



FICHES MÉTIERS

Responsable des systèmes d'information et de la cybersécurité

BRANCHE DES COMMERCES DE GROS

IDCC 0573



Administration - Informatique & numérique

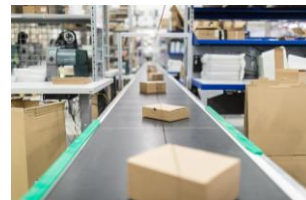


Métier émergent

Cette fiche métier présente un large éventail des missions susceptibles d'être exercées par le titulaire du poste, ainsi que les compétences associées dans les entreprises des commerces de gros (CCN 3044). Elle est réservée à un usage d'information sur le métier et ne peut en aucun cas être utilisée comme fiche emploi repère dans le cadre de la classification de la branche.

Édition
2025

 **BSERVATOIRE
AKTO**



Informations générales

Finalité du métier :

Le / la responsable des systèmes d'information et de la cybersécurité est chargé(e) de :

- Gérer ou superviser le parc informatique, matériel et logiciel de l'établissement
- Sécuriser les systèmes d'information et les données de l'établissement ; anticiper les menaces cyber et prévoir et assurer le plan de continuité d'activité
- Sensibiliser et former les équipes aux risques cyber et aux bonnes pratiques
- Conseiller la direction en matière d'investissement, de choix technologiques, de pratiques liées au respect de l'environnement
- Piloter / coordonner les projets numériques et leur déploiement fonctionnel et opérationnel

Dans le cas de service systèmes d'information constitué de plusieurs salariés, il / elle encadre et manage les membres de l'équipe (techniciens) et leur délègue une partie des activités (interventions techniques, suivi de contrats / prestataires...) tout en gardant une vue et un pilotage d'ensemble.



Branche :

Commerces de gros



Domaine professionnel :

Administration – Informatique & numérique



Autres appellations :

- Responsable informatique
- Responsable systèmes et réseau
- Administrateur(trice) systèmes et réseau
- Directeur(trice) des systèmes d'information



Correspondance ROME :

- M1812 – Responsable de la sécurité des systèmes d'information (RSSI)

Relation(s) hiérarchique(s)

Il / elle intervient sous la responsabilité du Chef d'établissement, Directeur Général, Directeur Financier, Directeur des Opérations, ou DSI Groupe (pour les filiales).

Activités

- Gérer, administrer, maintenir et sécuriser les systèmes d'information
- Concevoir des projets IT, en lien étroit avec les enjeux métiers et la stratégie de l'entreprise et en assurer le déploiement fonctionnel et opérationnel
- Communiquer et sensibiliser les utilisateurs aux bonnes pratiques
- Encadrer et manager une équipe (le cas échéant)

Compétences associées aux activités

Gérer, administrer, maintenir et sécuriser les systèmes d'information

- Paramétrer le réseau numérique selon les procédures en vigueur au sein de l'entreprise
- Créer des procédures, guides d'utilisation et tutoriels afin de favoriser l'autonomie des utilisateurs dans l'usage quotidien des matériels, équipements informatiques et services numériques et la résolution de problèmes
- Gérer les habilitations des utilisateurs selon les procédures établies
- Mettre en place des politiques de sauvegarde et de récupération des données
- Renforcer la conformité avec les réglementations cybersécurité (ISO 27001, NIS2...)
- Élaborer le plan de continuité d'activité afin de prévenir les cas d'attaque et/ou d'incident informatique
- Assurer le maintien en conditions opérationnelles des infrastructures, de la sécurité et des applications
- Sélectionner les prestataires et les offres selon les critères d'attentes et de contraintes définis au sein de l'entreprise
- Suivre / piloter et contrôler la réalisation des prestations prévues par les contrats

Concevoir des projets IT, en lien étroit avec les enjeux métiers et la stratégie de l'entreprise et en assurer le déploiement fonctionnel et opérationnel

- Recueillir les besoins des différents utilisateurs en matériels, logiciels et services numériques de l'entreprise en sondant régulièrement les utilisateurs et en étant à l'écoute
- Réaliser une veille technologique pour proposer des solutions numériques et préconisations d'investissement adaptées aux différents services de l'entreprise
- Définir, avec la direction, les orientations stratégiques en matière informatique et numérique
- Elaborer des outils métiers
- Piloter le déploiement de nouvelles solutions, projets ou outils numérique en lien avec la stratégie de l'entreprise
- Assurer le pilotage d'un ou plusieurs projets numériques (coût, délai, qualité et risques)

Communiquer et sensibiliser les utilisateurs aux bonnes pratiques

- Participer à la définition des messages et des moyens de sensibilisation des utilisateurs à la sécurité numérique, au respect des obligations RGPD, au droit à la déconnexion, à la sobriété numérique...
- Former les collaborateurs aux risques cyber et aux attaques types (hameçonnage, malware, etc.)
- Mettre en place une charte de cybersécurité et veiller à sa mise en application

Encadrer et manager une équipe (le cas échéant)

- Participer au recrutement des membres de l'équipe
- Organiser au quotidien le suivi des plannings en identifiant les moyens matériels nécessaires à l'organisation, la planification et le suivi de l'activité
- Identifier et formaliser les besoins en compétences au sein de l'équipe en menant des entretiens avec les équipes opérationnelles
- Mettre en place un management collaboratif et participatif en utilisant les outils numériques adéquats et différentes techniques d'animation de l'équipe afin de favoriser le partage d'information



Prérequis

- Métier accessible avec un diplôme de niveau Bac+2 (BTS) voire Bac +3 (BUT, Licence pro) en informatique
- La pratique de l'anglais (vocabulaire technique) peut être requise.

Voies d'accès au métier par la certification

- Exemples de certifications d'accès au métier appréciées par les entreprises :
 - BTS Services informatiques aux organisations option A solutions d'infrastructure, systèmes et réseaux (niveau 5)
 - BTS cybersécurité, informatique et réseaux, électronique option B électronique et réseaux (niveau 5)
 - Licence pro mention métiers de l'informatique : administration et sécurité des systèmes et des réseaux (niveau 6)
 - Licence pro mention métiers des réseaux informatiques et télécommunications (niveau 6)
 - BUT informatique parcours intégration d'applications et management du système d'information (niveau 6)
 - BUT réseaux et télécommunications parcours cybersécurité (niveau 6)
 - BUT réseaux et télécommunications parcours pilotage de projets de réseaux (niveau 6)

Domaines de compétences

Savoirs / Connaissances

- Systèmes d'information
- Langages informatiques, systèmes d'exploitation (Windows, Linux...)
- Réseaux informatiques (LAN, WAN, WLAN) et gestion des infrastructures serveurs (virtualisation, sauvegarde...)
- Sécurité des infrastructures réseaux et Cloud (VPN, firewall...)
- Principales normes et principes de sécurité informatique, RGPD et de cybersécurité
- Bases en contrôle de gestion (pour pilotage de budget informatique et dialogue avec la direction administrative et financière)
- Anglais technique
- Enjeux et principes de la sobriété numérique
- Labels numériques responsables, indicateurs
- Risques et enjeux éthiques de l'intelligence artificielle (moyen-long termes)
- Connaissance du marché des prestataires (cabinets de conseils, éditeurs)
- Notions en droit (RGPD, droit de l'Internet...)

Savoir-faire / Compétences opérationnelles

- Assurer la gestion des logiciels, du matériel et des services numériques en coordination avec les prestataires et éditeurs de logiciels
- Administrer un système d'information, travailler sur différents environnements numériques
- Analyser les usages, l'expérience utilisateur
- Déployer, intégrer un logiciel, un système d'information, une application
- Sensibiliser un public
- Concevoir des outils et supports de communication, définir des règles et procédures-utilisateurs
- Accompagner le changement
- Réaliser une veille technique ou technologique pour anticiper les évolutions
- Négocier, rédiger des contrats
- Manager une équipe
- Transmettre des bonnes pratiques et développer des compétences
- Gérer l'hébergement et le nom de domaine d'un site internet
- Savoir proposer une stratégie numérique responsable et identifier les leviers d'actions
- Maîtriser les outils d'intelligence artificielle (moyen-long termes)
- Détecter et analyser les menaces à l'aide d'outils cyber et assurer la continuité d'activité
- Mettre en œuvre des politiques de sécurité et de gestion des risques cyber
- Réagir efficacement en cas d'incident cyber et assurer la continuité d'activité
- Interagir avec les utilisateurs

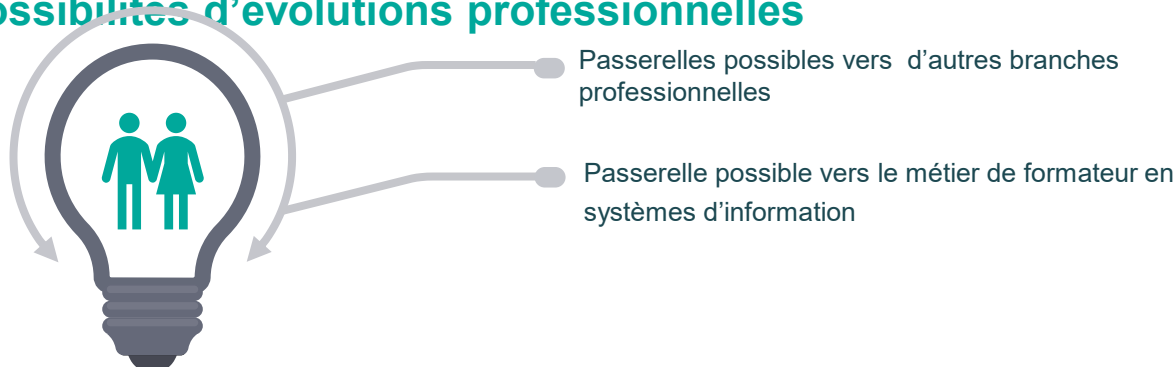
Savoir-être / Compétences comportementales

- Sens de l'écoute dans les rapports hiérarchiques et fonctionnels
- Prise d'initiatives et force de proposition
- Travail en équipe, capacité de s'interfacer avec des experts externes et les services internes (métiers)
- Réactif
- Gestion des situations d'urgence (en particulier en cas de cyberattaque)
- Sens du service
- Bonne expression écrite et orale
- Pédagogue (y compris face aux cyber-risques et pour la sobriété numérique)
- Ténacité
- Vision stratégique

Conditions d'exercice du métier

- Le métier s'exerce majoritairement sur site, ou à distance.
- Possibilité de réaliser ponctuellement des déplacements extérieurs en fonction des pratiques et des besoins (par exemple pour participer à des salons sur les sujets informatiques et réseaux, participer à des groupes de travail, etc.)
- Possibilité de réaliser des astreintes
- Interactions quotidiennes avec des acteurs internes à l'établissement (utilisateurs, Directeur(trice) général(e) dont lors de CODIR, services de l'administration, commercialisation et exploitation) et externes (prestataires)

Possibilités d'évolutions professionnelles



Évolutions prospectives

Chiffres clés

Salariés en 2023



~ 4 160

Part des salariées
femmes en 2023



17%

Evolution du métier



Métier émergent



Moins de 20 ans : 0,1%

60 ans et plus : 3,2%

Données Insee - Base Tous Salariés 2023 - PCS 388 A B C

Principaux facteurs d'évolution et impacts sur les métiers



TRANSITION ECOLOGIQUE

- Optimisation de la gestion des équipements informatiques pour prolonger leur durée de vie et réduire l'empreinte carbone.
- Sensibilisation aux bonnes pratiques de sobriété numérique et aux impacts environnementaux des infrastructures IT.
- Engagement à minimiser l'impact de la logistique informatique et mise en place de stratégies de nettoyage des données pour limiter la consommation énergétique des serveurs.



TRANSITION NUMÉRIQUE

- Adaptation du métier et des compétences aux évolutions rapides des systèmes d'information et des technologies numériques : IA, Cloud, logiciels métiers...
- Maîtrise accrue des matériels et équipements connectés (en lien avec l'automatisation dans les stocks...) avec le développement de la domotique et des solutions IoT.
- Développement de compétences pour pallier la croissance du danger des cyberattaques et renforcer la sécurité des infrastructures.
- Mise en œuvre du RGPD pour garantir la conformité des systèmes et la protection des données.



TRANSITION ÉCONOMIQUE

- Enjeu financier majeur de se prémunir contre les cyberattaques et de disposer d'équipements numériques performants pour répondre à la concurrence croissante.



TRANSITION SOCIALE

- Développement des compétences pédagogiques et d'accompagnement pour faciliter l'appropriation des outils numériques par les utilisateurs.
- Collaboration renforcée avec les équipes métiers pour adapter les solutions informatiques aux besoins opérationnels.