité* **»** s'adresse aux professionnels et aux passionnés de l'informatique souhaitant développer leurs compétences en cybersécurité. Afin d'aborde cette certification dans les meilleures conditions, il est recommandé aux candidats de posséder un socle de connaissances préalables :

Avoir des bases en informatique : compréhension théorique des systèmes d'exploitation, des réseaux, des bases de données et du développement logiciel.

3.5- Modalités d'évaluation

L'évaluation de la certification se déroule entièrement **en ligne** via une plateforme dédiée. Afin de garantir l'intégrité et la fiabilité des épreuves, un système de **e-surveillance** est mis en place. Ce dispositif inclut une supervision à distance permettant de s'assurer du respect des conditions d'examen. La e-surveillance est réalisée par **GH Digital Evolution**. Afin d'évaluer le candidat, l'examen comprend plusieurs types de modalités d'évaluation :

- **Des questions à choix multiple** (QCM). Une question est posée avec plusieurs réponses possibles, dont une ou plusieurs sont correctes. Le candidat doit sélectionner la ou les bonnes réponses. Ce format permet de tester un large éventail de connaissances de manière rapide et efficace.
  - *Exemple :* Quelle norme est liée à la protection des données personnelles en Europe ?
    a) ISO 27001
    b) NIST 800-53
    c) RGPD
    d) PCI-DSS

- **Des questions à trous**. Une phrase ou un texte est présenté avec un ou plusieurs mots manquants. Le candidat doit compléter les espaces vides avec les termes appropriés. Ce type de question permet d'évaluer la précision des connaissances.
  - *Exemple :* La norme ISO 27001 concerne la gestion de la _____ de l'information.

- **Des études de cas**. Une situation réelle ou fictive est présentée, et le candidat doit analyser le problème, identifier les risques ou proposer des solutions adaptées. Ce format permet d'évaluer la capacité à appliquer les connaissances dans un contexte concret.
  - *Exemple :* Une entreprise subit une attaque par ransomware. Décrivez les étapes à suivre pour gérer cette crise et renforcer la sécurité du système d'information.

Les candidats doivent disposer d'un ordinateur avec une connexion internet stable, d'une webcam et d'un microphone pour le bon déroulement de la surveillance en ligne. Toute tentative de fraude entraînera l'annulation de l'examen. Les détails concernant l'organisation de l'examen figurent dans le document dédié à cet effet.

3.6- Validation de la certification

L'évaluation de la certification « *Maîtriser les Concepts de la CyberSécurité* » est basée sur un système de notation en pourcentage.

Pour valider la certification, le candidat doit obtenir un score minimum de **80 %** sur l'ensemble des épreuves. Cette exigence garantit que les compétences essentielles en cybersécurité sont maîtrisées.

En cas d'échec à l'examen, le candidat a la possibilité de le repasser selon les conditions suivantes :

- Le seuil de réussite est toujours à 80%.
- La seconde tentative est autorisée sans frais supplémentaires, dans un délai de **30 jours** après la première tentative.
- Si le candidat échoue une seconde fois, il devra se réinscrire à un nouveau cycle de certification.
- Lors de la seconde tentative, l'examen portera sur un nouveau jeu de questions et d'études de cas, afin de garantir une évaluation équitable et éviter toute répétition des sujets précédents.

Toute tentative de fraude ou de non-respect des règles d'examen entraînera l'annulation des résultats et pourra compromettre la possibilité de repasser la certification.

3.7- Les voies d'accès à la certification

L'obtention de la certification « *Maîtriser les concepts de la cybersécurité* » peut se faire via deux voies :

1- **Formation continue**

   Suivi d'un programme de formation dispensé par un organisme accrédité, tel que **GHDE Formation**. Acquisition progressive des compétences via des modules d'apprentissage encadrés.

2- **Candidature individuelle**

   Acquisition des compétences en autonomie à travers des ressources documentaires, des plateformes d'e-learning et des projets pratiques. Inscription directe à l'examen de certification sans obligation de suivre une formation préalable.

Quelle que soit la voie choisie, les candidats doivent répondre aux prérequis définis et réussir l'évaluation finale pour obtenir la certification.

4- Le référentiel de certification

Le référentiel de compétences de la certification « *Maîtriser les concepts de la cybersécurité* » définit les compétences, les savoirs et les savoir-faire nécessaires pour assurer la protection des systèmes et des données dans un contexte digital.

Ce référentiel est structuré en trois blocs de compétences, chacun couvrant un aspect essentiel de la cybersécurité :

- **Bloc 1 : [BC1]** – Comprendre les fondamentaux et l'écosystème de la Cybersécurité.
- **Bloc 2 : [BC2]** – Mettre en œuvre des solutions de sécurité adaptées aux menaces identifiées.
- **Bloc 3 : [BC3]** – Adopter et promouvoir les bonnes pratiques de cybersécurité.

Chaque bloc est composé de **compétences spécifiques (CS),** huit au totale qui détaillent les capacités attendues des candidats. Ces compétences sont elles-mêmes déclinées en :

- **Savoirs associés (SA)** : Connaissances théoriques fondamentales à maîtriser.
- **Savoir-faire (SF)** : Compétences techniques et opérationnelles permettant l'application des savoirs dans un contexte professionnel.

Ce référentiel a été élaboré en collaboration avec des experts du domaine et s'aligne sur les exigences du secteur de la cybersécurité afin de garantir une formation pertinente et adaptée aux enjeux actuels. Il sert de base à l'évaluation des candidats lors de l'examen de certification.

4.1- Présentation des blocs de compétences

4.1.1 Comprendre les fondamentaux et l'écosystème de la Cybersécurité

Dans un monde où les cybermenaces sont omniprésentes, la cybersécurité est devenue une priorité pour les entreprises et les organisations. Ce bloc de compétences vise à donner aux candidats une compréhension approfondie des concepts fondamentaux de la cybersécurité ainsi que de son écosystème global.

L'objectif est d'acquérir les connaissances nécessaires pour analyser les risques, identifier les menaces et comprendre l'organisation des acteurs qui participent à la protection des systèmes d'information. En maîtrisant ces notions, le candidat pourra mieux appréhender les enjeux de la cybersécurité et contribuer efficacement à la mise en place de stratégies de défense adaptées aux besoins des entreprises. En effet, ce bloc de compétences permet aux entreprises de s'assurer que leurs collaborateurs disposent des connaissances fondamentales en cybersécurité leur permettant :

- De comprendre et d'anticiper les cybermenaces
- De reconnaître et de savoir réagir face aux principales menaces
- De se conformer aux réglementations
- De développer une culture de cybersécurité

Ce bloc de compétences est adapté à tous les métiers ayant un lien de près ou de loin avec le numérique.

4.1.2 Mettre en œuvre des solutions de sécurité adaptées aux menaces identifiées

Dans un contexte où les cyberattaques sont de plus en plus sophistiquées et fréquentes, les entreprises doivent non seulement comprendre les menaces, mais aussi être en mesure de mettre en place des solutions de sécurité adaptées. L'implémentation de ces solutions est essentielle pour assurer la protection des infrastructures, des données et des utilisateurs. Ce bloc de compétences permet aux entreprises de :

- De renforcer la sécurité de leurs systèmes d'information
- D'améliorer la détection et la réponse aux incidents.
- D'optimiser la gestion des identités et des accès

En maîtrisant l'implémentation de solutions de cybersécurité adaptées, les entreprises augmentent leur résilience face aux menaces et assurent une meilleure protection de leurs actifs numériques, garantissant ainsi la continuité et la confiance de leurs clients et partenaires.

4.1.3 Adopter et promouvoir les bonnes pratiques de cybersécurité

La cybersécurité ne repose pas uniquement sur des solutions techniques. Les erreurs humaines et le manque de sensibilisation sont des facteurs majeurs de vulnérabilité. Adopter et promouvoir les bonnes pratiques en cybersécurité est essentiel pour renforcer la posture de sécurité d'une organisation et limiter les risques d'incidents. Ce bloc de compétences permet aux entreprises de :

- De renforcer la culture de la cybersécurité
- D'optimiser la veille en cybersécurité
- Instaurer un environnement de travail sécurisé
- Faciliter la mise en place d'une politique de cybersécurité efficace

L’adoption et la promotion des bonnes pratiques constituent un levier stratégique pour garantir la pérennité et la compétitivité des entreprises face aux défis du numérique.

4.2- Vue synthétique des blocs de compétences

BC1	Comprendre les fondamentaux et l'écosystème de la Cybersécurité	
↘	**CS1**	Comprendre la cybersécurité pour renforcer la défense contre les cybermenaces en analysant son écosystème
↘	**CS2**	Identifier et évaluer les menaces et vulnérabilités afin de renforcer la sécurité informatique en se basant sur une analyse de risques
↘	**CS3**	Comprendre les réglementations et les normes en cybersécurité pour assurer la conformité du système d'information en analysant leurs exigences
BC2	Mettre en œuvre des solutions de sécurité pour la protection des données	
↘	**CS4**	Sécuriser les données et les communications afin de protéger les informations en mettant en place les principaux mécanismes de protection
↘	**CS5**	Utiliser efficacement les outils de sécurité pour protéger les systèmes et les données en configurant, surveillant et exploitant leurs fonctionnalités
↘	**CS6**	Détecter et gérer les incidents de sécurité pour assurer la protection des systèmes d'information en analysant les menaces
BC3	Adopter et promouvoir les bonnes pratiques en cybersécurité	
↘	**CS7**	Implémenter les bonnes pratiques en cybersécurité afin d'augmenter le niveau général de la sécurité en adoptant les méthodes appropriées
↘	**CS8**	Réduire les risques liés à l’utilisation des outils numériques en mettant en place des politiques de sécurité

4.3- Détail du référentiel de certification

Le référentiel de compétences et d'évaluation a été combinés afin d'améliorer la lisibilité et la cohérence des informations.

Référentiel de compétences	*Suite (partie 1 / 8)*
BC1	Comprendre les fondamentaux et l'écosystème de la Cybersécurité
CS1	Comprendre les réglementations et les normes en cybersécurité pour assurer la conformité du système d'information en analysant leurs exigences

Descriptif :

Cette compétence vise à doter les professionnels des connaissances nécessaires pour comprendre les principales obligations légales et normatives en matière de cybersécurité.

Cette compétence permet ainsi aux entreprises de garantir la confidentialité, l'intégrité et la disponibilité des données tout en réduisant les risques juridiques et financiers liés à la non-conformité.

Savoirs associés	*Savoir-faire*
• Identifier les principales normes et standards liées la cybersécurité (normes ISO, NIST, CRA etc.…). • Comprendre l'organisation d'une norme.	• Savoir lire et interpréter les exigences d'une norme. • Savoir mettre en œuvre des mesures de protection des données personnelles conformément au RGPD.

Référentiel d'évaluation	
Modalités d'évaluation	*Critères d'évaluation*
ME1.1 - Evaluation théorique à travers un **QCM**. Le QCM comprend une série de questions dédiées aux concepts fondamentaux et à l'écosystème de la cybersécurité.	**CE1.1** - Chaque question du QCM est pondérée en fonction de sa complexité, et un score de **80% minimum** est requis pour valider la compétence.

Référentiel de compétences

Suite (partie 2 / 8)

BC1	Comprendre les fondamentaux et l'écosystème de la Cybersécurité
CS2	Identifier et évaluer les menaces et vulnérabilités afin de renforcer la sécurité informatique en se basant sur une analyse de risques

Descriptif :

Cette compétence permet d'acquérir les connaissances et méthodologies nécessaires pour identifier et analyser les menaces, détecter les vulnérabilités et évaluer leur impact sur un système d'information.

Grâce à cette compétence, les professionnels de l'IT seront en mesure d'adopter une approche proactive en matière de cybersécurité, en anticipant les menaces et en renforçant les dispositifs de protection pour limiter les risques d'incidents.

Savoirs associés	*Savoir-faire*
• Savoir faire la différence entre menace et vulnérabilité. • Connaître les différents types de malwares et comprendre comment ils fonctionnent. • Reconnaître les principales menaces et comprendre leur fonctionnement (malwares, ransomwares, phishing, DDoS, attaques sur les identités). • Comprendre les modèles de sécurité (Zero Trust, Défense en profondeur, Modèle CIA). • Comprendre les principales techniques de détection de vulnérabilité.	• Savoir utiliser des outils de détection de vulnérabilités / menaces, tels que les scanners de sécurité et les systèmes de détection d'intrusion. • Savoir mettre en œuvre des mesures correctives après l'identification des vulnérabilités. • Savoir réaliser une analyse de risques pour évaluer l'impact des menaces et vulnérabilités sur un système d'information. • Savoir élaborer un plan de remédiation pour corriger les vulnérabilités identifiées et renforcer la sécurité.

Référentiel d'évaluation

Modalités d'évaluation	*Critères d'évaluation*
ME2.1 - Evaluation théorique à travers un **QCM**. Le QCM comprend une série de questions dédiées au sujet des menaces et vulnérabilités. Le QCM comprend des questions de difficulté variée, couvrant aussi bien les notions générales que des cas concrets permettant d'évaluer la capacité de réflexion et d'analyse du candidat.	**CE2.1** - Chaque question du QCM est pondérée en fonction de sa complexité, et un score de **80% minimum** est requis pour valider la compétence.

Suite du référentiel d'évaluation de la compétence C1.2	
Modalités d'évaluation	*Critères d'évaluation*
ME2.2 - Evaluation à travers des **études de cas**. Divers contextes mettant en évidence une situation de vulnérabilité ou d'attaque sont présentés au candidat. Celui-ci doit identifier les risques et proposer des mesures de correction ou d'atténuation.	**CE2.2** - Compréhension de la situation et identification des risques (40% de la note). **CE2.3** - Pertinence des solutions proposées (30% de la note). **CE2.4** - Justification et argumentation (30% de la note) Le candidat doit obtenir un score minimum de **70%** à l'épreuve de l'étude de cas pour valider cette compétence.

Référentiel de compétences

Suite (partie 3 / 8)

BC1	Comprendre les fondamentaux et l'écosystème de la Cybersécurité
CS3	Comprendre les réglementations et les normes en cybersécurité pour assurer la conformité du système d'information en analysant leurs exigences

Descriptif :

Cette compétence vise à doter les professionnels des connaissances nécessaires pour comprendre les principales obligations légales et normatives en matière de cybersécurité.

Cette compétence permet ainsi aux entreprises de garantir la confidentialité, l'intégrité et la disponibilité des données tout en réduisant les risques juridiques et financiers liés à la non-conformité.

Savoirs associés	*Savoir-faire*
• Identifier les principales normes et standards liées la cybersécurité (normes ISO, NIST, CRA etc.…). • Comprendre l'organisation d'une norme.	• Savoir lire et interpréter les exigences d'une norme. • Savoir mettre en œuvre des mesures de protection des données personnelles conformément au RGPD.

Référentiel d'évaluation

Modalités d'évaluation	*Critères d'évaluation*
ME3.1 - Evaluation théorique à travers un **QCM**. Le QCM comprend une série de questions dédiées au sujet des normes et réglementations.	**CE3.1** - Chaque question du QCM est pondérée en fonction de sa complexité, et un score de **65% minimum** est requis pour valider la compétence.
ME3.2 - Évaluation à travers des **questions à trous**. Des questions sur des normes et réglementations sont posées au candidat. La réponse est partiellement fournie. Le candidat doit compléter la réponse avec les bons mots.	**CE3.2** - Chaque réponse correcte rapporte des points en fonction de sa complexité et de son importance. Un taux de réussite de **60% minimum** est requis pour valider cette compétence.
ME3.3 - Evaluation à travers des **questions ouvertes**. Des fragments d'exigences sont présentés au candidat, celui-ci doit fournir sous forme de texte sa compréhension de l'exigence.	**CE3.3** - L'interprétation de l'exigence du candidat doit être fournie et être en adéquation avec la raison d'être de l'exigence. La note est attribuée en fonction de la précision des réponses, de la capacité d'analyse et de la qualité rédactionnelle. Un taux de **60% de bonnes réponses** est requis pour valider cette compétence.

Référentiel de compétences

Suite (partie 4 / 8)

BC2	Mettre en œuvre des solutions de sécurité pour la protection des données
CS4	Sécuriser les données et les communications afin de protéger les informations en mettant en place les principaux mécanismes de protection

Descriptif :

Cette compétence vise à comprendre et appliquer les principaux mécanismes de protection, tels que le chiffrement, l'authentification sécurisée et l'utilisation de protocoles de communication sûrs.

Les professionnels doivent être en mesure d'identifier les vulnérabilités liées aux échanges d'informations, de mettre en œuvre des solutions de chiffrement robustes et d'assurer une gestion efficace des accès et des identités.

Savoirs associés	*Savoir-faire*
• Comprendre les principaux mécanismes d'authentification. • Comprendre les principes de base du chiffrement des données (AES, RSA, SSL/TLS). • Comprendre les principes de base de la signature numérique. • Identifier les protocoles de communication sécurisés.	• Savoir utiliser un outil de chiffrement. • Savoir configurer un VPN. • Savoir mettre en place un outil permettant de vérifier le correspondant lors des échanges de mails. • Savoir vérifier l'intégrité d'une donnée.

Référentiel d'évaluation

Modalités d'évaluation	*Critères d'évaluation*
ME4.1 - Evaluation théorique à travers un **QCM**. Le QCM comprend une série de questions dédiées à la sécurisation des données.	**CE4.1** - Chaque question du QCM est pondérée en fonction de sa complexité, et un score de **80% minimum** est requis pour valider la compétence.
ME4.2 - Évaluation à travers des **questions à trous** sur les notions fondamentales, les mécanismes et outils de protection et l'identification des menaces et des risques.	**CE4.2** - Chaque réponse correcte rapporte des points en fonction de sa complexité et de son importance. Un taux de réussite de **60% minimum** est requis pour valider cette compétence.

Référentiel de compétences

Suite (partie 5 / 8)

BC2	Mettre en œuvre des solutions de sécurité pour la protection des données
CS5	Utiliser efficacement les outils de sécurité pour protéger les systèmes et les données en configurant, surveillant et exploitant leurs fonctionnalités

Descriptif :

Cette compétence consiste à maîtriser l'utilisation des outils et technologies de cybersécurité afin de protéger les systèmes informatiques et les données sensibles.

En maîtrisant cette compétence, le professionnel de la sécurité informatique peut garantir une protection robuste des systèmes et des données contre les cybermenaces.

Savoirs associés	*Savoir-faire*
• Identifier les principaux organes dédiés à la sécurité.	• Savoir configurer un pare-feu. • Savoir configurer et utiliser un IDS pour surveiller les activités suspectes sur le réseau. • Savoir automatiser des sauvegardes régulières. • Savoir réduire son empreinte numérique pour limiter les risques de cybersécurité. • Savoir naviguer sur internet de façon anonyme en utilisant le réseau TOR, les VPN ou des extensions de confidentialité.

Référentiel d'évaluation

Modalités d'évaluation	*Critères d'évaluation*
ME5.1 - Evaluation théorique à travers un **QCM**. Le QCM comprend une série de questions dédiées aux outils de sécurité.	**CE5.1** - Chaque question du QCM est pondérée en fonction de sa complexité, et un score de **80% minimum** est requis pour valider la compétence.
ME5.1 - Evaluation à travers des **études de cas**. Divers contextes mettant en évidence une situation où le candidat doit fournir son analyse pour améliorer la protection des données et des systèmes.	**CE5.1** - Compréhension de la situation et identification des risques (40% de la note). **CE5.2** - Pertinence des solutions proposées (30% de la note). **CE5.3** - Justification et argumentation (30% de la note) Le candidat doit obtenir un score minimum de **70%** à l'épreuve de l'étude de cas pour valider cette compétence.

Référentiel de compétences

Suite (partie 6 / 8)

BC2	Mettre en œuvre des solutions de sécurité pour la protection des données
CS6	Détecter et gérer les incidents de sécurité pour assurer la protection des systèmes d'information en analysant les menaces

Descriptif :

L'objectif de cette compétence est de garantir la sécurité et l'intégrité des systèmes d'information en détectant et en gérant efficacement les incidents de sécurité.

En maîtrisant cette compétence, le professionnel de la sécurité informatique peut assurer une protection robuste des systèmes d'information contre les cybermenaces et garantir la continuité des opérations.

Savoirs associés	*Savoir-faire*
• Reconnaître les signes d'un incident de cybersécurité (activité suspecte, fuite de données, ransomware). • Identifier les éléments permettant de détecter des comportements suspects. • Comprendre les actions à entreprendre en cas de compromission d'un compte ou d'un appareil. • Comprendre les bases de la gestion d'un incident de sécurité et l'importance du signalement. • Comprendre les concepts d'une analyse forensique.	• Savoir analyser les journaux de sécurité pour détecter des comportements anormaux • Savoir organiser des exercices de simulation d'incidents pour préparer les équipes à réagir efficacement.

Référentiel d'évaluation

Modalités d'évaluation	*Critères d'évaluation*
ME6.1 - Evaluation théorique à travers un **QCM**. Le QCM comprend une série de questions dédiées à la gestion des incidents.	**CE6.1** - Chaque question du QCM est pondérée en fonction de sa complexité, et un score de **80% minimum** est requis pour valider la compétence.
ME6.2 - Évaluation à travers de **questions à trous** sur la gestion des incidents.	**CE6.2** - Chaque réponse correcte rapporte des points en fonction de sa complexité et de son importance. Un taux de réussite de **60% minimum** est requis pour valider cette compétence.

Référentiel de compétences

Suite (partie 7 / 8)

BC3	Adopter et promouvoir les bonnes pratiques en cybersécurité
CS7	Implémenter les bonnes pratiques en cybersécurité afin d'augmenter le niveau général de la sécurité en adoptant les méthodes appropriées

Descriptif :

L'objectif de cette compétence est de garantir la protection des systèmes d'information et des données sensibles en adoptant des méthodes de cybersécurité éprouvées et efficaces.

En maîtrisant cette compétence, le professionnel de la cybersécurité peut augmenter le niveau général de sécurité de l'organisation et protéger efficacement les systèmes d'information contre les cybermenaces.

Savoirs associés	*Savoir-faire*
• Comprendre l'importance des mises à jour. • Comprendre l'importance d'une bonne gestion de mot de passe. • Comprendre le mécanisme de veille informationnelle. • Comprendre l'importance de la sensibilisation.	• Savoir mettre en place une gestion des accès et des identités (IAM, RBAC ect.).

Référentiel d'évaluation

Modalités d'évaluation	*Critères d'évaluation*
ME7.1 - Evaluation théorique à travers un **QCM**. Le QCM comprend une série de questions dédiées à l'implémentation des bonnes pratiques	**CE7.1** - Chaque question du QCM est pondérée en fonction de sa complexité, et un score de **80% minimum** est requis pour valider la compétence.
ME7.2 - Évaluation à travers des **questions à trous** sur les bonnes pratiques en matière de sécurité.	**CE7.2** - Chaque réponse correcte rapporte des points en fonction de sa complexité et de son importance. Un taux de réussite de **60% minimum** est requis pour valider cette compétence.

Référentiel de compétences

Suite (partie 8 / 8)

BC3	Adopter et promouvoir les bonnes pratiques en cybersécurité
CS8	Réduire les risques liés à l'utilisation des outils numériques en mettant en place des politiques de sécurité

Descriptif :

L'objectif de cette compétence est de minimiser les risques associés à l'utilisation des outils numériques en adoptant des politiques de sécurité robustes et efficaces.

En maîtrisant cette compétence, le professionnel de la sécurité informatique peut réduire significativement les risques liés à l'utilisation des outils numériques et garantir la protection des systèmes et des données sensibles.

Savoirs associés	*Savoir-faire*
• Comprendre l'importance des politiques de sécurité.	• Savoir mettre en œuvre une politique de mot de passe robuste. • Savoir organiser des sessions de sensibilisation au bon format. • Savoir rédiger et mettre en œuvre des politiques de sécurité pour protéger les informations et les systèmes.

Référentiel d'évaluation

Modalités d'évaluation	*Critères d'évaluation*
ME8.1 - Evaluation théorique à travers un **QCM**. Le QCM comprend une série de questions dédiées aux politiques de sécurité.	**CE8.1** - Chaque question du QCM est pondérée en fonction de sa complexité, et un score de **80% minimum** est requis pour valider la compétence.
ME8.2 - Évaluation à travers des **questions à trous** sur les politiques de sécurité.	**CE8.2** - Chaque réponse correcte rapporte des points en fonction de sa complexité et de son importance. Un taux de réussite de **60% minimum** est requis pour valider cette compétence.

5- Liste des sigles

Sigle	Signification
GHDE	**GH Digital Evolution**
GHDEF	**GHDE F**ormation
QCM	**Q**uestionnaire à **C**hoix **M**ultiple
MCCS	**M**aîtriser les **C**oncepts de la **C**yber**S**écurité
BC	**B**loc de **C**ompétences
CS	**C**ompétence **S**pécifique
SA	**S**avoir **A**ssocier
SF	**S**avoir-**F**aire
ME	**M**odalité d'**E**valuation
CE	**C**ritère d'**E**valuation