

Administrateur des systèmes, réseaux et sécurité

RNCP41807 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326n
Formacode(s)	31034, 24220, 31045
Code(s) ROME	M1801, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	18/12/2025
Date d'échéance	18/12/2028

Certificateur(s)

DORANCO ESPACE MULTIMEDIA · SIRET : 38935885400054

Partenaires habilités

2 organismes habilités, d'après la liste publiée par France compétences : 2 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
INSTITUT FRANCAIS DES AFFAIRES	38480937200046	Former et organiser l'évaluation
M2S CAMPUS	82175021300034	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

La certification « Administrateur Systèmes, Réseaux et Sécurité » (ASR) a pour objectif d'être une réponse concrète aux besoins accrus de compétences opérationnelles exprimées par les entreprises.

L'Administrateur Systèmes, Réseaux et Sécurité est un professionnel clé du fonctionnement des systèmes d'information dans les organisations. Il a pour mission de garantir la disponibilité, la performance et la sécurité des infrastructures informatiques en assurant leur déploiement, leur maintenance, leur supervision et leur protection.

ACTIVITÉS VISÉES

Diagnostic initial des spécificités de l'entreprise
Réalisation d'un audit des infrastructures existantes
Conception et dimensionnement des infrastructures
Conception et gestion d'un environnement hybride
Rédaction et mise à jour de la documentation technique
Déploiement et configuration de l'infrastructure réseau
Déploiement et configuration des bases de données
Paramétrage et administration des systèmes d'exploitation (Linux, Windows)
Configuration et déploiement des postes clients et services transverses
Définition et automatisation des procédures de déploiement
Analyse des risques et configuration des alertes
Définition et diffusion de procédures de réponse aux alertes
Organisation et vérification de la conformité des contrôles d'accès
Mise en place et suivi des indicateurs de performance

Organisation de la maintenance préventive et corrective des matériels et logiciels

Gestion des incidents de cybersécurité et des pertes de données

Conduite des audits de sécurité et amélioration continue des infrastructures

COMPÉTENCES ATTESTÉES

Analyser les besoins fonctionnels et techniques des équipes métiers et IT en tenant compte des contraintes organisationnelles, budgétaires et réglementaires, afin de définir les exigences d'infrastructure adaptées.

Évaluer les exigences réglementaires et normatives applicables (RGPD, NIS II, DORA LPM, RGAA, etc.) en intégrant les contraintes d'accessibilité et les enjeux environnementaux, afin d'assurer la conformité et la sécurité dès la conception des infrastructures.

Cartographier les infrastructures existantes (serveurs, réseaux, applications critiques) en exploitant des outils de découverte et de modélisation (Nmap, Visio), afin d'identifier leur état, leur résilience et leurs capacités d'évolution.

Identifier les vulnérabilités des infrastructures existantes en réalisant des tests de sécurité (black box, grey box) et en analysant les configurations à l'aide d'outils spécialisés (Nessus, Metasploit), afin d'identifier les axes d'amélioration à mettre en oeuvre lors de la conception de l'architecture et de définir le niveau de maturité de départ de l'organisation.

Concevoir une architecture systèmes et réseaux modulaire et évolutive en intégrant les principes de cybersécurité (Security by Design), d'éco-conception (Green IT, virtualisation) et en sélectionnant les solutions adaptées (on-premise, cloud hybride, SD-WAN), afin d'optimiser la performance et la sécurité des infrastructures

Dimensionner les ressources matérielles et logicielles, en fonction du niveau de disponibilité attendu des services (serveurs, stockage, équipements réseau), en appliquant les principes de coût total de possession (TCO) et de retour sur investissement (ROI), afin de garantir la performance, la pérennité et l'optimisation financière des infrastructures.

Concevoir une infrastructure hybride intégrant des environnements locaux et cloud (public/privé), en définissant un plan de migration, une stratégie d'interconnexion sécurisée (VPN, SD-WAN), des dispositifs d'accessibilité numérique adaptés et une démarche FinOps, afin d'assurer la continuité des services, la flexibilité opérationnelle.

Intégrer les principes de sécurité spécifiques aux environnements hybrides et Cloud dès la conception en définissant une politique de gouvernance et de gestion des accès (RBAC, MFA, journalisation, etc.), de protection des données (classification, chiffrement, sauvegarde, etc.) de sécurité réseau (Zero Trust, segmentation, filtrage, VPN, sécurité des APIs etc.), protection des API, afin d'assurer la conformité aux exigences réglementaires (RGPD, Cloud Act, ISO 27018).

Rédiger les documentations techniques et les guides utilisateurs des infrastructures (administration, exploitation, sécurité), en intégrant les exigences d'accessibilité numérique

(mise en forme lisible, compatibilité lecteurs d'écran, navigation claire) et les besoins spécifiques des destinataires, y compris en anglais lorsque nécessaire, afin d'assurer une compréhension inclusive et une diffusion adaptée des informations.

Installer les équipements réseau (switches, routeurs, points d'accès, firewalls, SD-WAN etc.), en appliquant les protocoles adaptés (OSPF, BGP) et en veillant à leur bon dimensionnement, à la redondance des liens critiques et au respect des exigences de performance et de disponibilité, afin de garantir une infrastructure réseau fiable, responsable et résiliente.

Mettre en œuvre les mécanismes de sécurité réseau (filtrage, IDS/IPS, NAC, segmentation, contrôle d'accès), les solutions de sécurisation des services cloud (Zero Trust, IAM, CASB, chiffrement), les accès sécurisés pour le télétravail (ZTNA, VPN, SASE), ainsi que la segmentation des réseaux IoT (VLAN dédiés, passerelles, Zero Trust), afin de garantir la protection des infrastructures et la sécurité des flux dans des environnements hybrides

Installer les bases de données relationnelles (SQL Server, PostgreSQL) et non-relationnelles (NoSQL) en configurant les mécanismes de sauvegarde et de réplication haute disponibilité (clustering), afin d'assurer la continuité des services et la performance des infrastructures.

Sécuriser les bases de données en appliquant des mesures avancées de chiffrement et de gestion des accès (IAM, RBAC, Bastion Hosts) conformément aux exigences réglementaires (RGPD, NIS2), afin de garantir la confidentialité et l'intégrité des données sensibles.

Administrer les systèmes d'exploitation serveurs et postes clients (Linux, Windows) en appliquant les stratégies de durcissement (contrôle des accès, surveillance, minimisation des services...) et en assurant la gestion des mises à jour et correctifs de sécurité, afin de garantir la stabilité et la protection des environnements IT.

Gérer les contrôles d'accès logiques et physiques aux systèmes d'information (postes de travail, systèmes d'exploitation, serveurs, etc.), en utilisant les services centralisés (LDAP, Active Directory) et des techniques d'IAM et de sûreté (RBAC, MFA, SSO pour les accès logiques ; badge, caméra, verrouillage des salles serveurs pour les accès physiques etc.) afin d'assurer la protection des environnements IT et la prévention des risques liés aux

interventions physiques.

Configurer les postes de travail et les services collaboratifs (messagerie, outils bureautiques, accès distants, annuaire centralisé) selon les profils utilisateurs et les contraintes d'accès (BYOD, Remote Desktop, VDI), tout en garantissant un haut niveau de sécurité (chiffrement disque natif, authentification forte MFA), afin d'assurer un environnement fiable et adapté aux besoins spécifiques des utilisateurs, y compris ceux en situation de handicap.

Déployer des services avancés de conteneurisation et de virtualisation (Docker, Kubernetes, Virtual Desktop Infrastructure) au sein des infrastructures existantes, en intégrant les politiques de sécurité (Zero Trust, IAM, segmentation réseau), afin d'améliorer l'évolutivité et la sécurité des environnements IT.

Automatiser le déploiement des infrastructures systèmes et réseaux en documentant les workflows de déploiement et en mobilisant des outils d'Infrastructure as Code (Terraform, Ansible, Puppet, Chef) et les pratiques NetDevOps, afin d'assurer la reproductibilité, la traçabilité et la fiabilité des installations.

Concevoir, en coordination avec les équipes de développement, des pipelines CI/CD intégrant les pratiques SecDevOps (tests de sécurité automatisés, validation des configurations) afin de garantir la sécurité et la conformité des infrastructures dès leur mise en production.

Analyser les risques de surcharge et les menaces d'intrusion sur les infrastructures (vulnérabilités Oday, Shadow IT, APT) en s'appuyant sur les bulletins de veille sécuritaire (CERT) et les outils d'analyse des risques, afin d'anticiper les incidents critiques et de recommander des actions de prévention.

Configurer les alertes de sécurité sur les outils de supervision (SIEM, IDS/IPS, EDR/XDR) en adaptant les seuils de détection aux risques identifiés et en intégrant des scénarios d'alerte précis, afin d'optimiser la réactivité aux anomalies critiques.

Définir les procédures de réponse aux incidents de sécurité, en établissant une classification par niveau de criticité, des modèles de communication adaptés et une liste d'interlocuteurs internes et externes, afin d'assurer une gestion efficace et coordonnée des crises IT.

Concevoir des playbooks SOAR et des checklist opérationnelles de réponses à incident en réalisant des simulations régulières, afin d'améliorer l'efficacité des outils et la réactivité des équipes de supervision face aux cyberattaques.

Gérer les droits d'accès aux systèmes et bases de données

des utilisateurs en appliquant une segmentation des utilisateurs selon leur profil et leur droit d'en connaître (IAM, RBAC, Zero Trust, MFA, Bastion hosts), afin de sécuriser l'accès aux ressources critiques.

Contrôler la conformité des mécanismes d'accès aux systèmes et bases de données des utilisateurs en réalisant des audits réguliers des permissions et des mécanismes d'authentification, afin d'identifier les écarts et mettre en œuvre les mesures correctives nécessaires conformément aux exigences réglementaires (RGPD, ISO 27001, NIS2).

Définir les indicateurs clés de performance (KPI) des infrastructures systèmes et réseaux en fonction des besoins métier et techniques, afin de mesurer et suivre l'état et l'évolution des performances et de la sécurité à l'aide d'outils de supervision dédiés (Nagios, Zabbix, etc.).

Automatiser la surveillance des performances et l'analyse des anomalies en configurant les seuils d'alerte et en appliquant des processus d'optimisation continue, afin d'anticiper les incidents et garantir la résilience des infrastructures.

Planifier la maintenance préventive et corrective des infrastructures en s'appuyant sur l'analyse prédictive des pannes (via l'IA et le

machine learning), et l'automatisation des mises à jour (avec des outils comme Ansible, WSUS), tout en intégrant les contraintes

environnementales et énergétiques, afin d'optimiser les interventions garantir la continuité des services et renforcer la durabilité des infrastructures.

Superviser l'application des correctifs logiciels et des mises à jour de sécurité en validant leur impact avant mise en production, afin d'assurer une application rapide et homogène sur l'ensemble des infrastructures IT.

Gérer le suivi des demandes utilisateurs et des interventions techniques via un outil ITSM (GLPI, ServiceNow), en veillant à prendre en compte les besoins spécifiques, y compris ceux liés à des situations de handicap, afin d'assurer une traçabilité optimale et une gestion efficace des priorités selon leur criticité métier

Exécuter les procédures de réponse aux cyberattaques en mobilisant les playbooks SOAR, les outils d'automatisation et les checklists de réponse à incident, afin d'assurer une remédiation efficace et minimiser l'impact sur les infrastructures.

Mettre en œuvre une stratégie de sauvegarde et de restauration des données (PCA/PRA) et réaliser des tests de récupération réguliers, afin de garantir la continuité d'activité après un incident majeur.

Analyser les causes des incidents de cybersécurité et pertes de données en coordination avec les équipes de supervision, afin de définir des mesures correctives et renforcer la résilience des infrastructures.

Réaliser des audits organisationnels et techniques des infrastructures pour évaluer leur conformité aux exigences réglementaires et sécuritaires (ISO 27001, NIS2) et identifier les axes d'amélioration.

Mettre en place un suivi des plans d'amélioration en assurant la mise en œuvre des actions correctives et en intégrant des critères de durabilité et d'éco-responsabilité (Green IT), afin de garantir l'adaptabilité des infrastructures aux évolutions technologiques et réglementaires.

Superviser l'efficacité des mesures d'amélioration et des audits en assurant un suivi régulier des performances et des risques identifiés, afin de garantir l'évolution continue des infrastructures IT en lien avec les enjeux métiers.

Blocs de compétences

RNCP41807BC01 — Concevoir des infrastructures systèmes et réseaux adaptées aux besoins de l'entreprise

LISTE DE COMPÉTENCES

Analyser les besoins fonctionnels et techniques des équipes métiers et IT en tenant compte des contraintes organisationnelles, budgétaires et réglementaires, afin de définir les exigences d'infrastructure adaptées.

Évaluer les exigences réglementaires et normatives applicables (RGPD, NIS II, DORA LPM, RGAA, etc.) en intégrant les contraintes d'accessibilité et les enjeux environnementaux, afin d'assurer la conformité et la sécurité dès la conception des infrastructures.

Cartographier les infrastructures existantes (serveurs, réseaux, applications critiques) en exploitant des outils de découverte et de modélisation (Nmap, Visio), afin d'identifier leur état, leur résilience et leurs capacités d'évolution.

Identifier les vulnérabilités des infrastructures existantes en réalisant des tests de sécurité (black box, grey box) et en analysant les configurations à l'aide d'outils spécialisés (Nessus, Metasploit), afin d'identifier les axes d'amélioration à mettre en œuvre lors de la conception de l'architecture et de définir le niveau de maturité de départ de l'organisation.

Concevoir une architecture systèmes et réseaux modulaire et évolutive en intégrant les principes de cybersécurité (Security by Design), d'éco-conception (Green IT, virtualisation) et en sélectionnant les solutions adaptées (on-premise, cloud hybride, SD-WAN), afin d'optimiser la performance et la sécurité des infrastructures.

Dimensionner les ressources matérielles et logicielles, en fonction du niveau de disponibilité attendu des services (serveurs, stockage, équipements réseau), en appliquant les principes de coût total de possession (TCO) et de retour sur investissement (ROI), afin de garantir la performance, la pérennité et l'optimisation financière des infrastructures.

Concevoir une infrastructure hybride intégrant des environnements locaux et cloud (public/privé), en définissant un plan de migration, une stratégie d'interconnexion sécurisée (VPN, SD-WAN), des dispositifs d'accessibilité numérique adaptés et une démarche FinOps, afin d'assurer la continuité des services, la flexibilité opérationnelle.

Intégrer les principes de sécurité spécifiques aux environnements hybrides et Cloud dès la conception en définissant une politique de gouvernance et de gestion des accès (RBAC, MFA, journalisation, etc.), de protection des données (classification, chiffrement, sauvegarde, etc.) de sécurité réseau (Zero Trust, segmentation, filtrage, VPN, sécurité des APIs etc.), protection des API, afin d'assurer la conformité aux exigences réglementaires (RGPD, Cloud Act, ISO 27018).

Rédiger les documentations techniques et les guides utilisateurs des infrastructures (administration, exploitation, sécurité), en intégrant les exigences d'accessibilité numérique

(mise en forme lisible, compatibilité lecteurs d'écran, navigation claire) et les besoins spécifiques des destinataires, y compris en anglais lorsque nécessaire, afin d'assurer une compréhension inclusive et une diffusion adaptée des informations.

MODALITÉS D'ÉVALUATION

Projet professionnel + soutenance orale devant un jury

RNCP41807BC02 — Déployer et configurer des infrastructures sécurisées

LISTE DE COMPÉTENCES

Installer les équipements réseau (switches, routeurs, points d'accès, firewalls, SD-WAN etc.), en appliquant les protocoles adaptés (OSPF, BGP) et en veillant à leur bon dimensionnement, à la redondance des liens critiques et au respect des exigences de performance et de disponibilité, afin de garantir une infrastructure réseau fiable, responsable et résiliente.

Mettre en œuvre les mécanismes de sécurité réseau (filtrage, IDS/IPS, NAC, segmentation, contrôle d'accès), les solutions de sécurisation des services cloud (Zero Trust, IAM, CASB, chiffrement), les accès sécurisés pour le télétravail (ZTNA, VPN, SASE), ainsi que la segmentation des réseaux IoT (VLAN dédiés, passerelles, Zero Trust),

afin de garantir la protection des infrastructures et la sécurité des flux dans des environnements hybrides
Installer les bases de données relationnelles (SQL Server, PostgreSQL) et non-relationnelles (NoSQL) en configurant les mécanismes de sauvegarde et de réplication haute disponibilité (clustering), afin d'assurer la continuité des services et la performance des infrastructures.

Sécuriser les bases de données en appliquant des mesures avancées de chiffrement et de gestion des accès (IAM, RBAC, Bastion Hosts) conformément aux exigences réglementaires (RGPD, NIS2), afin de garantir la confidentialité et l'intégrité des données sensibles.

Administrer les systèmes d'exploitation serveurs et postes clients (Linux, Windows) en appliquant les stratégies de durcissement (contrôle des accès, surveillance, minimisation des services...) et en assurant la gestion des mises à jour et correctifs de sécurité, afin de garantir la stabilité et la protection des environnements IT.

Gérer les contrôles d'accès logiques et physiques aux systèmes d'information (postes de travail, systèmes d'exploitation, serveurs, etc.), en utilisant les services centralisés (LDAP, Active Directory) et des techniques d'IAM et de sûreté (RBAC, MFA, SSO pour les accès logiques ; badge, caméra, verrouillage des salles serveurs pour les accès physiques etc.) afin d'assurer la protection des environnements IT et la prévention des risques liés aux interventions physiques.

Configurer les postes de travail et les services collaboratifs (messagerie, outils bureautiques, accès distants, annuaire centralisé) selon les profils utilisateurs et les contraintes d'accès (BYOD, Remote Desktop, VDI), tout en garantissant un haut niveau de sécurité (chiffrement disque natif, authentification forte MFA), afin d'assurer un environnement fiable et adapté aux besoins spécifiques des utilisateurs, y compris ceux en situation de handicap.

Déployer des services avancés de conteneurisation et de virtualisation (Docker, Kubernetes, Virtual Desktop Infrastructure) au sein des infrastructures existantes, en intégrant les politiques de sécurité (Zero Trust, IAM, segmentation réseau), afin d'améliorer l'évolutivité et la sécurité des environnements IT.

Automatiser le déploiement des infrastructures systèmes et réseaux en documentant les workflows de déploiement et en mobilisant des outils d'Infrastructure as Code (Terraform, Ansible, Puppet, Chef) et les pratiques NetDevOps, afin d'assurer la reproductibilité, la traçabilité et la fiabilité des installations.

Concevoir, en coordination avec les équipes de développement, des pipelines CI/CD intégrant les pratiques SecDevOps (tests de sécurité automatisés, validation des configurations) afin de garantir la sécurité et la conformité des infrastructures dès leur mise en production.

MODALITÉS D'ÉVALUATION

Projet professionnel + soutenance orale devant un jury

RNCP41807BC03 — Superviser et sécuriser les infrastructures

LISTE DE COMPÉTENCES

Analyser les risques de surcharge et les menaces d'intrusion sur les infrastructures (vulnérabilités Oday, Shadow IT, APT) en s'appuyant sur les bulletins de veille sécuritaire (CERT) et les outils d'analyse des risques, afin d'anticiper les incidents critiques et de recommander des actions de prévention.

Configurer les alertes de sécurité sur les outils de supervision (SIEM, IDS/IPS, EDR/XDR) en adaptant les seuils de détection aux risques identifiés et en intégrant des scénarios d'alerte précis, afin d'optimiser la réactivité aux anomalies critiques.

Définir les procédures de réponse aux incidents de sécurité, en établissant une classification par niveau de criticité, des modèles de communication adaptés et une liste d'interlocuteurs internes et externes, afin d'assurer une gestion efficace et coordonnée des crises IT.

Concevoir des playbooks SOAR et des checklist opérationnelles de réponses à incident en réalisant des simulations régulières, afin d'améliorer l'efficacité des outils et la réactivité des équipes de supervision face aux cyberattaques.

Gérer les droits d'accès aux systèmes et bases de données

des utilisateurs en appliquant une segmentation des utilisateurs selon leur profil et leur droit d'en connaître (IAM, RBAC, Zero Trust, MFA, Bastion hosts), afin de sécuriser l'accès aux ressources critiques.

Contrôler la conformité des mécanismes d'accès aux systèmes et bases de données des utilisateurs en réalisant des audits réguliers des permissions et des mécanismes d'authentification, afin d'identifier les écarts et mettre en œuvre les mesures correctives nécessaires conformément aux exigences réglementaires (RGPD, ISO 27001, NIS2).

Définir les indicateurs clés de performance (KPI) des infrastructures systèmes et réseaux en fonction des besoins métier et techniques, afin de mesurer et suivre l'état et l'évolution des performances et de la sécurité à l'aide d'outils de supervision dédiés (Nagios, Zabbix, etc.).

Automatiser la surveillance des performances et l'analyse des anomalies en configurant les seuils d'alerte et en appliquant des processus d'optimisation continue, afin d'anticiper les incidents et garantir la résilience des

infrastructures.

MODALITÉS D'ÉVALUATION

Projet professionnel + soutenance orale devant un jury

RNCP41807BC04 — Gérer les incidents et assurer la maintenance des infrastructures

LISTE DE COMPÉTENCES

Planifier la maintenance préventive et corrective des infrastructures en s'appuyant sur l'analyse prédictive des pannes (via l'IA et le machine learning), et l'automatisation des mises à jour (avec des outils comme Ansible, WSUS), tout en intégrant les contraintes

environnementales et énergétiques, afin d'optimiser les interventions garantir la continuité des services et renforcer la durabilité des infrastructures.

Superviser l'application des correctifs logiciels et des mises à jour de sécurité en validant leur impact avant mise en production, afin d'assurer une application rapide et homogène sur l'ensemble des infrastructures IT.

Gérer le suivi des demandes utilisateurs et des interventions techniques via un outil ITSM (GLPI, ServiceNow), en veillant à prendre en compte les besoins spécifiques, y compris ceux liés à des situations de handicap, afin d'assurer une traçabilité optimale et une gestion efficace des priorités selon leur criticité métier

Exécuter les procédures de réponse aux cyberattaques en mobilisant les playbooks SOAR, les outils d'automatisation et les checklists de réponse à incident, afin d'assurer une remédiation efficace et minimiser l'impact sur les infrastructures.

Mettre en œuvre une stratégie de sauvegarde et de restauration des données (PCA/PRA) et réaliser des tests de récupération réguliers, afin de garantir la continuité d'activité après un incident majeur.

Analyser les causes des incidents de cybersécurité et pertes de données en coordination avec les équipes de supervision, afin de définir des mesures correctives et renforcer la résilience des infrastructures.

Réaliser des audits organisationnels et techniques des infrastructures pour évaluer leur conformité aux exigences réglementaires et sécuritaires (ISO 27001, NIS2) et identifier les axes d'amélioration.

Mettre en place un suivi des plans d'amélioration en assurant la mise en œuvre des actions correctives et en intégrant des critères de durabilité et d'éco-responsabilité (Green IT), afin de garantir l'adaptabilité des infrastructures aux évolutions technologiques et réglementaires.

Superviser l'efficacité des mesures d'amélioration et des audits en assurant un suivi régulier des performances et des risques identifiés, afin de garantir l'évolution continue des infrastructures IT en lien avec les enjeux métiers.

MODALITÉS D'ÉVALUATION

Projet professionnel + soutenance orale devant un jury

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les Administrateurs Systèmes, Réseaux et Sécurité (ASR) exercent dans une grande diversité d'organisations : grandes entreprises, PME, administrations publiques, établissements d'enseignement, collectivités territoriales, ou encore associations. La taille de la structure et la maturité numérique de l'organisation influencent fortement la spécialisation ou la polyvalence du poste.

TYPE D'EMPLOIS ACCESSIBLES

Administrateur cloud / Administrateur cloud hybride

Administrateur d'infrastructures informatiques / Administrateur infrastructures hybrides

Administrateur réseau et sécurité

Administrateur sécurité informatique / Administrateur cybersécurité

Administrateur systèmes et réseaux

Administrateur systèmes Linux / Windows

Administrateur systèmes, réseaux et sécurité

Administrateur virtualisation / conteneurisation

Intégrateur systèmes et réseaux

Spécialiste systèmes et réseaux

Superviseur infrastructure et réseaux

RÉGLEMENTATIONS D'ACTIVITÉ

Règlement général sur la protection des données (RGPD) - Règlement (UE) 2016/679 – Loi n°2018-493 du 20 juin 2018: L'Administrateur Systèmes et Réseaux est un acteur clé dans la mise en œuvre des mesures de sécurité et de confidentialité visant à protéger les données personnelles.

Directive NIS 2 - Directive (UE) 2022/2555 : Transposée en droit français, la directive NIS 2 impose un renforcement des pratiques de cybersécurité pour les structures publiques et privées jugées critiques.

Règlement DORA – Résilience opérationnelle numérique - Règlement (UE) 2022/2554 – Digital Operational Resilience Act: Applicable à partir du 17 janvier 2025, DORA impose aux entités financières et à leurs prestataires IT des obligations renforcées de résilience numérique, notamment sur la gouvernance, la gestion des incidents, la continuité d'activité, les tests de résilience, et la gestion des tiers.

Référentiel général d'amélioration de l'accessibilité (RGAA): Les ASR sont amenés à déployer des postes de travail, services collaboratifs ou interfaces d'administration accessibles à tous, notamment aux personnes en situation de handicap. Le respect du RGAA garanti l'accessibilité numérique.

ISO 27001 – Sécurité de l'information: Sans être juridiquement obligatoire, la norme ISO 27001 constitue une référence dans la gestion de la sécurité des systèmes d'information.

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)	Modérée (3/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 4 sur 5.
Facteurs principaux	Intensité d'embauche, Inadéquation géographique
Salaire médian (mensuel)	2 419 €
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)
Projets de recrutement (BMO 2026)	9 549
Jugés difficiles à recruter	46 %
Emplois saisonniers	3 %
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

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Pour accéder à la formation menant à la certification professionnelle "Administrateur des Systèmes, Réseaux et Sécurité", ainsi qu'aux blocs de compétences constitutifs du titre, les candidats doivent satisfaire aux conditions préalables suivantes :

Être titulaire d'une certification professionnelle ou d'un diplôme de niveau 5

Ou être titulaire du baccalauréat ou d'une certification professionnelle de niveau 4 et justifier d'une expérience significative, d'une durée de six mois à un an, dans le secteur de l'administration des systèmes.

Les candidats peuvent également intégrer la formation après un niveau 4 validé pour un cycle de formation de 3 ans.

Les prérequis sont vérifiés dans le cadre d'une évaluation diagnostique (tests d'entrée et étude de dossier) par notre équipe pédagogique.

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

Le jury de certification est composé de 3 personnes :

2 professionnels en activité dans l'administration des systèmes, externe au réseau Doranco
1 représentant du certificateur

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle	7 702 €
Selon la branche	5 287 € – 9 074 €

Prise en charge	Branches concernées
7 702 €	Valeur par défaut · 202 branches
9 074 €	CPNE des Télécoms, CPNEF de la Branche des organismes de formation, CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
7 604 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement
9 010 €	CPNE de l'ingénierie, des services informatiques et du conseil
8 700 €	CPNEFP ICGV entreprises de la viande
7 500 €	CPNE des industries de santé (CPNEIS)
7 421 €	CPNEFP dans les établissements d'enseignement privés sous contrat
7 000 €	CPNEFP de la métallurgie
5 287 €	CPNEFP des commerces de gros

Base légale

Date de décision	18/12/2025
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	18/12/2028
Date de dernière délivrance possible	18/12/2032

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2024	59	0	76 %	—
2023	65	0	81 %	56 %
2022	187	0	85 %	64 %
2021	10	0	100 %	60 %

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP35093

CORRESPONDANCES (PAR BLOCS)
RNCP38117, RNCP39851

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.nexa.fr/formations/bachelor-administrateur-reseau-cybersecurite-en-alternance>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/41807/>

Où se former

Formations référencées	1
Organismes	1
Régions couvertes	1
Prix indicatif	6 700 €

Offre de formation — MonCompteFormation (Caisse des Dépôts), licence ouverte.

Se former en apprentissage

Formations en apprentissage	2
Organismes gestionnaires (CFA)	2
Organismes formateurs	2
Régions couvertes	2
Départements couverts	2
Organismes certifiés Qualiopi	2
Sessions	de 08/2026 à 10/2029

Catalogue des formations en apprentissage — réseau des Carif-Oref. Sans frais pour l'alternant : formation financée par l'OPCO de la branche (NPEC).