

Administrateur systèmes, réseaux et cybersécurité

RNCP42837 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326, 326n, 326r
Formacode(s)	24210, 24273, 31009, 31008, 31034
Code(s) ROME	M1801, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	30/09/2026
Date d'échéance	30/09/2031

Certificateur(s)

CESI · SIRET : 77572257201109

<http://www.cesi.fr>

Partenaires habilités

55 organismes habilités, d'après la liste publiée par France compétences : 55 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
C E SI	77572257200366	Former et organiser l'évaluation
C E SI	77572257200820	Former et organiser l'évaluation
C E SI	77572257200846	Former et organiser l'évaluation
C E SI	77572257200911	Former et organiser l'évaluation
C E SI	77572257200929	Former et organiser l'évaluation
C E SI	77572257200960	Former et organiser l'évaluation
C E SI	77572257200978	Former et organiser l'évaluation
C E SI	77572257201018	Former et organiser l'évaluation
C E SI	77572257201034	Former et organiser l'évaluation
C E SI	77572257201042	Former et organiser l'évaluation

Liste complète des 55 partenaires habilités : <https://data.aktaconseil.fr/certifications/rncp42837-administrateur-systemes-reseaux-et-cybersecurite/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'Administrateur systèmes, réseaux et cybersécurité occupe un rôle stratégique dans les organisations, qu'il intervienne au sein d'un service informatique interne ou en tant que prestataire. Il est en charge de la conception, du déploiement, de l'administration et de la sécurisation des infrastructures systèmes et réseaux de l'entreprise. Il met en œuvre des environnements numériques intégrant serveurs, réseaux, services cloud, solutions collaboratives et équipements mobiles. Il veille à leur interopérabilité, à leur performance et à leur disponibilité. Il supervise les infrastructures, analyse les incidents, met en œuvre les actions correctives et préventives, et garantit la continuité de

service. L'Administrateur systèmes, réseaux et cybersécurité applique les politiques de cybersécurité fixées par sa direction et protège les systèmes et les données contre les menaces numériques. Il sensibilise les utilisateurs aux bonnes pratiques de sécurité et leur apporte des conseils et un support technique sur l'utilisation des outils. Il accompagne également sa direction sur les projets d'évolution du système d'information, grâce à une veille technologique permanente, à une analyse des innovations et des offres des fournisseurs. Il intègre pleinement une démarche de numérique responsable en préconisant des solutions durables, en optimisant les ressources tout en tenant compte du cycle de vie des équipements, de leur acquisition à leur recyclage.

ACTIVITÉS VISÉES

Concevoir le plan de déploiement des infrastructures systèmes
Administrer des infrastructures systèmes complexes
Administrer des infrastructures Cloud
Administrer des infrastructures de virtualisation
Concevoir le plan de déploiement des infrastructures réseaux
Administrer des infrastructures réseaux
Sécuriser des infrastructures réseaux
Assurer la maintenance en condition opérationnelle des infrastructures informatiques
Garantir la continuité de service du système d'information
Contribuer au Plan de Continuité d'Activité (PCA) et au Plan de Reprise d'Activité (PRA)
Auditer la sécurité des infrastructures informatiques
Sécuriser l'accès aux infrastructures informatiques
Réagir à une faille de sécurité

COMPÉTENCES ATTESTÉES

Analyser le système d'information à partir de la documentation existante (inventaire, plan d'assurance qualité, PCA/PRA, etc.) pour identifier les matériels et logiciels à conserver, à améliorer (upgrader) ou à remplacer
Concevoir le POC (Proof Of Concept) en intégrant les besoins techniques et fonctionnels identifiés à partir des exigences du client interne ou externe et en mobilisant des outils de virtualisation du système pour confirmer les hypothèses et établir le plan de déploiement de l'infrastructure système
Concevoir le plan de déploiement de l'infrastructure système dans le respect des réglementations et normes en vigueur (RGPD, NIS2, etc.) ou d'usage (DORA, HDS, etc.) et en mobilisant une méthode de planification de projet (WBS par ex) pour préparer le déploiement
Planifier le déploiement de l'infrastructure système en communiquant auprès de tous les acteurs impactés pour garantir sa mise en place
Configurer les systèmes d'exploitation de l'infrastructure système (Microsoft Windows, Linux, etc.) pour garantir l'interopérabilité des environnements et la continuité de service en installant les rôles et fonctionnalités (annuaire, stockage, authentification, DNS, etc.)
Concevoir un script en mobilisant des outils de scripting et/ou d'orchestration (PowerShell, Ansible, Terraform, etc.) pour automatiser les tâches d'administration de l'infrastructure système (massification et traçabilité des actions, détection de dysfonctionnements)
Configurer l'infrastructure système, dans le respect des préconisations de l'ANSSI en utilisant les outils de la sécurisation du SI 'by design' (renforcement de la sécurité du SI (Hardening), gestion des accès, journalisation, segmentation, cloisonnement, etc.), pour garantir son intégrité
Proposer l'évolution de la politique de sécurité Cloud (dont le contrôle des identités, la gestion des accès, la segmentation et/ou cloisonnement du réseau, le chiffrement des données, etc.), dans le respect de la réglementation en vigueur (RGPD, NIS2, préconisations ANSSI, etc.) pour la soumettre et l'intégrer à la PSSI de l'entreprise
Administrer les ressources Cloud (SaaS, IaaS et/ou PaaS) dans des environnements publics, privés ou hybrides, pour garantir l'interopérabilité et donc un niveau de services conforme aux attentes des utilisateurs
Configurer les services Cloud (AWS, Azure, GCP, etc.) pour garantir l'interopérabilité du SI local (on-premise) et donc un niveau de services conforme aux attentes des utilisateurs (annuaire, authentification, stockage, etc.)
Proposer l'évolution de la politique de sécurisation de l'infrastructure de virtualisation (dont le contrôle des identités, la gestion des accès, la segmentation et/ou cloisonnement du réseau, le chiffrement des données, journalisation, mécanisme de sauvegarde des VM, etc.), dans le respect de la réglementation en vigueur (RGPD, NIS2, préconisations ANSSI, etc.) pour la soumettre et l'intégrer à la PSSI de l'entreprise
Configurer des infrastructures virtualisées au sein du SI local (on-premise) ou en hybride pour garantir l'interopérabilité des différents services (accès aux données, répliquions du système, etc.) et donc un niveau de

services conforme aux attentes des utilisateurs

Déployer un cluster de serveurs de virtualisation en activant les fonctionnalités de haute disponibilité, d'équilibrage de charge, de partage de stockage, et de cliché instantané pour assurer la continuité de l'activité dans l'entreprise

Analyser le système d'information à partir de la documentation existante (inventaire, plan d'assurance qualité, PCA/PRA, etc.) pour identifier les composants du réseau à conserver, à améliorer (upgrader) ou à remplacer

Concevoir le POC (Proof Of Concept) en intégrant les besoins techniques et fonctionnels identifiés à partir des exigences du client interne ou externe et en mobilisant des outils de virtualisation du réseau pour confirmer les hypothèses et établir le plan de déploiement de l'infrastructure réseaux

Concevoir le plan de déploiement de l'infrastructure réseaux dans le respect des réglementations et normes en vigueur (RGPD, NIS2, etc.) en mobilisant une méthode de planification de projet (WBS par ex) pour préparer le déploiement

Planifier le déploiement de l'infrastructure réseaux en communiquant auprès de tous les acteurs impactés pour garantir sa mise en place

Concevoir l'infrastructure intégrant les architectures convergentes entre le réseau local - LAN (dont le réseau virtuel) et le réseau étendu - WAN pour garantir l'interopérabilité des réseaux dans le respect des différentes normes et protocoles (VLAN, routage inter-VLAN, WLAN, STP, DNA, HSRP, BGP, EIGRP, SNMP, etc.) et donc un niveau de services conforme aux attentes des utilisateurs

Concevoir un script en mobilisant des outils de scripting et/ou d'orchestration (Python, etc.) pour automatiser les tâches d'administration de l'infrastructure réseau (massification et traçabilité des actions, détection de dysfonctionnements, SysOps)

Collecter automatiquement et régulièrement les logs sur les équipements du réseau, en s'assurant de leur intégrité, pour les archiver dans un point central identifié sur le réseau conformément à la PSSI et les exploiter au besoin (diagnostic de panne, de cyberattaque, etc.)

Configurer les équipements de protection du réseau (Firewall Next Gen, Appliance, etc.) en intégrant des règles de filtrage, le contrôle d'accès, l'authentification multi facteurs, etc. dans le respect des préconisations de l'ANSSI pour limiter les expositions aux risques cyber ou de sécurité

Assurer une veille technologique et cyber, sous couvert du RSSI, pour garantir la mise à jour des équipements de protection du réseau du point de vue du système d'exploitation (IOS, Firmware, etc.) et ainsi protéger l'entreprise de nouvelles failles de sécurité

Concevoir les interconnexions multisites (MPLS, SDWAN, Hub and Spoke, etc.) pour autoriser, selon les conditions, les accès aux ressources de l'entreprise

Configurer les solutions de connexion sécurisées à distance (VPN SSL ou VPN IPSec) pour autoriser, selon les conditions, les accès aux ressources de l'entreprise

Proposer l'évolution de la PSSI de l'entreprise, dans le respect des réglementations en vigueur et selon les préconisations de l'ANSSI, en intégrant la gestion des configurations pour la partager avec les membres de la DSI et l'associer au PCA/PRA

Adapter le plan de maintenance des infrastructures du SI en prévoyant les mises à jour, les pannes (matérielles et/ou logicielles) et les défaillances, leur mode de résolution associé (systématique, conditionnel et prédictif) et la fréquence d'intervention pour garantir le maintien en condition opérationnelle (MCO) de l'infrastructure

Déployer le plan de maintenance des infrastructures du SI en considérant sa disponibilité et celles des mises à jour, et en gérant les aléas, pour garantir le MCO du SI et son intégrité

Documenter les actions réalisées dans le cadre du plan de maintenance des infrastructures du SI pour assurer une traçabilité et un archivage des configurations (versioning) accessible à l'ensemble de l'équipe technique

Dimensionner les SLA (Service Level Agreement), MTTR (Mean Time To Repair) et MTBF (Mean Time Between Failure) pour configurer les solutions dans le respect d'ITIL permettant d'assurer une disponibilité (GTR et GTI) conforme aux exigences du métier

Déterminer les seuils d'alertes des dysfonctionnements des matériels et logiciels en fonction de leurs criticités pour concevoir une supervision proactive de l'ensemble du SI et réagir en traitant l'incident ou le sinistre

Définir les indicateurs (réserve, charge, etc.) pour piloter la disponibilité et le niveau de performance de l'ensemble du SI en rendant leur évolution accessible à toutes les parties prenantes

Proposer des améliorations à partir de l'exploitation et de l'analyse des données (indicateurs, incidents, sinistres et leurs traitements, etc.) pour garantir la continuité de service et l'efficacité de l'ensemble du SI

Déployer des solutions combinées de sauvegarde (granulaire, glacier, snapshot, méthode 3-2-1, etc.) et de réplication pour répondre aux besoins métier et garantir la reprise partielle ou complète d'un SI intègre

Elaborer le plan de sauvegarde en tenant compte des RPO (Recovery Point Objective) et RTO (Recovery Time

Objective) définis dans la PSSI de l'entreprise pour assurer l'efficacité de la sauvegarde et la cohérence entre les sauvegardes et la restauration

Réviser les procédures des PCA et PRA, dans le respect des exigences réglementaires et normatives et des bonnes pratiques de l'ANSSI, pour capitaliser (suite à sinistre ou tests), les maintenir à jour (suite à évolution matérielle) et pour les partager avec l'ensemble de l'équipe technique

Assurer une veille des risques cyber pour identifier les vulnérabilités, les failles et des solutions innovantes de sécurisation et à terme pour évaluer le niveau de maturité de l'infrastructure, en s'appuyant sur les normes et réglementations en vigueur, sur les bonnes pratiques (ISO 27001, RGS, NIST, ANSSI, etc.) et les partages au sein de communautés d'experts

Réaliser un audit (conformité et sécurité) de l'infrastructure en mobilisant des outils d'intrusion et/ou de scans automatisés pour établir un état des lieux (scoring) de l'infrastructure et proposer la mise à jour du plan de remédiation au RSSI

Appliquer la gestion des identités, des accès (IAM) et des privilèges (PAM) et l'authentification forte (MFA, certificats, bastion d'administration), issues de la PSSI de l'entreprise, dans le respect des bonnes pratiques de l'ANSSI (charte de l'administrateur par exemple) pour garantir la traçabilité d'accès aux données et l'administration de l'infrastructure du SI

Configurer les firewalls (de type NextGen par exemple) dans le respect de la réglementation en vigueur (NIS2, RGPD, DORA, etc.), des bonnes pratiques de l'ANSSI (préconisations Zéro Trust Network Access, etc.) et des règles de détection et de protection (IDS, IPS, etc.) définies dans la PSSI de l'entreprise pour sécuriser les accès distants (VPN, MPLS, SD Wan)

Auditer la traçabilité des connexions en centralisant, à l'aide d'un outil de type SIEM, l'ensemble des logs de tous les équipements pour surveiller le SI et identifier les failles et/ou vulnérabilités

Qualifier l'incident de sécurité détecté par les outils et services intégrés au SI (SIEM, supervision, journalisation, SOC, etc.) pour alerter sa hiérarchie et réagir en temps réel

Déployer des contre-mesures en réponse à une alerte de sécurité pour contrôler l'intrusion et préserver l'intégrité des données du SI et l'activité de l'entreprise tout en rendant compte à la hiérarchie

Collecter des éléments de preuve par une méthode d'investigation numérique (démarche forensique par exemple) pour qu'ils soient exploitables par les autorités et/ou les assurances cyber

Simuler une attaque offensive non invasive (Red Team, Pentest, etc.) pour tester la conformité des outils et services intégrés au SI et pour sensibiliser les collaborateurs

Contribuer au post-mortem de l'incident en collectant les journaux des outils et services intégrés au SI pour alimenter le retour d'expérience (REX) et le partager avec les membres de la DSI

Blocs de compétences

RNCP42837BC01 — Déployer et administrer des infrastructures systèmes sécurisées

LISTE DE COMPÉTENCES

Analyser le système d'information à partir de la documentation existante (inventaire, plan d'assurance qualité, PCA/PRA, etc.) pour identifier les matériels et logiciels à conserver, à améliorer (upgrader) ou à remplacer

Concevoir le POC (Proof Of Concept) en intégrant les besoins techniques et fonctionnels identifiés à partir des exigences du client interne ou externe et en mobilisant des outils de virtualisation du système pour confirmer les hypothèses et établir le plan de déploiement de l'infrastructure système

Concevoir le plan de déploiement de l'infrastructure système dans le respect des réglementations et normes en vigueur (RGPD, NIS2, etc.) ou d'usage (DORA, HDS, etc.) et en mobilisant une méthode de planification de projet (WBS par ex) pour préparer le déploiement

Planifier le déploiement de l'infrastructure système en communiquant auprès de tous les acteurs impactés pour garantir sa mise en place

Configurer les systèmes d'exploitation de l'infrastructure système (Microsoft Windows, Linux, etc.) pour garantir l'interopérabilité des environnements et la continuité de service en installant les rôles et fonctionnalités (annuaire, stockage, authentification, DNS, etc.)

Concevoir un script en mobilisant des outils de scripting et/ou d'orchestration (PowerShell, Ansible, Terraform, etc.) pour automatiser les tâches d'administration de l'infrastructure système (massification et traçabilité des actions, détection de dysfonctionnements)

Configurer l'infrastructure système, dans le respect des préconisations de l'ANSSI en utilisant les outils de la

sécurisation du SI 'by design' (renforcement de la sécurité du SI (Hardening), gestion des accès, journalisation, segmentation, cloisonnement, etc.), pour garantir son intégrité

Proposer l'évolution de la politique de sécurité Cloud (dont le contrôle des identités, la gestion des accès, la segmentation et/ou cloisonnement du réseau, le chiffrement des données, etc.), dans le respect de la réglementation en vigueur (RGPD, NIS2, préconisations ANSSI, etc.) pour la soumettre et l'intégrer à la PSSI de l'entreprise

Administrer les ressources Cloud (SaaS, IaaS et/ou PaaS) dans des environnements publics, privés ou hybrides, pour garantir l'interopérabilité et donc un niveau de services conforme aux attentes des utilisateurs

Configurer les services Cloud (AWS, Azure, GCP, etc.) pour garantir l'interopérabilité du SI local (on-premise) et donc un niveau de services conforme aux attentes des utilisateurs (annuaire, authentification, stockage, etc.)

Proposer l'évolution de la politique de sécurisation de l'infrastructure de virtualisation (dont le contrôle des identités, la gestion des accès, la segmentation et/ou cloisonnement du réseau, le chiffrement des données, journalisation, mécanisme de sauvegarde des VM, etc.), dans le respect de la réglementation en vigueur (RGPD, NIS2, préconisations ANSSI, etc.) pour la soumettre et l'intégrer à la PSSI de l'entreprise

Configurer des infrastructures virtualisées au sein du SI local (on-premise) ou en hybride pour garantir l'interopérabilité des différents services (accès aux données, répliquions du système, etc.) et donc un niveau de services conforme aux attentes des utilisateurs

Déployer un cluster de serveurs de virtualisation en activant les fonctionnalités de haute disponibilité, d'équilibrage de charge, de partage de stockage, et de cliché instantané pour assurer la continuité de l'activité dans l'entreprise

MODALITÉS D'ÉVALUATION

Application professionnelle réelle ou simulée de déploiement et d'administration d'infrastructures systèmes donnant lieu à la production d'un document écrit suivi d'une présentation orale

RNCP42837BC02 — Déployer et administrer des infrastructures réseaux sécurisées

LISTE DE COMPÉTENCES

Analyser le système d'information à partir de la documentation existante (inventaire, plan d'assurance qualité, PCA/PRA, etc.) pour identifier les composants du réseau à conserver, à améliorer (upgrader) ou à remplacer

Concevoir le POC (Proof Of Concept) en intégrant les besoins techniques et fonctionnels identifiés à partir des exigences du client interne ou externe et en mobilisant des outils de virtualisation du réseau pour confirmer les hypothèses et établir le plan de déploiement de l'infrastructure réseaux

Concevoir le plan de déploiement de l'infrastructure réseaux dans le respect des réglementations et normes en vigueur (RGPD, NIS2, etc.) en mobilisant une méthode de planification de projet (WBS par ex) pour préparer le déploiement

Planifier le déploiement de l'infrastructure réseaux en communiquant auprès de tous les acteurs impactés pour garantir sa mise en place

Concevoir l'infrastructure intégrant les architectures convergentes entre le réseau local - LAN (dont le réseau virtuel) et le réseau étendu - WAN pour garantir l'interopérabilité des réseaux dans le respect des différentes normes et protocoles (VLAN, routage inter-VLAN, WLAN, STP, DNA, HSRP, BGP, EIGRP, SNMP, etc.) et donc un niveau de services conforme aux attentes des utilisateurs

Concevoir un script en mobilisant des outils de scripting et/ou d'orchestration (Python, etc.) pour automatiser les tâches d'administration de l'infrastructure réseau (massification et traçabilité des actions, détection de dysfonctionnements, SysOps)

Collecter automatiquement et régulièrement les logs sur les équipements du réseau, en s'assurant de leur intégrité, pour les archiver dans un point central identifié sur le réseau conformément à la PSSI et les exploiter au besoin (diagnostic de panne, de cyberattaque, etc.)

Configurer les équipements de protection du réseau (Firewall Next Gen, Appliance, etc.) en intégrant des règles de filtrage, le contrôle d'accès, l'authentification multi facteurs, etc. dans le respect des préconisations de l'ANSSI pour limiter les expositions aux risques cyber ou de sécurité

Assurer une veille technologique et cyber, sous couvert du RSSI, pour garantir la mise à jour des équipements de protection du réseau du point de vue du système d'exploitation (IOS, Firmware, etc.) et ainsi protéger l'entreprise de nouvelles failles de sécurité

Concevoir les interconnexions multisites (MPLS, SDWAN, Hub and Spoke, etc.) pour autoriser, selon les conditions, les accès aux ressources de l'entreprise

Configurer les solutions de connexion sécurisées à distance (VPN SSL ou VPN IPSec) pour autoriser, selon les conditions, les accès aux ressources de l'entreprise

Proposer l'évolution de la PSSI de l'entreprise, dans le respect des réglementations en vigueur et selon les

préconisations de l'ANSSI, en intégrant la gestion des configurations pour la partager avec les membres de la DSI et l'associer au PCA/PRA

MODALITÉS D'ÉVALUATION

Application professionnelle réelle ou simulée de déploiement et d'administration d'infrastructures réseaux donnant lieu à la production d'un document écrit suivi d'une présentation orale

RNCP42837BC03 — Maintenir en condition opérationnelle les infrastructures informatiques

LISTE DE COMPÉTENCES

Adapter le plan de maintenance des infrastructures du SI en prévoyant les mises à jour, les pannes (matérielles et/ou logicielles) et les défaillances, leur mode de résolution associé (systématique, conditionnel et prédictif) et la fréquence d'intervention pour garantir le maintien en condition opérationnelle (MCO) de l'infrastructure

Déployer le plan de maintenance des infrastructures du SI en considérant sa disponibilité et celles des mises à jour, et en gérant les aléas, pour garantir le MCO du SI et son intégrité

Documenter les actions réalisées dans le cadre du plan de maintenance des infrastructures du SI pour assurer une traçabilité et un archivage des configurations (versioning) accessible à l'ensemble de l'équipe technique

Dimensionner les SLA (Service Level Agreement), MTTR (Mean Time To Repair) et MTBF (Mean Time Between Failure) pour configurer les solutions dans le respect d'ITIL permettant d'assurer une disponibilité (GTR et GTI) conforme aux exigences du métier

Déterminer les seuils d'alertes des dysfonctionnements des matériels et logiciels en fonction de leurs criticités pour concevoir une supervision proactive de l'ensemble du SI et réagir en traitant l'incident ou le sinistre

Définir les indicateurs (réserve, charge, etc.) pour piloter la disponibilité et le niveau de performance de l'ensemble du SI en rendant leur évolution accessible à toutes les parties prenantes

Proposer des améliorations à partir de l'exploitation et de l'analyse des données (indicateurs, incidents, sinistres et leurs traitements, etc.) pour garantir la continuité de service et l'efficacité de l'ensemble du SI

Déployer des solutions combinées de sauvegarde (granulaire, glacier, snapshot, méthode 3-2-1, etc.) et de réplication pour répondre aux besoins métier et garantir la reprise partielle ou complète d'un SI intègre

Elaborer le plan de sauvegarde en tenant compte des RPO (Recovery Point Objective) et RTO (Recovery Time Objective) définis dans la PSSI de l'entreprise pour assurer l'efficacité de la sauvegarde et la cohérence entre les sauvegardes et la restauration

Réviser les procédures des PCA et PRA, dans le respect des exigences réglementaires et normatives et des bonnes pratiques de l'ANSSI, pour capitaliser (suite à sinistre ou tests), les maintenir à jour (suite à évolution matérielle) et pour les partager avec l'ensemble de l'équipe technique

MODALITÉS D'ÉVALUATION

Application professionnelle réelle ou simulée de maintien en condition opérationnelle des infrastructures donnant lieu à la production d'un document écrit suivi d'une présentation orale

RNCP42837BC04 — Auditer et sécuriser les infrastructures informatiques

LISTE DE COMPÉTENCES

Assurer une veille des risques cyber pour identifier les vulnérabilités, les failles et des solutions innovantes de sécurisation et à terme pour évaluer le niveau de maturité de l'infrastructure, en s'appuyant sur les normes et réglementations en vigueur, sur les bonnes pratiques (ISO 27001, RGS, NIST, ANSSI, etc.) et les partages au sein de communautés d'experts

Réaliser un audit (conformité et sécurité) de l'infrastructure en mobilisant des outils d'intrusion et/ou de scans automatisés pour établir un état des lieux (scoring) de l'infrastructure et proposer la mise à jour du plan de remédiation au RSSI

Appliquer la gestion des identités, des accès (IAM) et des privilèges (PAM) et l'authentification forte (MFA, certificats, bastion d'administration), issues de la PSSI de l'entreprise, dans le respect des bonnes pratiques de l'ANSSI (charte de l'administrateur par exemple) pour garantir la traçabilité d'accès aux données et l'administration de l'infrastructure du SI

Configurer les firewalls (de type NextGen par exemple) dans le respect de la réglementation en vigueur (NIS2, RGPD, DORA, etc.), des bonnes pratiques de l'ANSSI (préconisations Zéro Trust Network Access, etc.) et des règles de détection et de protection (IDS, IPS, etc.) définies dans la PSSI de l'entreprise pour sécuriser les accès distants (VPN, MPLS, SD Wan)

Auditer la traçabilité des connexions en centralisant, à l'aide d'un outil de type SIEM, l'ensemble des logs de tous les

équipements pour surveiller le SI et identifier les failles et/ou vulnérabilités
Qualifier l'incident de sécurité détecté par les outils et services intégrés au SI (SIEM, supervision, journalisation, SOC, etc.) pour alerter sa hiérarchie et réagir en temps réel
Déployer des contre-mesures en réponse à une alerte de sécurité pour contrôler l'intrusion et préserver l'intégrité des données du SI et l'activité de l'entreprise tout en rendant compte à la hiérarchie
Collecter des éléments de preuve par une méthode d'investigation numérique (démarche forensique par exemple) pour qu'ils soient exploitables par les autorités et/ou les assurances cyber
Simuler une attaque offensive non invasive (Red Team, Pentest, etc.) pour tester la conformité des outils et services intégrés au SI et pour sensibiliser les collaborateurs
Contribuer au post-mortem de l'incident en collectant les journaux des outils et services intégrés au SI pour alimenter le retour d'expérience (REX) et le partager avec les membres de la DSI

MODALITÉS D'ÉVALUATION

Application professionnelle réelle ou simulée d'audit et de sécurisation des infrastructures donnant lieu à la production d'un document écrit suivi d'une présentation orale

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'Administrateur systèmes, réseaux et cybersécurité peut exercer dans tout secteur d'activité et toute taille d'entreprise.

TYPE D'EMPLOIS ACCESSIBLES

Administrateur systèmes, réseaux et sécurité
Administrateur système et/ou réseau
Administrateur infrastructure
Chef de projet systèmes et réseaux
Responsable systèmes et réseaux
Responsable cloud et virtualisation

RÉGLEMENTATIONS D'ACTIVITÉ

Le métier d'Administrateur systèmes, réseaux et cybersécurité s'exerce dans un cadre réglementaire très précis. En fonction de l'environnement dans lequel il évolue, il ne peut se soustraire :

Aux réglementations :

Le règlement général sur la protection des données (RGPD)

Le Cyber Résilience Act

Aux directives :

La directive 2002/96/CE du 27 janvier 2003 relative aux déchets d'équipements électriques et électroniques

La directive Sécurité des réseaux et de l'information dite directive NIS et NIS2

Aux normes :

La norme internationale de sécurité des systèmes d'information (ISO/CEI 27000)

La norme internationale pour les systèmes de management de la continuité d'activité (SMCA/ISO 22301)

La certification Hébergeur de Données de Santé (HDS)

La norme de communication de tous les systèmes informatiques en réseau (Modèle OSI)

Aux référentiels :

Le référentiel général de sécurité (RGS)

Aux bonnes pratiques :

La bibliothèque pour l'infrastructure des technologies de l'information (ITIL : Information Technology Infrastructure Library),

L'Autorité Nationale en matière de Sécurité et de défense des Systèmes d'Information (ANSSI)

La méthode d'évaluation des risques en informatique EBIOS

La méthode de sécurisation de l'information MEHARI

Aux engagements pour un numérique responsable :

La Charte numérique responsable de l'INRO (Institut du Numérique Responsable) : https://charter.isit-europe.org/?lang=fr_FR

A différents protocoles :

dont les protocoles TCP, IP, SNMP, VLAN, WLAN, HSRP, BGP, EIGRP, etc.

Enfin, dans le cadre de son activité de déploiement et d'installation de logiciels sur les réseaux et serveurs, l'Administrateur systèmes, réseaux et cybersécurité doit respecter le droit des affaires (contrat de licences logicielles) et le droit de la propriété intellectuelle (droit d'auteur, brevet).

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 704 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % des actifs en emploi)
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	14 307
Jugés difficiles à recruter	46 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue, Apprentissage, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Le candidat doit être titulaire d'une certification de niveau 5 à dominante informatique. Tout autre profil relève du dérogatoire.

La sélection des candidats comprend un dossier de candidature avec CV et lettre de motivation, des tests de positionnement, un entretien individuel de sélection.

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, VAE

Le jury est composé de 4 membres professionnels externes dont 50% en activité dans le métier ou qui supervisent des personnes l'exerçant.

Base légale

Date de décision	30/09/2026
Durée de l'enregistrement	5 ans

Date d'échéance de l'enregistrement 30/09/2031

Date de dernière délivrance possible 30/09/2035

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2024	636	0	80 %	—
2023	631	4	85 %	68 %
2022	610	2	87 %	68 %
2021	918	5	88 %	72 %

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP36075

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42837/>