RIASEC : C

M1817
ADMINISTRATEUR / ADMINISTRATRICE SÉCURITÉ INFORMATIQUE

Emploi cadre

Transition numérique

Définition

L' Administrateur(rice) sécurité informatique assure la protection des données et des systèmes d'information de l'entreprise.

- Met en place des politiques de sécurité informatique pour protéger les données et les systèmes
- Surveille et évalue les menaces potentielles pour la sécurité informatique
- Gère les incidents de sécurité et coordonne les réponses appropriées
- Réalise des audits de sécurité pour identifier les vulnérabilités
- Forme le personnel aux bonnes pratiques de sécurité informatique
- Maintient à jour les logiciels de sécurité et les systèmes de protection des données

Accès à l'emploi

Ce métier est accessible avec un niveau Bac + 5 Master en Sécurité informatique, une Certification Professionnelle en cybersécurité ou Diplôme d'Ingénieur en informatique.

Certifications et diplômes :

- Titre d'ingénieur diplômé par l'Etat spécialité informatique
- Certificat de compétence analyste en cybersécurité
- Certificat professionnel technicien de maintenance micro réseaux et internet spécialisation cybersécurité des PME
- Mastère spécialisé cybersécurité
- Mastère spécialisé cybersécurité et cyberdéfense
- Mastère spécialisé sécurité informatique

Compétences

Savoir-faire

Savoir-faire principaux

Production, Construction, Qualité, Logistique

- Concevoir et maintenir un système de cybersécurité — Transition numérique
- Analyser les risques et les dysfonctionnements, les marges d'amélioration des systèmes de sécurité
- Piloter la gestion des risques

Communication, Création, Innovation, Nouvelles technologies

- Administrer un système d'informations — Transition numérique
- Analyser les performances d'un système d'information — Transition numérique

Coopération, Organisation et Développement de ses compétences

- Documenter les procédures de sécurité, ainsi que les incidents

Pilotage, Gestion, Cadre réglementaire

- Veiller au respect des normes de sécurité

Management, Social, Soin

- Former les utilisateurs aux bonnes pratiques de sécurité informatique — Transition numérique

Savoir-faire secondaires

Production, Construction, Qualité, Logistique

- Elaborer et suivre des tableaux de bord des incidents sécurité
- Evaluer, prévenir, et gérer les risques et la sécurité
- Surveiller les tentatives d'accès non autorisées et les alertes de sécurité
- Collaborer avec les équipes techniques pour améliorer la sécurité
- Configurer des pare-feu et des systèmes de détection d'intrusions — Transition numérique
- Définir des procédures de traitement et de sécurisation

© Copyright octobre 2026 France Travail - Reproduction et diffusion interdites sans l'accord de France Travail

Communication, Création, Innovation, Nouvelles technologies

- Gérer la sécurité informatique — Transition numérique
- Gérer les droits d'accès des utilisateurs — Transition numérique
- Réaliser une veille technique ou technologique pour anticiper les évolutions — Transition numérique

Coopération, Organisation et Développement de ses compétences

- Structurer, synthétiser des informations
- Argumenter en faveur de l'adoption de nouvelles technologies de sécurité — Transition numérique
- Communiquer auprès de ses interlocuteurs internes et externes
- Communiquer efficacement les mises à jour de sécurité aux équipes concernées

Pilotage, Gestion, Cadre réglementaire

- Construire un plan de récupération après sinistre pour les serveurs — Transition numérique

Savoir-être professionnels

- Faire preuve de rigueur et de précision
- Organiser son travail selon les priorités et les objectifs
- Etre force de proposition
- Avoir l'esprit d'équipe

Savoirs

Domaines d'expertise

- Analyse de risque
- Audit de sécurité informatique — Transition numérique
- Cryptographie — Transition numérique
- Développement sécurisé de logiciels — Transition numérique
- Formation en sécurité informatique — Transition numérique
- Gestion des comptes utilisateurs — Transition numérique
- Infogérance / télémaintenance
- Logiciels d'interface (middleware) — Transition numérique
- Systèmes de gestion de base de données
- Sécurité des applications web — Transition numérique
- Sécurité des applications et des communications mobiles — Transition numérique
- Sécurité des réseaux — Transition numérique
- Système d'exploitation informatique Android — Transition numérique
- Système d'exploitation informatique VMWare (virtualisation d'architecture) — Transition numérique
- Système d'exploitation Linux — Transition numérique
- Système d'exploitation MacOS — Transition numérique
- Système d'exploitation Solaris — Transition numérique

© Copyright octobre 2026 France Travail - Reproduction et diffusion interdites sans l'accord de France Travail

- Système d'exploitation Unix — Transition numérique
- Système d'exploitation Windows — Transition numérique
- Sécurité des systèmes embarqués — Transition numérique

Normes et procédés

- Normes de sécurité
- Normes qualité
- Intégration de systèmes — Transition numérique
- Protection des données numériques — Transition numérique
- Règlement Général européen sur la Protection des Données (RGPD) — Transition numérique
- Règles d'installations informatiques
- Règles de sécurité Informatique et Télécoms — Transition numérique
- Règles de traitement des opérations bancaires
- Surveillance des systèmes de sécurité (pare-feu, VPN, systèmes de détection d'intrusion) — Transition numérique

Contextes de travail

Conditions de travail et risques professionnels

- En bureau d'études
- Travail en mode projet

Horaires et durée du travail

- Travail en journée

Publics spécifiques

- Clientèle d'affaires
- Clientèle d'entreprises

Statut d'emploi

- Salarié secteur privé (CDI, CDD)

Secteurs d'activité

- Informatique et télécommunication

© Copyright octobre 2026 France Travail - Reproduction et diffusion interdites sans l'accord de France Travail