Politique de Sécurité des Systèmes d'Information

Neo Financia

RÉFÉRENCE

CLASSIFICATION

VERSION

DATE D'APPROBATION

APPROBATION

PROPRIÉTAIRE

PÉRIODICITÉ DE RÉVISION

Table des matières

PSSI-NFQ-2025-V1.0

INTERNF

1. 0

20 avril 2025

Conseil d'Administration de Neo-Financia

RSS

Annuelle

Introduction et objectifs

Présentation de Neo Financia

Neo Financia est une néobanque européenne offrant des services bancaires innovants exclusivement à travers les canaux numériques. Fondée sur un modèle digital-first, Neo Financia sert 2 millions de clients avec une équipe de 1000 collaborateurs répartis entre son siège social à Paris et ses bureaux de Lyon et Londres.

La banque propose une gamme complète de services financiers incluant

- Crédits consommateurs et immobiliers
- Services aux professionnels
- Comptes courants personnels et professionnels
- Produits d'épargne réglementés (Livret A, LDDS, LEP, etc.)
- Comptes et plans d'épargne logement (CEL, PEL)
- Produits d'épargne non réglementés (Livret Boosté, Livret Engagé, etc.)

Contexte et enjeux

En tant que néobanque opérant exclusivement via les canaux digitaux, Neo Financia fait face à des enjeux de sécurité spécifiques:

Nos défis de sécurité particuliers :

- Dépendance totale aux infrastructures technologiques et digitales
- Complexité réglementaire liée à notre présence multi-juridictionnelle (France, UE, Royaume-Uni post-Brexit)
- Attentes élevées des clients en matière de disponibilité (24/7) et d'expérience utilisateur fluide
- Surface d'attaque élargie par la multiplication des canaux d'accès et des APIs
- Concurrence avec les acteurs traditionnels nécessitant d'innover sans compromettre la sécurité
- Gestion des risques transfrontaliers, particulièrement entre l'UE et le Royaume-Un
- Accroissement des menaces ciblant spécifiquement le secteur financier (ransomware, fraude, exfiltration de données)

Avec une maturité digitale actuelle de 3.3/5, Neo Financia poursuit sa transformation numérique tout en faisant face à un environnement de menaces en constante évolution.

Objectifs de la PSSI

La Politique de Sécurité des Systèmes d'Information (PSSI) constitue le socle stratégique de la démarche de cybersécurité de Neo Financia. Elle définit les exigences fondamentales destinées à :

- Protéger les actifs informationnels critiques de la banque et de ses clients
- Garantir la confidentialité, l'intégrité, la disponibilité et la traçabilité des données et services
- Assurer la conformité aux exigences réglementaires multiples (DORA, NIS2, RGPD, etc.)
- Maintenir la confiance des clients et des partenaires
- Renforcer la résilience opérationnelle face aux cybermenaces
- Fournir un cadre cohérent pour la gestion des risques cyber
- Promouvoir une culture de sécurité à tous les niveaux de l'organisation

Champ d'application

Cette politique s'applique à :

- L'ensemble des collaborateurs de Neo Financia, quel que soit leur statut (permanent, temporaire, alternant, stagiaire)
- Les prestataires et partenaires ayant accès aux systèmes d'information de Neo Financia, y compris les partenaires fintech comme Mangopay et Lemonway
- Tous les systèmes d'information utilisés pour traiter, stocker ou transmettre des informations appartenant à Neo Financia ou à ses clients
- L'ensemble des sites de Neo Financia (Paris, Lyon, Londres)
- Tous les environnements techniques, qu'ils soient internes, cloud (Azure, AWS, OVHcloud) ou externalisés

Principes directeurs

Neo Financia s'engage à respecter les principes suivants dans la mise en œuvre de sa politique de sécurité

- Approche basée sur les risques : Les mesures de sécurité sont proportionnées aux risques identifiés et à l'importance des actifs à protéger.
- Défense en profondeur : Mise en place de multiples couches de protection complémentaires pour réduire la probabilité d'une compromission complète.
- Sécurité par conception : Intégration de la sécurité dès les phases initiales de tout nouveau projet ou service
- Moindre privilège : Limitation des droits d'accès au strict nécessaire pour l'accomplissement des missions
- Résilience : Capacité à maintenir ou à rétablir rapidement les services essentiels face aux incidents
- Amélioration continue : Processus permanent d'évaluation et d'amélioration des mesures de sécurité
- Conformité : Respect des obligations légales, réglementaires et contractuelles.

Vision et stratégie de cybersécurité

La vision de cybersécurité de Neo Financia s'articule autour de quatre piliers

- Protection proactive : Anticiper et contrer les menaces avant qu'elles n'affectent nos services
- Sécurité by design : Intégrer la sécurité dès la conception de nos produits et services

- Confiance digitale : Garantir à nos clients la protection de leurs données et actifs
- Résilience opérationnelle : Maintenir la continuité de service même en cas d'incidents

---

Avec une appétence au risque modérée (niveau 3 sur 10), Neo Financia adopte une approche équilibrée qui vise à protéger efficacement ses actifs tout en permettant l'innovation et l'agilité nécessaires à son développement.

Organisation de la sécurité

Structure organisationnelle et gouvernance

L'organisation de la sécurité des systèmes d'information de Neo Financia repose sur une structure hiérarchique claire avec des responsabilités bien définies:

Conseil d'Administration ↓ Comité des Risques ↓ Comité Exécutif (COMEX) ↓ Comité de Sécurité (COSEC) ↓ RSSI DSI Conformité

Cette organisation garantit que la sécurité est prise en compte au plus haut niveau de l'entreprise et que les décisions stratégiques intègrent systématiquement la dimension sécurité.

Rôles et responsabilités

Entité/Fonction	Responsabilités principales
Conseil d'Administration	- Validation de la stratégie globale de sécurité
- Approbation de la PSSI et des investissements majeurs	
- Définition de l'appétence au risque	
- Supervision de l'efficacité du dispositif de sécurité	
Comité des Risques	- Revue trimestrielle des risques cyber significatifs
- Validation des plans de traitement des risques majeurs	
- Approbation des exceptions à la PSSI	
-	

Suivi des indicateurs de performance sécurité (KPI)	
Comité Exécutif (COMEX)	- Allocation des ressources nécessaires à la sécurité
- Arbitrage entre les objectifs business et les contraintes de sécurité	

	- Pilotage des projets stratégiques de sécurité
- Promotion de la culture sécurité	
---	---
Comité de Sécurité (COSEC)	- Coordination opérationnelle des activités de sécurité
- Suivi des incidents et des plans d'action	
- Revue des projets et des changements significatifs	
- Reporting mensuel au COMEX	
Responsable de la Sécurité des Systèmes d'Information (RSSI)	- Élaboration et mise à jour de la PSSI
- Pilotage du programme de sécurité	
- Supervision des audits et tests de sécurité	
- Conseil et expertise auprès des métiers et de la direction	
- Animation du COSEC	

Directeur des Systèmes d'Information (DSI)	- Mise en œuvre technique des mesures de sécurité
- Gestion de l'infrastructure sécurisée	
- Intégration de la sécurité dans les projets IT	
- Gestion des habilitations et des accès	
Chief Risk Officer (CRO)	- Intégration des risques cyber dans le dispositif global de gestion des risques
- Coordination avec les autres fonctions de risque	
- Pilotage des plans de continuité d'activité	
- Interface avec les régulateurs	
Chief Information Security Officer (CISO)	- Mise en œuvre opérationnelle de la stratégie de sécurité
- Gestion de l'équipe sécurité	
- Supervision des opérations de sécurité quotidiennes	
- Interface technique avec les partenaires et fournisseurs	
Délégué à la Protection des Données (DPO)	- Veille à la conformité au RGPD
- Gestion du registre des traitements	
- Analyse d'impact relative à la protection des données (AIPD)	

- Point de contact pour les autocités de contrôle	

Directions Métiers	- Application des règles de sécurité dans leurs périmètres
- Identification des besoins de sécurité spécifiques	
- Participation à l'analyse des risques	
- Sensibilisation des équipes	
---	---
Collaborateurs	- Respect de la PSSI et des procédures associées
- Signalement des incidents et anomalies	
- Participation aux formations de sensibilisation	
- Application des bonnes pratiques au quotidien	

Équipe cybersécurité

Neo Financia dispose d'une équipe cybersécurité de 15 professionnels, structurée en pôles fonctionnels avec des niveaux d'expertise variés (de l'alternant au professionnel expérimenté). Cette équipe est organisée selon les domaines de compétence suivants :

- Gouvernance, Risques et Conformité (GRC) : Pilotage de la politique de sécurité, gestion des risques, conformité réglementaire
- Sécurité Opérationnelle (SecOps) : Gestion des contrôles de sécurité, surveillance, détection et réponse aux incidents
- Architecture et Conseil : Conception des solutions sécurisées, revue des projets, accompagnement des métiers
- Ingénierie Sécurité : Implémentation et maintien des solutions de sécurité

- Tests et Évaluation : Audits, tests d'intrusion, exercices de simulation

Un plan d'évolution des effectifs prévoit un renforcement progressif de l'équipe pour atteindre 30 personnes d'ici 24 mois, avec le recrutement prioritaire de profils spécialisés en sécurité cloud, API et détection des menaces.

Comitologie et processus de décision

Instance	Fréquence	Participants	Objectifs
Conseil			
d'Administration	Annuelle	CA, DG, CRO, RSSI	Validation stratégie cyber, appétence au risque
Comité des Risques	Trimestrielle	Membres CA, DG, CRO, RSSI	Supervision risques cyber, validation
investissements majeurs			
COMEX Cyber	Trimestrielle	COMEX, RSSI	Pilotage exécutif, arbitrages stratégiques
COSEC	Mensuelle	RSSI, DSI, métiers,	
conformité	Suivi opérationnel, incidents, projets		

Comité de Crise Cyber Ad hoc Cellule de crise prédéfinie Gestion des incidents majeurs

Les décisions relatives à la sécurité suivent un processus d'escalade formalisé.

- Les décisions opérationnelles courantes sont prises au niveau du RSSI et de son équipe
- Les décisions impliquant plusieurs directions sont arbitrées en COSEC
- Les décisions stratégiques ou nécessitant des investissements importants sont escaladées au COMEX
- Les décisions affectant l'appétence au risque ou la stratégie globale sont soumises au Comité des Risques puis au CA

Gestion documentaire

La documentation de sécurité est structurée selon une hiérarchie à trois niveaux.

- Niveau 1 - Politique : La PSSI, document stratégique validé par le CA
- Niveau 2 - Directives : Documents thématiques précisant les exigences par domaine
- Niveau 3 - Procédures : Instructions techniques et opérationnelles détaillées

La gestion de cette documentation suit un cycle de vie rigoureux.

- Revue annuelle systématique de la PSSI
- Revue des directives au minimum tous les 18 mois
- Mise à jour des procédures en fonction des évolutions techniques
- Versioning formel avec traçabilité des modifications
- Processus d'approbation adapté au niveau documentaire
- Diffusion contrôlée via un référentiel documentaire centralisé

Gestion des exceptions

Neo Financia reconnaît que des exceptions temporaires à la PSSI peuvent être nécessaires dans certaines circonstances. Ces exceptions sont encadrées par un processus formel:

1. Soumission d'une demande d'exception documentée incluant :
   - Description de l'exception
   - Justification business
   - Évaluation des risques
   - Mesures compensatoires proposées
   - Durée prévue
2. Analyse et avis du RSS
3. Validation par le niveau approprié selon l'impact du risque
   - Risque modéré : COSEC
   - Risque élevé : Comité des Risques

   - Risque critique : Conseil d'Administration
   - Documentation et suivi centralisés des exceptions accordées
   - Revue périodique et clôture formelle à l'échéance

Toute exception dont la durée dépasse 12 mois doit faire l'objet d'un plan d'action pour revenir à la conformité

Mesure de la performance

Neo Financia mesure l'efficacité de son organisation et de ses processus de sécurité à travers un ensemble d'indicateurs clés de performance (KPIs):

Catégorie	Indicateurs	Cible	Fréquence
Gouvernance	- Taux de participation aux instances de gouvernance		
- Taux de réalisation du plan d'action sécurité			
- Niveau de maturité cybersécurité			
- ≥ 95%			

- ≥ 85%			
- 4.3/5 d'ici 24 mois			
Trimestrielle			
Opérationnel	- Délai moyen de correction des vulnérabilités critiques		
- Taux de couverture des contrôles de sécurité			
- Nombre d'incidents de sécurité			
- < 7 jours			
- ≥ 95%			
- Réduction annuelle de 20%			
Mensuelle			
Humain	- Taux de participation aux formations sécurité		
- Taux de clic aux campagnes de phishing simulé			
- Taux de signalement des incidents			
- ≥ 95%			
- < 5%			
- ≥ 95%			
Trimestrielle			
Technique	- Score de sécurité Azure		
- Taux de couverture du MFA			

- Conformité des configurations cloud			
- ≥ 95%			
- 100%			
- ≥ 95%			
Mensuelle			

Ces indicateurs font l'objet d'un reporting régulier aux différentes instances de gouvernance, avec des tableaux de bord adaptés au niveau de décision.

Organisation internationale

La fonction cybersécurité de Neo Financia est organisée selon un modèle centralisé, avec des adaptations pour les entités internationales:

- Le RSSI groupe définit la stratégie et les politiques globales

---

- Un correspondant local au Royaume-Uni assure la conformité aux exigences spécifiques post-Brexit
- Les équipes opérationnelles françaises et britanniques suivent les mêmes standards avec des ajustements aux contextes locaux
- Les incidents majeurs sont gérés de manière centralisée avec un reporting consolidé
- Des audits croisés entre entités garantissent la cohérence de l'approche sécurité

Cette organisation permet de concilier une gouvernance globale cohérente et des adaptations aux spécificités réglementaires locales.

Gestion des risques

Cadre méthodologique

Neo Financia applique une approche structurée et systématique de gestion des risques de sécurité de l'information alignée sur les standards reconnus et adaptée aux spécificités d'une néobanque européenne.

Référentiels méthodologiques adoptés :

- EBIOS Risk Manager 2023 pour l'analyse détaillée des risques cyber
- ISO 27005:2022 pour le cadre global de gestion des risques de sécurité
- NIST Cybersecurity Framework pour l'évaluation de la maturité et la gestion des contrôles
- BNR/RTS EBA pour les aspects spécifiques au secteur bancaire
- Approche MITRE ATT&CK pour la cartographie des menaces

Cette méthodologie garantit une approche holistique, tenant compte de l'ensemble des facteurs de risque, des contraintes réglementaires et des spécificités de notre environnement multicloud et transfrontalier.

Processus d'analyse de risques

Le processus d'analyse des risques de Neo Financia suit un cycle en 5 phases

1. Établissement du contexte

- Définition du périmètre d'analyse (systèmes, applications, processus)
- Identification des parties prenantes et de leurs enjeux
- Caractérisation de l'environnement réglementaire applicable
- Prise en compte des partenariats stratégiques (Mangopay, Lemonway)
- Analyse des dépendances critiques (services cloud, API)

2. Identification des risques

- Inventaire et valorisation des actifs (données, systèmes, services)
- Identification des menaces et vulnérabilités
- Cartographie des scénarios d'attaque pertinents
- Consultation des parties prenantes métier et techniques
- Exploitation des sources de renseignement sur les menaces (CTI)

3. Estimation des risques

- Évaluation de la vraisemblance des scénarios identifiés

- Évaluation des impacts potentiels (financiers, réglementaires, réputationnels, opérationnels)
- Prise en compte des contrôles existants et de leur efficacité
- Détermination du niveau de risque inhérent et résidue
- Priorisation des risques selon leur criticité

4. Traitement des risques

- Sélection des stratégies de traitement appropriées
- Définition de plans d'action détaillés
- Allocation des responsabilités et des ressources
- Planification de la mise en œuvre
- Validation par les instances de gouvernance

5. Suivi et révision

- Suivi de la mise en œuvre des plans d'action
- Mesure de l'efficacité des contrôles déployés
- Revue périodique des risques et adaptation des traitements
- Mise à jour de la cartographie des risques
- Reporting aux instances de gouvernance

Ce processus est appliqué de manière systématique selon le calendrier suivant.

- Analyse complète des risques cyber de l'organisation une fois par an
- Revue trimestrielle des risques critiques et majeurs en COSEC
- Analyse de risque spécifique pour tout nouveau projet ou changement significatif

- Évaluation des risques après un incident de sécurité majeur
- Actualisation en cas d'évolution significative du contexte (nouvelles menaces, acquisitions, etc.)

Critères d'évaluation des risques

L'évaluation des risques repose sur des critères formellement définis pour garantir la cohérence et la répétabilité des analyses.

Échelle de vraisemblance

Niveau	Valeur	Description	Fréquence estimée
5	Quasi certain	La menace est constante ou se produit très fréquemment	Plusieurs fois par mois
4	Probable	La menace est susceptible de se produire dans la plupart des circonstances	Plusieurs fois par an
3	Possible	La menace pourrait se produire à un moment donné	Une fois tous les 1-2 ans
2	Peu probable	La menace ne se produirait que dans des circonstances particulières	Une fois tous les 2-5 ans

---

Échelle d'impact

Niveau	Valeur	Impact financier	Impact réglementaire	Impact réputationnel	Impact opérationn
5	Catastrophique	> 10M€	Retrait d'agrément	Atteinte durable à l'image, couverture médiatique internationale	Arrêt complet de activités critiques 24h
4	Majeur	1-10M€	Sanctions significatives	Atteinte significative à l'image, couverture médiatique nationale	Arrêt partiel de activités critiques pendant 8- 24h
3	Modéré	100k€-1M€	Enquête réglementaire	Mécontentement d'un nombre significatif de clients	Dégradatio des servic pendant 4-
2	Mineur	10-100k€	Notification obligatoire	Mécontentement isolé de clients	Dégradatio mineure pendant 1-

1	Négligeable	< 10k€	Sans conséquence réglementaire	Pas d'impact externe perceptible	Impact opérationn non significat < 1h

Matrice de criticité

Impact ↓ Vraisemblance →	1 - Rare	2 - Peu probable	3 - Possible	4 - Probable	5 - Quasi certain
5 - Catastrophique	Élevé (5)	Élevé (10)	Critique (15)	Critique (20)	Critique (25)
4 - Majeur	Modéré (4)	Élevé (8)	Élevé (12)	Critique (16)	Critique (20)
3 - Modéré	Faible (3)	Modéré (6)	Élevé (9)	Élevé (12)	Élevé (15)
2 - Mineur	Faible (2)	Faible (4)	Modéré (6)	Modéré (8)	Élevé (10)
1 - Négligeable	Faible (1)	Faible (2)	Faible (3)	Faible (4)	Modéré (5)

Le niveau de criticité est obtenu en multipliant les scores de vraisemblance et d'impact :

- Critique (15-25) : Risque inacceptable nécessitant un traitement immédiat
- Élevé (8-14) : Risque significatif nécessitant un traitement prioritaire
- Modéré (5-7) : Risque à traiter dans le cadre du plan d'action annuel
- Faible (1-4) : Risque acceptable avec surveillance

Appétence au risque ## Cartographie des risques prioritaires

Neo Financia a formellement défini son appétence au risque cyber au niveau 3 sur 10, ce qui traduit une approche prudente, équilibrée par la nécessité d'innovation propre au modèle de néobanque. Cette appétence se décline en seuils d'acceptabilité par catégorie de risque :

Niveau de risque	Seuil d'acceptabilité	Autocité d'acceptation	Conditions d'acceptation
Critique (15-25)	Non acceptable	Conseil d'Administration	Traitement obligatoire, mesures d'urgence si nécessaire
Élevé (8-14)	Acceptable sous conditions	Comité des Risques	Plan de traitement obligatoire avec mesures compensatoires

Modéré (5-7)	Généralement acceptable	COSEC	Traitement selon rapport coût/bénéfice
Faible (1-4)	Acceptable	RSSI	Surveillance périodique

Cette appétence au risque est revue annuellement par le Conseil d'Administration et peut être ajustée en fonction de l'évolution du contexte.

Neo Financia a identifié les scénarios de risque suivants comme prioritaires

ID	Scénario de risque	Actifs concernés	Vraisemblance	Impact	Criticité	St
R1	Compromission des API Open Banking	API Gateway, services d'authentification	4	5	20 - Critique	Ré
R2	Exfiltration massive de données clients	Bases de données clients, stockage cloud	3	5	15 - Critique	Ré

R3	**Fraude par détournement des systèmes de paiement**	**Processus de paiement, intégrations Mangopay**	**4**	**4**	**16 - Critique**	**Réduire**
R4	Indisponibilité majeure des services bancaires en ligne	Infrastructure Azure (70%), front-end applicatif	3	4	12 - Élevé	Réduire + Transférer
R5	Attaque de la chaîne d'approvisionnement via fournisseurs	Fournisseurs critiques, partenaires fintech	3	4	12 - Élevé	Réduire
R6	Non-conformité réglementaire (DORA, NIS2, RGPD)	Processus, données personnelles	2	5	10 - Élevé	Réduire
R7	Compromission des postes de travail des collaborateurs	Endpoints, VPN, accès distants	4	3	12 - Élevé	Réduire
R8	Attaque ciblée par phishing sur les dirigeants	Comptes privilégiés, emails des dirigeants	4	4	16 - Élevé	Réduire
R9	Vol d'identifiants d'authentification des clients	Systèmes d'authentification, applications mobiles	4	4	16 - Élevé	Réduire

R10	Ransomware touchant l'infrastructure critique	Systèmes internes, serveurs, stockage	3	5	15- Élevé	Réduire + Transférer

Cette cartographie fait l'objet d'une revue trimestrielle en COSEC et est mise à jour en fonction de l'évolution des menaces, de l'efficacité des contrôles et des changements dans l'environnement de Neo Financia.

Stratégies de traitement des risques

Neo Financia applique les stratégies de traitement suivantes en fonction du niveau de risque et du contexte

- Contrôles préventifs (réduction de la vraisemblance)
- Contrôles détectifs (identification précoce)
- Contrôles correctifs (limitation de l'impact)
- Contrôles dissuasifs (découragement des acteurs malveillants)

- Assurance cyber (pour les risques assurables)
- Externalisation (avec contrôle adéquat du prestataire)
- Garanties contractuelles
- Abandon d'une technologie ou d'un service trop risqué
- Redéfinition du périmètre fonctionnel
- Architecture alternative
- Acceptation du risque résiduel après traitement
- Acceptation exceptionnelle et temporaire avec surveillance renforcée
- Documentation des justifications et validation par l'autocité appropriée

Le choix de la stratégie prend en compte les facteurs suivants

- Niveau de criticité du risque
- Rapport coût/efficacité des mesures de traitement
- Faisabilité technique et organisationnelle
- Impact sur les activités et l'expérience client
- Contraintes réglementaires applicables
- Appétence au risque définie

Suivi et reporting des risques

Neo Financia a mis en place un dispositif structuré de suivi et de reporting des risques cyber.

Outils et processus de suivi

- Outil GRC centralisé pour le suivi des risques et des plans d'action
- Tableaux de bord dynamiques avec indicateurs de risque en temps réel
- Suivi des métriques d'efficacité des contrôles
- Alertes automatiques en cas de dépassement des seuils
- Intégration avec les outils de surveillance technique (SIEM, CSPM)

Cadence de reporting

Instance	Fréquence	Contenu
Conseil d'Administration	Annuelle	Synthèse de haut niveau, risques critiques, tendances, investissements majeurs
Comité des Risques	Trimestrielle	Risques critiques et élevés, efficacité des mesures, évolutions significatives
COMEX	Trimestrielle	Tableau de bord exécutif, risques opérationnels, impacts business

---

COSEC	Mensuelle	Suivi détaillé de tous les risques, plans d'action, incidents
Équipe sécurité	Hebdomadaire	Suivi opérationnel, métriques techniques, alertes

Processus d'alerte et d'escalade

En cas d'évolution significative du niveau de risque ou d'émergence d'une nouvelle menace :

- Analyse initiale par l'équipe sécurité
- Notification immédiate au RSSI pour les risques critiques émergents
- Convocation d'un COSEC exceptionnel si nécessaire
- Escalade au COMEX pour les risques à fort impact business
- Information du Comité des Risques pour les risques systémiques

Intégration avec les autres processus

La gestion des risques cyber est intégrée aux autres processus de Neo Financia pour garantir une approche holistique.

Processus	Integration avec la gestion des risques cyber
Gestion de projets	- Analyse de risque obligatoire dès la phase de conception
- Validation sécurité aux jalons clés (Security Gate)	
- Intégration des contrôles de sécurité dans les livrables	
Gestion des changements	- Évaluation d'impact sécurité pour tout changement significatif
-	

Revue de sécurité avant mise en production	
- Test de non-régression des contrôles	
Gestion des fournisseurs	- Évaluation des risques tiers en amont de la contractualisation
- Clauses contractuelles de sécurité	
- Audit de sécurité périodique des fournisseurs critiques	
Conformité réglementaire	- Alignement des contrôles de sécurité avec les exigences réglementaires
- Partage des résultats d'analyse de risques avec les fonctions conformité	
- Coordination des reportings réglementaires	
Continuité d'activité	- Utilisation des scénarios de risque cyber pour les PCA/PRA
- Tests conjoints (cyber crisis, DR tests)	
- Stratégies de résilience coordonnées	

# Politique de sécurité des ressources humaines	

Principes fondamentaux

Neo Financia reconnaît que le facteur humain est à la fois un élément clé de la protection de ses actifs informationnels et une source potentielle de vulnérabilité. La politique de sécurité des ressources humaines vise à établir un cadre clair pour intégrer la sécurité de l'information à chaque étape du cycle de vie de l'emploi, de la phase de recrutement jusqu'au départ du collaborateur.

Objectifs de la politique RH-Sécurité :

- Garantir que tous les collaborateurs comprennent leurs responsabilités en matière de sécurité
- Réduire les risques d'erreur humaine, de vol, de fraude ou d'usage inapproprié des ressources
- S'assurer que les collaborateurs sont conscients des menaces et préparés à y répondre
- Promouvoir une culture de sécurité à tous les niveaux de l'organisation
- Protéger les intérêts de Neo Financia, de ses clients et de ses partenaires

Cette politique s'applique à l'ensemble des collaborateurs de Neo Financia (1000 personnes), quelle que soit leur localisation (Paris, Lyon, Londres), leur statut (CDI, CDD, alternants, stagiaires) ou leur niveau hiérarchique, ainsi qu'aux prestataires et consultants externes intervenant sur nos systèmes.

Mesures de sécurité avant l'embauche

Vérifications préalables

Avant tout recrutement, Neo Financia procède à des vérifications proportionnées à la sensibilité du poste concerné.

Niveau de sensibilité	Types de vérifications	Postes concernés
Standard	- Vérification d'identité	
- Vérification des diplômes et références professionnelles		
- Recherche de présence sur les réseaux sociaux professionnels		
Postes sans accès aux données sensibles ou systèmes critiques		

|Renforcé|-
Vérifications standard +

- Vérification des antécédents judiciaires (avec consentement)
- Enquête de solvabilité (avec consentement)
- Vérification approfondie des références

Postes avec accès à des données clients ou financières		
- Vérifications renforcées +		

- Évaluation de sécurité spécifique
- Enquête de réputation approfondie
- Vérification des conflits d'intérêts potentiels |Équipe de sécurité, administrateurs systèmes, développeurs d'applications critiques, dirigeants|

Ces vérifications sont réalisées dans le strict respect des lois applicables en matière de protection des données et d'emploi, avec le consentement explicite des candidats.

Termes et conditions d'emploi

Les contrats de travail et documents associés incluent systématiquement

- Des clauses de confidentialité et de non-divulgation
- Une mention explicite des responsabilités en matière de sécurité de l'information
- Les conséquences du non-respect de la politique de sécurité
- Les droits de propriété intellectuelle
- Les règles d'utilisation des ressources informatiques
- L'engagement à respecter la PSSI et les procédures associées

Chaque nouveau collaborateur doit prendre connaissance et accepter formellement ces dispositions avant sa prise de fonction.

Mesures pendant la période d'emploi

Responsabilités de la direction

La direction de Neo Financia s'engage à

- Communiquer clairement les attentes en matière de sécurité à tous les collaborateurs
- Veiller à l'application cohérente des politiques et procédures de sécurité
- Montrer l'exemple en matière de respect des règles de sécurité
- Allouer les ressources nécessaires aux programmes de sensibilisation et de formation
- Reconnaître et valoriser les comportements exemplaires en matière de sécurité
- Intégrer les critères de sécurité dans l'évaluation des performances

---

Sensibilisation, éducation et formation à la sécurité

Neo Financia déploie un programme complet de sensibilisation et de formation adapté aux différents profils

Type	Contenu	Format	Fréquence	Public
Sensibilisation de base	- Principes fondamentaux de sécurité			
- Politiques et procédures internes				
- Gestion des mots de passe				
- Reconnaissance du phishing				
- Manipulation sécurisée des données				
- Signalement des incidents				
E-learning, vidéos, newsletters, affiches	Onboarding + Rafraîchissement annuel	Tous les collaborateurs		
Formation spécifique par rôle	- Risques spécifiques au métier			
- Bonnes pratiques sectocielles				
- Étude de cas adaptés				
- Manipulation des données sensibles				
Ateliers, webinaires, formation présentielle	Semestrielle	Par département (Finance, RH, Service client)		
Formation	-			

technique avancée	Développement sécurisé			
- Administration système sécurisée				
- Gestion des incidents				
- Analyse des menaces				
Formations certifiantes, ateliers pratiques, labs	Selon besoins et évolutions technologiques	Équipes IT, Développement, Sécurité		

|Sensibilisation dirigeants|-
Enjeux stratégiques de la sécurité

- Gouvernance et conformité
- Gestion de crise cyber
- Risques spécifiques aux dirigeants

Sessions exécutives, simulations de crise	**Annuelle**	**COMEX, Conseil d'Administration**		
Exercices pratiques	- Campagnes de phishing simulé			

- Exercices de détection d'incidents
- Simulations d'ingénierie sociale |Mises en situation réelles|Trimestrielle|
  Échantillon représentatif, rotation sur l'ensemble des collaborateurs|

L'efficacité du programme est mesurée à travers :

- Taux de participation (objectif : ≥95%)
- Scores aux évaluations post-formation (objectif : ≥80%)
- Taux de clic aux campagnes de phishing simulé (objectif : <5%)
- Enquêtes de perception et de connaissance

Processus disciplinaire

Neo Financia a établi un processus disciplinaire formel et équitable pour traiter les violations de sécurité

1. Approche progressive

- Premier incident mineur : sensibilisation et rappel des règles
- Récidive ou incident plus grave : avertissement formel
- Violations répétées ou graves : mesures disciplinaires selon la convention collective
- Violations délibérées avec intention malveillante : sanctions sévères pouvant aller jusqu'au licenciement et poursuites judiciaires

2. Facteurs pris en compte

- Intention (erreur vs malveillance)
- Impact de la violation
- Historique du collaborateur
- Niveau de sensibilisation préalable
- Circonstances atténuantes ou aggravantes

---

3. Processus équitable :

- Investigation factuelle et documentée
- Droit d'explication du collaborateur
- Confidentialité de la procédure
- Validation par les RH et la direction juridique
- Application cohérente des sanctions

Ce processus est communiqué à tous les collaborateurs et rappelé lors des sessions de sensibilisation.

Mesures à la fin ou au changement d'emploi

Responsabilités liées à la cessation ou au changement d'emploi

Neo Financia applique une procédure formalisée pour gérer la sécurité lors des départs ou changements de poste.

Étape	Actions	Responsable	Délai
Notification de départ/changement	- Information au RSSI et à la DSI		
- Planification du processus de transition			
- Identification des accès à révoquer/modifier			
Responsable hiérarchique + RH	Dès connaissance du départ/changement		

Transfert des responsabilités	- Documentation des connaissances et procédures		
- Transmission des dossiers en cours			
- Formation du remplaçant si applicable			
Collaborateur + Manager	Pendant la période de préavis		
Restitution des actifs	- Récupération de tous les équipements (ordinateur, téléphone, badges)		
- Récupération des supports de stockage et documents			
- Vérification de l'inventaire			
IT + Manager	Dernier jour de présence		
Révocation des accès	- Désactivation des comptes utilisateurs		
- Révocation des certificats et tokens			
DSI	Dans les 4h suivant le départ effectif		

|Entretien de sortie|-
Modification des mots de passe partagés

- Désactivation des accès physiques

- Rappel des obligations de confidentialité post-emploi			

- Signature de l'attestation de fin de responsabilité
- Information sur les sanctions en cas de violation |RH + Juridique|Dernier jour|

|Suivi post-départ|-
Surveillance des accès et activités suspectes

- Vérification de la conformité avec les accords de non-divulgation |Sécurité + Juridique|3-6 mois après le départ|

En cas de départ à risque (licenciement conflictuel, départ vers un concurrent), des mesures de sécurité renforcées sont mises en place:

- Révocation immédiate des accès sensibles
- Escorte durant la période de préavis si maintenue
- Analyse forensique des équipements
- Surveillance renforcée des activités système
- Activation du plan de surveillance post-départ

Gestion des accès et privilèges

Principe du moindre privilège

Neo Financia applique strictement le principe du moindre privilège pour tous les collaborateurs.

- Attribution des droits strictement nécessaires à l'exercice des fonctions
- Séparation des environnements (développement, test, production)
- Privilèges temporaires pour les interventions ponctuelles
- Interdiction du partage de comptes et d'identifiants
- Revue périodique des droits (trimestrielle pour les accès critiques)
- Traçabilité de toutes les actions privilégiées

Gestion des comptes à privilèges élevés

Les comptes administratifs et à hauts privilèges font l'objet de mesures de sécurité renforcées :

- Attribution nominative et individuelle des droits
- Authentification forte multi-facteurs obligatoire
- Durée de session limitée avec déconnexion automatique
- Journalisation exhaustive des actions
- Révision mensuelle des droits par le RSSI
- Procédure formelle d'attribution et de révocation
- Audit trimestriel des actions privilégiées

Télétravail et travail mobile

Neo Financia encadre les pratiques de télétravail et de mobilité pour préserver la sécurité de ses systèmes

Politique de télétravail

- Limitation du télétravail aux collaborateurs formés aux risques spécifiques
- Signature obligatoire de la charte de télétravail sécurisé
- Utilisation exclusive des équipements fournis par Neo Financia

- Connexion systématique via VPN sécurisé avec authentification forte
- Interdiction de connexion depuis des réseaux publics non sécurisés
- Verrouillage automatique après inactivité
- Restrictions sur l'impression et le stockage local de documents
- Respect des règles de confidentialité dans l'environnement domestique

Équipements mobiles

- Chiffrement intégral des disques sur tous les équipements mobiles
- Déploiement d'une solution MDM (Mobile Device Management)
- Capacité d'effacement à distance en cas de perte ou vol
- Protection contre les malwares mobiles
- Mise à jour automatique des systèmes et applications
- Conteneurisation des données professionnelles
- Restrictions sur les applications installables
- Procédure de déclaration de perte ou vol sous 24h

Règles absolues en télétravail :

- Ne jamais laisser un équipement professionnel sans surveillance dans un lieu public
- Ne jamais contourner les mécanismes de sécurité (VPN, antivirus, MDM)
- Ne jamais connecter de périphérique non autocisé aux équipements professionnels
- Signaler immédiatement toute anomalie ou suspicion de compromission
- Ne jamais permettre l'utilisation des équipements professionnels par des tiers

Engagement des tiers

Neo Financia étend ses exigences de sécurité aux tiers intervenant sur ses systèmes d'information.

Catégories de tiers concernés

- Prestataires de services IT
- Consultants
- Auditeurs
- Développeurs externes
- Personnel de maintenance
- Partenaires fintech (Mangopay, Lemonway)

Mesures de sécurité appliquées

- Clauses contractuelles détaillant les exigences de sécurité
- Annexe de sécurité adaptée au niveau de sensibilité de la prestation
- Signature d'accords de confidentialité renforcés
- Vérification des antécédents pour les intervenants sur systèmes critiques
- Formation de sensibilisation obligatoire avant intervention
- Attribution des accès selon le principe du moindre privilège
- Supervision des activités pendant les interventions sensibles
- Révocation immédiate des accès à la fin de la mission

Un processus d'escalade spécifique est défini pour gérer les incidents de sécurité impliquant des tiers, avec une chaîne de responsabilité clairement établie.

Gestion des actifs informationnels

Principes généraux

La gestion efficace des actifs informationnels constitue un fondement essentiel de la sécurité des systèmes d'information de Neo Financia. Cette approche structurée permet d'identifier, de classifier et de protéger l'ensemble des ressources informationnelles selon leur criticité et leur sensibilité.

Objectifs de la gestion des actifs informationnels :

- Recenser exhaustivement les actifs informationnels de l'entreprise
- Attribuer clairement la propriété et les responsabilités pour chaque actil
- Classifier les actifs selon leur sensibilité et leur importance
- Mettre en œuvre des mesures de protection proportionnées à la valeur des actifs
- Garantir la traçabilité du cycle de vie complet des actifs
- Assurer une utilisation conforme aux exigences légales et réglementaires

Cette politique s'applique à l'ensemble des actifs informationnels de Neo Financia, qu'ils soient numériques, physiques ou organisationnels, et concerne tous les collaborateurs, prestataires et partenaires ayant accès à ces actifs.

Inventaire des actifs

Périmètre de l'inventaire

Neo Financia maintient un inventaire exhaustif et à jour de tous ses actifs informationnels, regroupés dans les catégories suivantes :

Catégorie	Description	Exemples
Actifs d'information	Données et informations sous toutes leurs formes	Données clients, données financières, contrats, documentation, politiques
Actifs logiciels	Applications, systèmes et logiciels	Systèmes bancaires core, applications mobiles, APIs, middleware, systèmes d'exploitation
Actifs physiques	Équipements informatiques matériels	Serveurs, postes de travail, équipements réseau, périphériques de stockage, équipements mobiles
Services	Services internes ou	Services cloud (Azure, AWS, OVHcloud),

	externes supportant les activités	télécommunications, services managés
Personnel	Ressources humaines avec compétences critiques	Administrateurs systèmes, experts sécurité, développeurs clés
Sites et infrastructures	Locaux et installations physiques	Datacenters, locaux techniques, bureaux (Paris, Lyon, Londres)
Infrastructure immatérielle	Structure organisationnelle et intangible	Réputation, image de marque, propriété intellectuelle, processus

Processus d'inventaire

L'inventaire des actifs est réalisé selon un processus formalisé.

- Identification : Recensement systématique de tous les actifs par les responsables des différents domaines
- Enregistrement : Documentation dans l'outil centralisé de gestion des actifs (CMDB)
- Validation : Vérification de l'exhaustivité et de l'exactitude par les propriétaires d'actifs
- Mise à jour : Actualisation continue pour refléter les changements (acquisitions, mises hors service)
- Audit : Vérification périodique de la cohérence entre l'inventaire et la réalité

Des outils automatisés de découverte et de suivi sont déployés pour maintenir l'inventaire à jour

- Scanning réseau pour les actifs connectés
- Intégration avec les outils de gestion de parc
- Découverte automatique des ressources cloud
- Réconciliation avec les processus d'achat et de décommissionnement

L'inventaire complet est revu formellement au moins une fois par an, et l'inventaire des actifs critiques est vérifié trimestriellement.

Propriété des actifs

Chaque actif informationnel est placé sous la responsabilité d'un propriétaire clairement identifié.

Rôles et responsabilités

Rôle	Responsabilités
Propriétaire fonctionnel	-

	Définir la classification de l'actif
- Déterminer les règles d'accès et d'usage	
- Valider les droits d'accès	
- S'assurer de la conformité réglementaire	
- Effectuer les revues périodiques	
Propriétaire technique	- Assurer la maintenance opérationnelle
- Mettre en œuvre les contrôles de sécurité	
- Gérer les sauvegardes et la restauration	
- Appliquer les correctifs de sécurité	
- Superviser les performances et la disponibilité	
Custodien des données	- Garantir l'intégrité et la qualité des données
- Mettre en œuvre les règles de rétention	
- Gérer les processus d'anonymisation/pseudonymisation	
- Superviser les traitements de données	
Utilisateur	- Utiliser l'actif conformément aux politiques
- Signaler les incidents ou anomalies	
- Respecter les règles de confidentialité	
- Appliquer les mesures de protection	

définies	

L'attribution de la propriété des actifs est formalisée et documentée dans l'inventaire, avec :

- Identification claire du propriétaire fonctionnel (nom, fonction)
- Désignation du propriétaire technique
- Procédure de transfert de propriété en cas de changement organisationnel
- Maintien d'une matrice RACI pour les actifs partagés

Classification de l'information

Neo Financia a défini un schéma de classification des informations pour déterminer le niveau de protection approprié

Niveaux de classification

Niveau	Description	Exemples	Contrôles requis
P0 - Public	Information destinée à être diffusée publiquement	Brochures produits, tarifs, communiqués de presse, conditions générales	- Contrôle d'intégrité
- Validation avant publication			
P1 - Interne	Information à usage interne uniquement	Procédures internes, annuaire, communications générales, formations	- Accès réservé aux collaborateurs
- Authentification simple			
- Pas de partage externe sans autocisation			
P2 - Confidentiel	Information sensible à accès restreint	Données clients, stratégies commerciales, rapports financiers internes	- Accès strictement contrôlé (need-to-know)

- Chiffrement en transit			
- Traçabilité des accès			
- Partage externe formellement approuvé			
P3 - Critique	Information hautement sensible et réglementée	Données d'authentification, clés cryptographiques, code source des applications critiques, plans stratégiques	- Chiffrement au repos et en transit
- Authentification forte multi-facteurs			
- Audit détaillé de tous les accès			
- Interdiction de stockage sur terminaux mobiles			
- Cloisonnement physique/logique			

Procédure de classification

- Classification initiale : Effectuée par le créateur/propriétaire de l'information
- Validation : Confirmation par le propriétaire fonctionnel ou responsable hiérarchique
- Marquage : Étiquetage visible de la classification (en-tête/pied de page, métadonnées`
- Marquage
- Révision : Réévaluation périodique ou lors de changements significatifs

---

La classification est appliquée de manière cohérente sur tous les supports (documents électroniques, emails, documents papier) avec des outils de classification automatique déployés pour faciliter le processus.

Règles de manipulation par niveau

P0 - Public

- Aucune restriction de diffusion
- Validation obligatoire par la Communication avant publication externe

P1 - Interne

- Circulation libre en interne
- Stockage sur les espaces collaboratifs internes
- Impression autocisée sans restrictior
- Partage externe uniquement avec NDA

P2 - Confidentiel

- Accès limité aux personnes autocisées
- Stockage dans des espaces sécurisés
- Chiffrement obligatoire pour l'envoi externe
- Impression sécurisée (récupération par code)
- Destruction sécurisée en fin de vie

P3 - Critique

- Accès sur justification uniquement avec validation
- Stockage dans des systèmes haute sécurité
- Interdiction d'envoi par email standarc
- Traçabilité exhaustive des consultations
- Impression limitée et contrôlée
- Transfert uniquement via canaux sécurisés

Utilisation acceptable des actifs

Neo Financia définit les règles d'utilisation acceptable pour l'ensemble de ses actifs informationnels :

Principes généraux

- Utilisation des actifs exclusivement pour des finalités professionnelles
- Interdiction d'utiliser les ressources pour des activités illégales ou contraires à l'éthique
- Respect de la confidentialité des informations traitées
- Obligation de signaler toute utilisation inappropriée constatée
- Présomption de propriété de Neo Financia sur les données traitées

Règles spécifiques par type d'actif

Type d'actif	Règles d'utilisation
Postes de travail	- Installation de logiciels limitée aux applications approuvées
- Verrouillage obligatoire en cas d'absence	

- Interdiction de désactiver les mécanismes de sécurité	
- Usage personnel toléré dans des limites raisonnables	
Équipements mobiles	- Protection physique en tout temps
- Interdiction de les laisser sans surveillance dans des lieux publics	
- Chiffrement obligatoire des données	
- Connexion uniquement aux réseaux approuvés ou via VPN	
Ressources réseau	- Interdiction de connecter des équipements non autocisés
- Utilisation de la bande passante de manière responsable	
- Interdiction de contourner les restrictions d'accès	
- Supervision des communications à des fins de sécurité	
Applications et données	- Accès limité aux fonctionnalités nécessaires aux activités
- Interdiction d'extraction massive sans autocisation	
- Protection des identifiants et mots de passe	
- Respect des procédures de sauvegarde	
Environnements cloud	-

	Utilisation des services validés par la sécurité
- Respect des architectures de référence	
- Surveillance des coûts et des ressources	
- Application des principes de moindre privilège	
Supports amovibles	- Usage restreint aux besoins métier validés
- Chiffrement obligatoire pour les données confidentielles	
- Inventaire et traçabilité des supports sensibles	
- Destruction sécurisée en fin de vie	

Ces règles sont formalisées dans la Charte d'utilisation des ressources informatiques, signée par chaque collaborateur et revue annuellement.

Gestion des médias et supports

Gestion des supports amovibles

Neo Financia encadre strictement l'utilisation des supports amovibles (clés USB, disques externes, cartes mémoire)

- Inventaire centralisé des supports autocisés
- Utilisation exclusive de supports chiffrés et validés par la sécurité
- Attribution nominative et traçabilité
- Restriction technique des ports USB sur les postes sensibles
- Scan antivirus automatique lors de la connexior
- Procédure formelle de prêt et de retour

Transfert des supports physiques

Le transport de supports contenant des informations sensibles est soumis à des règles strictes.

Classification	Mesures de protection pour le

	transport
P1 - Interne	- Transport en conteneur fermé
- Inventaire des supports transportés	
P2 - Confidentiel	- Chiffrement des données
- Transport en conteneur sécurisé	
- Traçabilité du transport	
- Envoi et réception par personne autocisée	
P3 - Critique	- Chiffrement renforcé
- Transport par coursier sécurisé	
- Double validation à la réception	
- Notification de remise	
- Transport par deux personnes pour les actifs les plus critiques	

Mise au rebut sécurisée

La mise au rebut des supports de stockage suit une procédure rigoureuse :

- 1. Identification : Recensement des supports à détruire
- 2. Évaluation : Détermination du niveau de sensibilité des données
- 3. Effacement sécurisé : Application des méthodes appropriées selon la sensibilité
- P1 : Formatage standard
- P2 : Effacement sécurisé multi-passes (DoD 5220.22-M`
- P3 : Effacement sécurisé renforcé et destruction physique
- 4. Destruction physique : Pour les supports critiques ou non-effaçables
- 5. Documentation : Certificat de destruction avec traçabilité

- 6. Audit : Vérification périodique des processus

La destruction physique est réalisée par un prestataire certifié, avec émission d'un certificat de destruction conforme aux exigences réglementaires.

Gestion des documents papier

Malgré sa nature digitale, Neo Financia maintient des procédures pour la gestion des documents papier.

- Politique d'impression sécurisée (libération par badge)
- Marquage visible de la classification sur tous les documents
- Rangement sécurisé (armoires fermées à clé pour P2, coffres pour P3)
- Règle du "bureau propre" imposée à tous les collaborateurs
- Destruction par broyeur sécurisé selon le niveau de classification
- Audit régulier des zones d'impression et de stockage

Gestion du cycle de vie des actifs

Neo Financia gère l'ensemble du cycle de vie de ses actifs informationnels, de l'acquisition à la mise hors service

Acquisition et développement

- Processus formel d'évaluation et de validation
- Intégration des exigences de sécurité dans les cahiers des charges
- Évaluation préalable des risques pour les actifs critiques
- Validation par la sécurité avant mise en production
- Documentation complète des caractéristiques et configurations

Déploiement et utilisation

- Procédure de mise en service documentée
- Configuration selon les standards de sécurité
- Enregistrement dans l'inventaire
- Attribution formelle au propriétaire
- Formation des utilisateurs si nécessaire

Maintenance et évolution

- Plan de maintenance préventive
- Gestion des correctifs de sécurité
- Procédure formelle de gestion des changements
- Tests de non-régression
- Mise à jour de la documentation

Mise hors service

- Procédure formelle de décommissionnement
- Récupération des données avant mise hors service
- Effacement sécurisé des données sensibles

- Révocation des certificats et identifiants
- Mise à jour de l'inventaire
- Respect des obligations légales d'archivage

- Réaffectation ou élimination écologique

Toutes les phases du cycle de vie sont documentées et font l'objet d'une traçabilité complète, notamment pour les actifs critiques.

Retour des actifs

Neo Financia a mis en place une procédure formelle pour le retour des actifs

Circonstances de retour

- Fin de contrat de travail
- Changement de fonction
- Absence prolongée
- Fin de mission pour les prestataires
- Remplacement ou mise à niveau de l'équipement

Processus de retour

- Notification : Information préalable de la DSI (minimum 48h avant pour les départs)
- Préparation : Sauvegarde des données professionnelles par l'utilisateur
- Inventaire : Vérification des actifs à restituer à l'aide de la liste d'attribution
- Remise : Remise en main propre à un représentant IT habilité
- Contrôle : Vérification de l'état et de l'intégrité des actifs
- Décharge : Signature d'un document attestant de la restitution complète
- Traitement : Réinitialisation, effacement des données ou mise en quarantaine selon les cas

Cette procédure est soutenue par des outils de gestion automatisée du parc informatique et par un processus d'intégration avec les systèmes RH pour anticiper les départs.

Responsabilités et sanctions

- Engagement contractuel de restitution dans les contrats de travail
- Responsabilité financière en cas de dommage ou de non-restitution
- Suivi des litiges par le service juridique
- Procédure d'escalade en cas de non-retour (blocage des accès, suspension de solde de tout compte)
- Procédure spéciale pour les départs conflictuels

Cloud Asset Management

Neo Financia applique des mesures spécifiques pour la gestion des actifs hébergés dans ses environnements cloud (Azure 70%, OVHcloud 20%, AWS 10%):

Gouvernance spécifique cloud

- Cadre d'architecture cloud validé par la sécurité

- Tagging obligatoire des ressources (propriétaire, environnement, classification)
- Surveillance automatisée des configurations (CSPM)
- Contrôles de conformité intégrés (policy-as-code)
- Gouvernance des identités cloud centralisée

Inventaire Cloud

- Découverte automatisée et continue des ressources cloud
- Intégration dans la CMDB globale
- Alertes sur les ressources non conformes
- Rapports de drift par rapport à l'infrastructure définie
- Cartographie des dépendances entre services cloud

Règles spécifiques

- Approbation obligatoire pour les déploiements dans le cloud public
- Définition des données autocisées par type de cloud (souverain vs public)
- Mécanismes d'autodestruction pour les ressources temporaires
- Surveillance des coûts et optimisation des ressources
- Gestion spécifique des backups cross-cloud
- Réversibilité planifiée pour les services critiques

Contrôle d'accès et gestion des identités

Principes fondamentaux

Le contrôle d'accès et la gestion des identités constituent un pilier essentiel de la sécurité des systèmes d'information de Neo Financia. Cette politique établit les règles et processus permettant de garantir que seules les personnes dûment autocisées accèdent aux ressources informationnelles, en fonction de leurs besoins professionnels légitimes.

Principes directeurs :

- Moindre privilège : Attribution des droits d'accès strictement nécessaires à l'exercice des fonctions
- Besoin d'en connaître : Accès aux informations uniquement si nécessaire aux missions
- Séparation des tâches : Distribution des responsabilités pour prévenir les abus
- Défense en profondeur : Mise en place de contrôles complémentaires et multiples
- Traçabilité : Enregistrement et analyse de toutes les actions d'accès

Cette politique s'applique à l'ensemble des utilisateurs (collaborateurs, prestataires, partenaires) et à tous les systèmes d'information de Neo Financia, qu'ils soient sur site ou hébergés dans le cloud.

Politique de gestion des accès

Processus de gestion des accès

Neo Financia a mis en place un processus formel de gestion des accès couvrant l'ensemble du cycle de vie.

1. Demande d'accès

- Formulaire standardisé précisant les accès requis
- Justification business du besoin
- Spécification de la durée (permanente ou temporaire)
- Classification d'usage (normal ou privilégié)

2. Validation

- Approbation par le responsable hiérarchique
- Validation par le propriétaire de la ressource
- Contrôle de conformité par la sécurité pour les accès sensibles
- Workflow d'approbation à plusieurs niveaux selon la sensibilité

3. Provisionnement

- Création ou modification des droits par l'équipe habilitée
- Mise en œuvre selon le principe du moindre privilège
- Documentation des accès accordés
- Notification à l'utilisateur et aux approbateurs

4. Revue périodique

- Revue trimestrielle des accès critiques
- Revue semestrielle des accès standard
- Certification formelle par les propriétaires
- Audit des anomalies et écarts

5. Modification et révocation

- Processus de changement formalisé
- Révocation immédiate lors des départs (<4h)
- Ajustement automatique lors des changements de fonction
- Expiration automatique des accès temporaires

Attribution des droits d'accès

L'attribution des droits d'accès est basée sur plusieurs approches complémentaires.

Approche	Description	Application
RBAC (Role-Based Access Control)	Droits basés sur des rôles prédéfinis liés aux fonctions	Applications métier, systèmes généraux
ABAC (Attribute-Based Access Control)	Droits basés sur les attributs de l'utilisateur, de la ressource et du contexte	Systèmes cloud, APIs, applications critiques
Modèles de profils	Ensembles de droits standardisés pour certaines fonctions	Onboarding, fonctions standard

Accès Just-In-Time	Élévation temporaire de privilèges avec approbation	Accès administratifs, opérations sensibles

---

Neo Financia maintient une matrice de droits d'accès documentant les autocisations standard par fonction, avec

- Cartographie des profils d'accès par département
- Définition claire des accès standards vs exceptionnels
- Règles d'escalade pour les demandes non-standard
- Procédure de validation des exceptions

Gestion des accès privilégiés

Les accès privilégiés (administratifs, super-utilisateurs) font l'objet de mesures de sécurité renforcées

- Solution PAM (Privileged Access Management) dédiée
- Attribution nominative de tous les accès privilégiés
- Principe de "break-glass" pour les accès d'urgence
- Sessions administratives enregistrées et journalisées
- Durée de validité limitée (maximum 4h) avec renouvellement explicite
- Authentification multi-facteurs obligatoire
- Workflow d'approbation spécifique par le RSSI pour les accès les plus sensibles
- Audit trimestriel des comptes privilégiés et des accès

Séparation des environnements

Neo Financia applique une stricte séparation des environnements

Environnement	Principes d'accès
Production	- Accès restreint aux équipes opérationnelles
- Validation à plusieurs niveaux	
- Double contrôle pour les modifications	
- Surveillance renforcée	
Pré-production	- Accès limité aux équipes IT et testeurs
- Données de production anonymisées	
-	

Traçabilité des accès	
Test/Recette	- Accès aux équipes projet et métier concernées
- Utilisation de jeux de données fictifs	
- Séparation des responsabilités développement/test	
Développement	- Accès aux développeurs et intégrateurs
- Interdiction d'utiliser des données réelles	

- Contrôle de code avant promotion	

Des mécanismes techniques empêchent les connexions croisées entre environnements sans autorisation explicite, avec.

- Segmentation réseau stricte
- Identités et comptes distincts par environnement
- Processus de promotion de code formalisé
- Contrôles de flux unidirectionnels

Gestion des identités

Cycle de vie des identités

Neo Financia gère les identités numériques selon un processus formalisé couvrant l'ensemble du cycle de vie

Phase	Processus	Responsable
Création	- Vérification de l'identité physique	
- Création dans le référentiel central (AD/IAM)		
- Attribution des attributs et affiliations		

- Documentation complète de l'identité		
IAM Team + RH		
Activation	- Procédure d'onboarding sécurisée	
- Authentification initiale face-à-face		
- Définition du mot de passe initial sécurisé		
- Enrôlement des facteurs d'authentification		
IAM Team + IT Support		
Maintien	- Synchronisation avec le SIRH	
- Mise à jour lors des changements de fonction		
- Gestion des suspensions temporaires		
- Renouvellement des certifications		
IAM Team + RH		
Désactivation	- Suspension immédiate à la fin du contrat	
- Révocation des certificats et sessions		
- Conservation de l'identité pour audit		
- Transfert des données professionnelles		
IAM Team + RH		

Suppression	- Archivage des informations d'audit	
IAM Team + DPO		

- Suppression définitive après période légale
- Attestation de suppression

Ce processus est largement automatisé grâce à l'intégration entre les systèmes RH et la plateforme IAM, garantissant cohérence et promptitude des actions sur les identités.

Fédération d'identité et Single Sign-On

Neo Financia a mis en place une architecture de fédération d'identité pour simplifier et sécuriser les accès

- Solution IAM centralisée comme source d'autocité
- Implémentation SSO sur l'ensemble des applications compatibles
- Fédération avec les environnements cloud (Azure AD, AWS IAM, OVHcloud)
- Support des protocoles standards (SAML 2.0, OAuth 2.0/OIDC)
- Authentification contextuelle basée sur le risque
- Provisionnement automatique via SCIM vers les applications SaaS
- Gouvernance des identités cross-plateforme

Avantages de l'approche IAM centralisée :

- Simplification de l'expérience utilisateur (authentification unique)
- Réduction de la surface d'attaque (moins de mots de passe)
- Cohérence des autocisations à travers les systèmes
- Révocation centralisée et immédiate des accès
- Visibilité complète sur l'ensemble des identités et accès
- Application uniforme des politiques de sécurité

Authentification forte et MFA

Neo Financia déploie une stratégie d'authentification forte à plusieurs facteurs :

Niveau de risque	Méthodes d'authentification	Applications concernées
Standard	Mot de passe complexe + second facteur pour première connexion ou nouvel appareil	Applications bureautiques, intranet, outils collaboratifs
Élevé	Mot de passe + second facteur systématique (TOTP, push notification)	VPN, applications métier, données client standard
Critique	Authentification multi-facteurs forte (cryptographique) + validation contextuelle	Administration systèmes, applications financières, données PCI-DSS

Les facteurs d'authentification déployés comprennent :

- Quelque chose que l'utilisateur connaît (mot de passe, code PIN)
- Quelque chose que l'utilisateur possède (token FIDO2, application mobile, certificat)
- Quelque chose que l'utilisateur est (biométrie sur appareils personnels)
- Analyse contextuelle (localisation, appareil, comportement)

L'authentification est renforcée par des contrôles additionnels

- Détection des anomalies de connexion
- Limitation des tentatives d'authentification
- Verrouillage progressif en cas d'échecs répétés
- Alertes sur les comportements de connexion inhabituels
- Re-authentification pour les opérations sensibles

Gestion des mots de passe

Neo Financia applique une politique de mots de passe robuste, alignée sur les recommandations NIST SP 800-63B

- Longueur minimale de 12 caractères pour les comptes standard
- Longueur minimale de 16 caractères pour les comptes privilégiés
- Complexité requise (combinaison de caractères variés)
- Vérification contre les dictionnaires et les mots de passe compromis
- Pas de changement périodique obligatoire, mais changement en cas de doute
- Histocique des mots de passe (10 derniers) pour éviter la réutilisation
- Utilisation d'un gestionnaire de mots de passe d'entreprise
- Stockage sécurisé (hachage salé utilisant des algorithmes reconnus)

Règles absolues concernant les mots de passe :

- Interdiction formelle de partager les mots de passe
- Interdiction de réutiliser les mots de passe professionnels pour des comptes personnels
- Interdiction de stocker les mots de passe en clair
- Obligation de signaler immédiatement tout soupçon de compromission
- Utilisation de mots de passe uniques pour chaque système non fédéré

Contrôle d'accès réseau

Segmentation réseau

Neo Financia a mis en place une architecture réseau segmentée pour isoler les différents environnements et limiter la propagation des menaces:

- Architecture en zones de sécurité distinctes
- Séparation physique et logique des environnements critiques
- Micro-segmentation pour les applications sensibles
- Filtrage de trafic inter-zones basé sur le principe du moindre privilège
- DMZ dédiée pour les services exposés

- Segmentation des environnements cloud via VNet/VPC isolés

- VLAN dédiés aux systèmes de même niveau de sensibilité

Le trafic entre zones est strictement contrôlé.

- Pare-feu nouvelle génération avec inspection approfondie
- Règles de filtrage documentées et révisées régulièrement
- Monitocing continu des flux inter-zones
- Détection des anomalies de trafic
- Architecture "zero-trust" pour les applications critiques

Accès distants sécurisés

Neo Financia sécurise les accès distants à ses systèmes d'information via

- Solution VPN sécurisée avec authentification forte obligatoire
- Vérification de l'état de sécurité des postes avant connexion
- Tunnels chiffrés de bout en bout (TLS 1.3 minimum)
- Segmentation des accès VPN selon les profils utilisateurs
- Limitation des plages horaires d'accès pour les fonctions sensibles
- Enregistrement détaillé des sessions d'accès distant
- Déconnexion automatique après inactivité (30 minutes maximum)
- Solution d'accès privilégié "zero trust" pour les administrateurs

Les accès distants font l'objet d'une surveillance renforcée.

- Monitocing en temps réel des connexions
- Détection des anomalies géographiques ou temporelles
- Limitation du nombre de sessions simultanées
- Audit régulier des journaux de connexior
- Tests d'intrusion spécifiques sur les accès distants

Contrôle d'accès Wi-Fi

Néo Financia applique une politique stricte pour ses réseaux sans fil.

Réseau	Utilisateurs	Contrôles
Wi-Fi Corporate	Collaborateurs avec équipements gérés	- Authentification 802.1X/EAP-TLS
- Chiffrement WPA3-Enterprise		
- Certificats machine		
- Intégration à l'IAM central		
Wi-Fi BYOD	Collaborateurs avec appareils personnels	- Authentification par portail captif avec MFA
- Accès limité à Internet et		

services non-critiques		

Wi-Fi Invités	Visiteurs, prestataires occasionnels	- Isolation des clients
- Inspection du trafic sortant		
---	---	---
	- Accès uniquement à Internet	
- Isolation totale du Sl interne		
- Validation par sponsor interne		
- Durée limitée (1 journée maximum)		

Des mesures complémentaires sont mises en œuvre.

- Surveillance permanente des réseaux sans fil
- Détection des points d'accès non autocisés
- Rotation régulière des clés
- Limitation de la puissance d'émission aux limites physiques des locaux
- Audits techniques périodiques des infrastructures Wi-Fi

Contrôle d'accès aux applications et aux données

Contrôle d'accès applicatif

Neo Financia implémente des contrôles d'accès granulaires au niveau applicatif.

- Intégration des applications critiques avec l'IAM central
- Gestion des autocisations par rôles applicatifs
- Filtrage des fonctionnalités selon les profils
- Contrôles d'accès contextuels (heure, localisation, appareil)
- Workflow d'approbation pour les opérations sensibles
- Politique de "quatre yeux" pour les transactions critiques
- Limitation volumétrique des opérations à risque

Les applications développées en interne suivent les principes suivants :

- Modèle d'autocisation centralisé
- Séparation des couches d'authentification et d'autocisation
- Validation côté serveur de toutes les autocisations
- Application de la séparation des tâches dans la conception
- Journalisation complète des actions sensibles

Contrôle d'accès aux bases de données

Les bases de données bénéficient de mesures de protection spécifiques

- Authentification forte obligatoire
- Interdiction des comptes applicatifs génériques
- Accès directs limités aux administrateurs de bases de données
- Utilisation de comptes de service à privilèges limités pour les applications

---

- Chiffrement des données sensibles au niveau colonne
- Masquage dynamique des données pour les utilisateurs non-privilégiés
- Audit des requêtes sur les données sensibles
- Détection des comportements anormaux d'accès

Contrôle d'accès aux API

Les API de Neo Financia, notamment celles exposées aux partenaires fintech (Mangopay, Lemonway), sont sécurisées par:

- Gateway API centralisée avec contrôles de sécurité uniformes
- Authentification OAuth 2.0 avec OpenID Connect
- Scopes limités aux fonctionnalités strictement nécessaires
- Tokens JWT signés avec durée de validité limitée (15 min max)
- Validation des signatures et vérification des claims
- Rate limiting adaptatif
- Validation des schémas de requêtes/réponses
- Protection contre les attaques courantes (injection, CSRF, etc.)
- Journalisation complète des appels

Pour les partenaires externes

- Processus d'onboarding sécurisé avec vérification
- Canal de distribution sécurisé des credentials
- Monitocing dédié des accès partenaires
- Rotation régulière des secrets
- Possibilité de révocation immédiate

Traçabilité et audit

Journalisation des accès

Neo Financia met en œuvre une journalisation exhaustive des accès et actions

- Enregistrement systématique des événements d'authentification (réussis et échoués)

- Journalisation des actions privilégiées
- Traçabilité des modifications de droits d'accès
- Horodatage précis et synchronisé (NTP sécurisé)
- Conservation de l'identité de l'utilisateur, de la source et de l'action
- Protection de l'intégrité des journaux (append-only, signature)
- Centralisation des logs dans un SIEM
- Rétention conforme aux exigences légales et réglementaires

Le niveau de journalisation est adapté à la sensibilité des ressources

- Standard : authentification et actions administratives
- Renforcé : toutes les actions utilisateur sur les données sensibles
- Maximum : enregistrement complet des sessions pour les systèmes critiques

---

Surveillance des activités suspectes

Neo Financia a mis en place des mécanismes de détection des comportements anormaux.

- Analyse comportementale des utilisateurs (UEBA)
- Détection des accès en dehors des plages horaires habituelles
- Identification des connexions depuis des localisations inhabituelles
- Alertes sur les tentatives d'accès multiples échouées
- Détection des élévations de privilèges non autocisées
- Surveillance des accès aux données sensibles
- Corrélation d'événements pour identifier les patterns d'attaque
- Intégration avec le SOC pour réponse rapide

Les alertes sont priorisées selon leur criticité et font l'objet d'un processus de traitement formalisé, avec escalade automatique pour les situations les plus à risque.

Audit et revue

Neo-Financia conduit des audits réguliers de son dispositif de contrôle d'accès :

- Revue trimestrielle des comptes privilégiés
- Audit semestriel des droits d'accès par les propriétaires de ressources
- Analyse des comptes dormants (inactifs depuis plus de 90 jours)
- Tests de pénétration ciblés sur les mécanismes d'authentification
- Vérification des séparations de tâches
- Contrôle de cohérence entre droits théoriques et effectifs
- Audit de la conformité aux politiques de mot de passe
- Reporting aux instances de gouvernance (COSEC, Comité des Risques)

Les résultats des audits font l'objet d'un suivi rigoureux avec

- Plans d'action documentés pour les écarts identifiés
- Assignation claire des responsabilités
- Délais de remédiation définis selon la criticité
- Vérification de l'efficacité des corrections
- Reporting aux instances de gouvernance

Gestion des identités externes

Accès des prestataires et partenaires

Neo Financia applique des mesures spécifiques pour gérer les accès des tiers :

- Processus dédié d'onboarding et d'offboarding
- Durée de validité limitée alignée sur les contrats
- Revue mensuelle des accès externes
- Désactivation automatique après période d'inactivité
- Accès via infrastructure dédiée (jump servers, VDI)
- Surveillance renforcée des actions effectuées

- Restrictions horaires et géographiques
- Interdiction de délégation ou partage d'accès

Les accès des partenaires fintech font l'objet de contrôles additionnels :

- Vérification préalable de la maturité sécurité
- Établissement de connexions sécurisées dédiées
- Limitations fonctionnelles et volumétriques
- Surveillance des flux en temps réel
- Capacité de coupure d'urgence en cas d'incident

Accès clients aux services digitaux

La sécurisation des accès pour les 2 millions de clients de Neo Financia repose sur

- Processus d'enrôlement rigoureux avec vérification d'identité
- Authentification adaptative selon le niveau de risque des opérations
- Options d'authentification forte multiple (biométrie, SMS OTP, TOTP)
- Détection des terminaux compromis
- Analyse comportementale pour identifier les activités anormales
- Validation renforcée pour les transactions sensibles
- Système anti-fraude intégré
- Education et sensibilisation des clients

La gestion des accès clients s'appuie sur

- Support multi-canal pour la réinitialisation sécurisée
- Verrous temporaires automatiques en cas de comportement suspect
- Notifications des actions sensibles
- Tableau de bord de gestion des appareils autocisés
- Options de personnalisation des contrôles de sécurité

Technologies de contrôle d'accès déployées

Neo Financia s'appuie sur un ensemble de solutions technologiques pour mettre en œuvre sa politique de contrôle d'accès:

Type de solution	Fonctionnalités clés	Couverture
Identity and Access Management (IAM)	- Gestion centralisée des identités	
-		

Single Sign-On (SSO)		
- Fédération d'identité		
- Gouvernance des accès		
Ensemble du Sl interne et cloud		
Privileged Access Management (PAM)	- Gestion des sessions privilégiées	
Administrateurs, comptes techniques		

| |-
Coffre-fort pour les secrets

- Accès "Just-In-Time"
- Enregistrement des sessions

Multi-Factoc Authentication (MFA)	- Authentification à plusieurs facteurs	

- Support FIDO2/WebAuthn
- Push notifications
- Authentification contextuelle |Tous les utilisateurs| |Cloud Access Security Broker (CASB)|-
  Contrôle des accès SaaS
- DLP cloud
- Détection des Shadow IT
- Classification des données cloud |Environnements Azure, AWS, SaaS| |Network Access Control (NAC)|-
  Contrôle des accès réseau
- Vérification de conformité
- Segmentation dynamique
- Quarantaine automatique |Réseaux internes et sans fil| |User and Entity Behavior Analytics (UEBA)|-
  Détection des comportements anormaux

- Établissement de profils de référence
- Calcul de scores de risque
- Alertes sur déviations |Utilisateurs critiques, systèmes sensibles| |Customer Identity and Access Management (CIAM)|-
  Gestion des identités clients
- Authentification progressive
- Intégration avec systèmes anti-fraude
- Expérience utilisateur optimisée |Services bancaires en ligne et mobiles|

Ces solutions sont intégrées dans une architecture cohérente, avec des processus de supervision et de maintenance assurant leur efficacité.

Sécurité physique et environnementale

Principes fondamentaux

La sécurité physique et environnementale constitue un élément fondamental de la stratégie de cybersécurité globale de Neo Financia. Malgré son modèle d'affaires principalement digital, l'institution reconnaît l'importance cruciale de protéger physiquement ses installations, ses équipements et ses personnels contre les menaces et risques pouvant compromettre la confidentialité, l'intégrité et la disponibilité des systèmes d'information.

Objectifs de la sécurité physique et environnementale :

- Prévenir les accès physiques non autocisés aux zones sensibles de l'organisation
- Protéger les équipements contre les dommages, vols ou compromissions
- Garantir la continuité des services par des mesures de protection environnementale
- Assurer la résilience des infrastructures critiques face aux incidents physiques
- Réduire les risques d'espionnage, de sabotage ou d'attaques via le canal physique
- Maintenir un niveau de protection cohérent avec les exigences réglementaires

Cette politique s'applique à l'ensemble des sites de Neo Financia (Paris, Lyon, Londres), ainsi qu'aux infrastructures hébergées (datacenters partenaires) et aux situations de travail à distance.

Périmètres de sécurité physique

Neo Financia applique une approche de défense en profondeur avec plusieurs périmètres de sécurité concentriques.

Classification des zones physiques

Zone	Description	Niveau de protection	Exemples
Zone publique (Z0)	Espaces accessibles librement	Surveillance de base	Hall d'entrée, parking extérieur
Zone contrôlée (Z1)	Accès général pour le personnel	Contrôle d'accès simple	Espaces de bureaux généraux, salles de réunion
Zone restreinte (Z2)	Accès limité aux personnels autocisés	Contrôle d'accès individuel	Bureaux des équipes IT, salles de développement
Zone sécurisée (Z3)	Accès très limité, contrôle renforcé	Double authentification	Salles serveurs, locaux sécurité, salles COMEX
Zone critique (Z4)	Accès hautement restreint	Accès supervisé, traçabilité complète	Datacenters, salles coffres, infrastructures sensibles

---

Chaque zone est délimitée par des barrières physiques appropriées (murs, portes sécurisées, vitres renforcées) et fait l'objet de mesures de protection proportionnées à sa sensibilité.

Matrice d'autocisation par zone

Les accès aux différentes zones sont strictement contrôlés selon la matrice suivante.

Profil	Z0	Z1	Z2	Z3	Z4
Visiteurs	Oui	Escorté	Non	Non	Non
Personnel administratif	Oui	Oui	Non	Non	Non
Personnel IT général	Oui	Oui	Oui	Non	Non
Équipe sécurité	Oui	Oui	Oui	Oui	Escorté
Administrateurs systèmes autocisés	Oui	Oui	Oui	Oui	Oui, avec approbation
Direction / RSSI	Oui	Oui	Oui	Oui	Oui

Contrôles d'accès physiques

Neo Financia met en œuvre un ensemble de contrôles techniques et organisationnels pour réguler les accès physiques

Systèmes de contrôle d'accès

- Badges électroniques : Système de contrôle d'accès centralisé avec badges personnalisés pour tous les employés
- Authentification biométrique : Utilisée en complément pour les zones Z3 et Z4 (empreinte digitale ou reconnaissance faciale)
- Sas de sécurité : Installés aux points d'entrée des zones sensibles pour prévenir les passages multiples
- Tourniquets : Aux entrées principales des bâtiments avec badge obligatoire
- Badges visiteurs : Temporaires, avec accès limités et visuellement distincts
- Système de gestion des visiteurs : Enregistrement préalable, vérification d'identité, badge temporaire

Surveillance et détection

- Vidéosurveillance : Système CCTV couvrant les périmètres, entrées et zones sensibles
- Conservation des enregistrements : 30 jours minimum, 90 jours pour les zones critiques
- Détection d'intrusion : Capteurs volumétriques, contacts de porte, bris de glace
- Système d'alarme : Relié au poste de sécurité 24/7 et à une société de télésurveillance
- Détection de mouvement : Activée en dehors des heures de bureau dans les zones sensibles
- Rondes de sécurité : Programmées et aléatoires sur les sites principaux

Procédures d'accès

- Attribution des accès : Basée sur les responsabilités professionnelles, avec validation par le management
- Revue périodique : Audit trimestriel des droits d'accès physiques
- Gestion des visiteurs : Pré-enregistrement obligatoire, accueil à la réception, accompagnement permanent
- Procédure d'urgence : Protocole de gestion des situations d'urgence avec bypass contrôlé des systèmes
- Accès des prestataires : Procédure spécifique avec validation préalable et supervision

Règles impératives de sécurité physique :

- Le prêt de badge est strictement interdit
- Tout visiteur doit être constamment accompagné en zone contrôlée
- Les portes sécurisées ne doivent jamais être bloquées en position ouverte
- Toute perte de badge doit être signalée immédiatement (blocage sous 1h)
- Les accès hors horaires standard (20h-7h) doivent faire l'objet d'une autocisation

Sécurité spécifique par site

Neo Financia a défini des mesures adaptées à chacun de ses sites

Siège social - Paris

- Périmètre extérieur : Contrôle d'accès véhicules, barrières anti-bélier, éclairage périmétrique
- Entrée principale : Accueil sécurisé 24/7, sas de sécurité, détection de métaux
- Étages sécurisés : 8ème étage (Direction) et sous-sol (IT) avec contrôles renforcés
- Poste de contrôle : Centre de sécurité centralisé avec supervision des alarmes et caméras
- Gestion de crise : Salle de crise équipée et autonome

Site de Lyon

- Sécurité multilocataire : Partage des locaux avec contrôles d'accès par étage
- Zones dédiées : Espaces Neo Financia sécurisés indépendamment
- Salle serveurs locale : Zone Z3 avec double contrôle d'accès
- Surveillance à distance : Pilotée depuis le siège de Paris en dehors des heures de bureau

Bureau de Londres

- Environnement partagé : Bureaux dans un business center avec sécurité commune
- Contrôles spécifiques : Couche de sécurité additionnelle pour les espaces Neo Financia
- Conformité UK : Respect des exigences britanniques post-Brexit
- Connexion sécurisée : Lien dédié chiffré avec le siège
- Équipement minimal : Infrastructure limitée, principalement postes de travail

Protection des datacenters

Neo Financia opère ses systèmes critiques dans des datacenters hautement sécurisés :

Datacenter primaire (interne)

- Classification : Zone critique (Z4) avec protection maximale
- Localisation : Site dédié en région parisienne
- Contrôles d'accès : Authentification multi-facteurs (badge + biométrie + code)
- Enregistrement : Journalisation complète des accès avec vidéosurveillance
- Compartimentage : Zones dédiées par fonction (réseau, serveurs, stockage)
- Protection : Cages sécurisées pour les équipements les plus sensibles
- Procédure d'accès : Validation préalable obligatoire, présence de deux personnes minimum

Datacenter secondaire (prestataire Tier III+)

- Localisation : Site distant (>100km) pour la résilience
- Contrat : SLA incluant des clauses de sécurité physique strictes
- Certification : ISO 27001, PCI-DSS, Tier III+ minimum
- Accès : Procédure formalisée avec préavis et validation
- Audit : Droit d'audit contractuel exercé annuellement

- Reporting : Rapports mensuels sur les incidents et accès

Environnements cloud

Pour ses infrastructures cloud (Azure 70%, OVHcloud 20%, AWS 10%), Neo Financia :

- Vérifie les certifications de sécurité physique des fournisseurs
- Exige des garanties contractuelles sur la sécurité physique
- Revoit annuellement les rapports d'audit tiers (SOC 2 Type II)
- Évalue la localisation géographique des données
- Impose des contraintes de souveraineté pour les données critiques

Sécurité environnementale

Neo Financia protège ses infrastructures contre les risques environnementaux :

Protection électrique

Mesure	Description	Sites concernés
Alimentation redondante	Double arrivée électrique depuis deux postes sources différents	Datacenter primaire
Onduleurs (UPS)	Batteries avec autonomie N+1 (30 minutes minimum)	Tous datacenters, salles serveurs
Groupes électrogènes	Capacité 72h avec tests mensuels et contrats de réapprovisionnement	Datacenter primaire
Protection contre les surtensions	Dispositifs parafoudres et régulateurs	Tous sites

---

Surveillance de la qualité électrique Monitocing des paramètres électriques avec alertes Datacenters, salles serveurs

Contrôle climatique

- Systèmes HVAC : Climatisation redondante N+1 dans les datacenters
- Surveillance température/humidité : Capteurs avec alertes (18-27°C, 40-60% humidité)
- Allées chaudes/froides : Organisation optimisée des flux d'air
- Maintenance préventive : Contrats de service avec GTI/GTR optimisés

Protection incendie

- Détection précoce : Systèmes VESDA (Very Early Smoke Detection Apparatus) dans les zones critiques
- Détecteurs : Optiques et thermiques avec double détection
- Extinction automatique : Systèmes à gaz inerte dans les salles serveurs (sans danger pour les équipements)
- Compartimentage : Cloisons et portes coupe-feu (résistance 2h minimum)

- Procédures : Protocoles d'évacuation et formation du personnel
- Exercices : Tests d'évacuation semestriels

Protection contre les dégâts des eaux

- Détecteurs de fuite : Sous les faux-planchers des zones sensibles
- Surélévation : Équipements positionnés à minimum 10cm du sol
- Absence de canalisations : Interdiction dans les plafonds des salles critiques
- Systèmes de drainage : Évacuation rapide en cas d'inondation

Sécurité des équipements

Protection des équipements critiques

- Inventaire : Recensement exhaustif et marquage des actifs physiques
- Fixation : Dispositifs anti-arrachement pour les équipements sensibles
- Armoires sécurisées : Verrouillage électronique avec traçabilité
- Documentation sécurisée : Plans et schémas d'infrastructure classifiés
- Redondance : Duplication des composants critiques (N+1 minimum)

Câblage sécurisé

- Protection des chemins de câbles : Conduits sécurisés pour câblage sensible
- Séparation : Distinction physique entre réseaux (production/administratif)
- Étiquetage : Identification claire selon le standard TIA-606-C
- Documentation : Plans de câblage tenus à jour
- Inspection : Vérification périodique de l'intégrité des câblages

Maintenance des équipements

- Contrats de maintenance : SLA adaptés à la criticité des équipements
- Procédures : Protocoles d'intervention formalisés

- Contrôles des intervenants : Vérification des identités et accompagnement
- Journalisation : Enregistrement détaillé des interventions
- Tests post-maintenance : Vérification du bon fonctionnement et de la sécurité

Mise au rebut sécurisée

- Procédure formelle : Validation RSSI pour tout équipement sortant
- Effacement des données : Processus certifié selon le niveau de sensibilité
- Destruction physique : Pour les supports de stockage critiques
- Traçabilité : Certificats de destruction/recyclage conservés
- Prestataires qualifiés : Entreprises certifiées pour le recyclage DEEE

Sécurité du travail à distance

Neo Financia encadre la sécurité physique des situations de travail hors des locaux contrôlés.

Travail à domicile

- Guide de bonnes pratiques : Recommandations pour la sécurité physique à domicile
- Équipements sécurisés : Verrouillage Kensington, écrans de confidentialité
- Stockage sécurisé : Rangement des équipements en lieu sûr
- Confidentialité : Protection contre l'observation visuelle (positionnement des écrans)
- Formation : Sensibilisation aux risques spécifiques du travail à domicile

Travail en mobilité

- Équipements durcis : Ordinateurs portables renforcés pour les déplacements
- Transport sécurisé : Sacoche de transport discrète et sécurisée
- Surveillance visuelle constante : Interdiction d'abandonner les équipements
- Espaces publics : Utilisation de filtres de confidentialité, vigilance accrue
- Procédure de perte/vol : Déclaration immédiate et effacement à distance

Contrôles et surveillance

Neo Financia maintient un programme complet de contrôle et d'amélioration continue de la sécurité physique

Audits et tests

- Audit annuel complet : Évaluation de l'ensemble du dispositif de sécurité physique
- Tests d'intrusion physique : Exercices de simulation avec équipe Red Team
- Inspections régulières : Contrôles mensuels des dispositifs de sécurité
- Tests des systèmes d'alerte : Vérification trimestrielle du bon fonctionnement
- Exercices d'évacuation : Simulations semestrielles avec débriefing

Surveillance et gestion des incidents

- Centre de surveillance 24/7 : Supervision permanente des systèmes de sécurité
- Procédures d'escalade : Protocoles formalisés selon la gravité
- Investigation : Processus d'enquête interne sur les incidents

---

- Retour d'expérience : Analyse et amélioration après chaque incident
- Reporting : Indicateurs de sécurité physique inclus dans le tableau de bord mensuel du COSEC

Gouvernance et documentation

- Politique de sécurité physique détaillée : Document spécifique rattaché à la PSSI
- Plans de sécurité par site : Documentation spécifique à chaque implantation
- Matrices de responsabilité : Attribution claire des rôles (sécurité, facilités, IT)
- Revue annuelle : Mise à jour des exigences et mesures
- Indicateurs de performance : KPIs spécifiques à la sécurité physique

Sécurité des opérations

Principes fondamentaux

La sécurité des opérations vise à garantir le fonctionnement correct et sécurisé des infrastructures, systèmes et services de Neo Financia. Ce domaine couvre l'ensemble des processus, procédures et contrôles permettant d'assurer l'intégrité, la disponibilité et la protection des systèmes d'information pendant leur exploitation quotidienne.

Objectifs de la sécurité opérationnelle :

- Maintenir un niveau optimal de sécurité pendant l'exploitation des systèmes
- Assurer que les changements sont mis en œuvre de manière contrôlée et sécurisée
- Garantir la disponibilité et la performance des services informatiques
- Protéger l'intégrité des systèmes de production
- Détecter et prévenir les incidents de sécurité
- Maintenir la traçabilité complète des actions opérationnelles
- Renforcer la résilience face aux menaces et dysfonctionnements

Cette politique s'applique à l'ensemble des systèmes d'information de Neo Financia, qu'ils soient hébergés en interne dans des datacenters partenaires ou dans le cloud.

Procédures opérationnelles et responsabilités

Documentation des procédures

Neo Financia maintient une documentation exhaustive et formalisée des procédures opérationnelles.

- Catalogue centralisé : Référentiel unique des procédures accessible aux équipes concernées
- Format standardisé : Structure homogène avec identification claire des responsabilités
- Cycle de vie documentaire : Processus de création, validation, révision et retrait
- Contrôle des versions : Traçabilité des modifications avec justification
- Revue périodique : Vérification annuelle minimum de l'actualité des procédures
- Classification : Niveau de confidentialité et criticité attribué à chaque document

Les domaines couverts incluent notamment

- Gestion des infrastructures (serveurs, stockage, réseau)
- Administration des bases de données
- Exploitation des applications métier
- Gestion des services cloud (Azure, AWS, OVHcloud)
- Sauvegarde et restauration
- Surveillance et supervision
- Gestion des incidents et problèmes
- Procédures de reprise d'activité

Principes d'exploitation sécurisée

- Moindre privilège : Attribution des droits minimaux nécessaires aux opérations

- Séparation des tâches : Division des responsabilités pour éviter les conflits d'intérêts
- Principe des 4 yeux : Validation par une seconde personne pour les opérations critiques
- Traçabilité : Journalisation complète des actions opérationnelles sensibles
- Automatisation : Scripts et procédures automatisées pour limiter les erreurs humaines
- Réversibilité : Capacité à revenir en arrière après une modification

Organisation des équipes opérationnelles

Équipe	Responsabilités	Modèle d'exploitation
Infrastructure	- Gestion des serveurs et systèmes d'exploitation	
- Administration des environnements virtualisés		
- Stockage et sauvegarde		
Service 8h-20h + astreinte 24/7		
Cloud Operations	- Administration des environnements cloud	
- Optimisation des ressources		
- Surveillance spécifique cloud		
Service 8h-20h + astreinte 24/7		
Réseau et Sécurité	- Administration des équipements réseau	
- Gestion des accès réseau et firewall		
- Protection périmétrique		
Service 8h-20h + astreinte 24/7		
Bases de données	- Administration des SGBD	

- Optimisation des performances		
- Gestion des sauvegardes spécifiques		
Service 8h-20h + astreinte 24/7		
Production applicative	- Exploitation des applications métier	
- Gestion des traitements batch		
Service 24/7		

|Monitocing & Support|-
Support niveau 3 |Service 24/7| | | |---|---|---| |-
Surveillance des systèmes et services

- Gestion des alertes
- Support niveau 1 et 2 |

Gestion des changements

Neo Financia applique un processus formalisé de gestion des changements pour garantir que toutes les modifications apportées à ses systèmes d'information sont évaluées, autocisées, testées et mises en œuvre de manière contrôlée :

Typologie des changements

Type	Description	Processus d'approbation	Préavis
Standard	Changements récurrents, à faible risque, procédure définie	Pré-approuvé (catalogue)	24h
Normal	Changements planifiés avec impact modéré	CAB hebdomadaire	5 jours
Majeur	Changements à fort impact ou sur systèmes critiques	CAB + approbation COSEC	15 jours
Urgent	Changements correctifs nécessaires immédiatement	Approbation Fast-Track (RSSI + DSI)	Immédiat
Emergency	Changements critiques pour résoudre incident majeur	Circuit d'urgence (RSSI ou délégué)	Immédiat

Processus de gestion des changements

- Demande : Formalisation du besoin avec justification, impact et risques
- Évaluation : Analyse technique, impacts métier et sécurité, ressources requises
- Approbation : Validation selon le type de changement et niveau d'autocité
- Planification : Définition des fenêtres d'intervention et ressources
- Test : Validation préalable dans un environnement de pré-production
- Mise en œuvre : Exécution contrôlée avec suivi en temps réel
- Vérification : Contrôle post-implémentation et tests fonctionnels
- Clôture : Documentation des résultats et retour d'expérience
- Rollback : Procédure de retour arrière en cas d'échec

Comité d'Approbation des Changements (CAB)

- Composition : DSI, responsables infrastructure, applications, sécurité, représentants métiers

---

- Fréquence : Réunion hebdomadaire + sessions extraordinaires si besoin
- Rôle : Analyse et validation des changements proposés
- Documentation : PV formalisé avec décisions et conditions
- Suivi : Tableau de bord des changements et de leur efficacité

Calendrier de changements

- Fenêtres de maintenance planifiées : Créneaux réservés hebdomadaires (samedi 22h-dimanche 6h)
- Périodes gelées : Restrictions pendant les périodes d'activité critique (fin de mois, clôtures)
- Communication : Notification préalable aux utilisateurs et parties prenantes
- Coordination : Gestion des dépendances entre changements

Gestion des capacités et des performances

Neo Financia surveille et gère les capacités de ses systèmes pour garantir les performances requises

Monitocing des ressources

- Supervision continue : Surveillance temps réel des indicateurs clés
- Métriques suivies : CPU, mémoire, stockage, bande passante, transactions, temps de réponse
- Seuils d'alerte : Définition de niveaux progressifs (attention, avertissement, critique)
- Tableaux de bord : Visualisation centralisée des performances
- Histocisation : Conservation des données de performance (1 an minimum)

Planification des capacités

- Analyse prévisionnelle : Projection des besoins futurs basée sur la croissance et les projets

- Modélisation des charges : Simulation des pics d'activité saisonniers ou événementiels
- Revue trimestrielle : Évaluation régulière de l'adéquation capacités/besoins
- Plan d'évolution : Roadmap d'augmentation des capacités alignée sur les projets
- Optimisation : Identification des opportunités d'amélioration (tuning, consolidation)

Gestion des performances

- Tests de charge : Validation régulière de la capacité à supporter les volumes attendus
- Optimisation des applications : Amélioration continue du code et des configurations
- Gestion des ressources cloud : Auto-scaling, rightsizing des instances
- SLA internes : Définition d'objectifs de performance par service
- Reporting : Mesure et communication régulière des indicateurs de performance

Séparation des environnements

Neo Financia maintient une séparation stricte entre ses différents environnements pour protéger les systèmes de production:

Architecture multi-environnements

Environment

Function

Contrôles spécifiques

|Production|Exécution des services en exploitation|-
Accès hautement restreint

- Modification uniquement via processus formel
- Surveillance renforcée 24/7
- Sauvegardes complètes | |---|---|---| |Pré-production|Tests finaux avant mise en production|-
  Architecture identique à la production
- Données anonymisées représentatives
- Validation des performances et de la sécurité
- Accès limité aux équipes d'exploitation et QA | |Test/Recette|Validation fonctionnelle par les métiers|-
  Jeu de données de test
- Accès ouvert aux testeurs métier

- Reset périodique des données
- Surveillance allégée | |Développement|Développement et tests unitaires|-Données fictives uniquement
- Architecture simplifiée
- Flexibilité pour les développeurs
- Pas de connexion avec la production | |Sandbox|Expérimentation et innovation|-Isolation complète du Sl
- Données synthétiques uniquement
- Durée de vie limitée
- Mécanismes de protection spécifiques |

Mesures de séparation

- Isolation réseau : Segmentation physique et/ou logique complète
- Contrôles d'accès distincts : Droits spécifiques à chaque environnement
- Gestion des identités séparée : Comptes dédiés par environnement pour les administrateurs
- Flux contrôlés : Communications inter-environnements strictement limitées et tracées
- Procédures de promotion : Processus formalisé de passage d'un environnement à l'autre

Anonymisation des données

- Politique de données de test : Règles strictes d'utilisation des données en environnements non-productifs
- Techniques d'anonymisation : Masquage, pseudonymisation, synthétisation
- Vérification : Contrôles automatisés pour détecter les données de production non anonymisées
- Processus automatisé : Outils dédiés pour créer des jeux de données conformes

---

- Validation DPO : Approbation des méthodes d'anonymisation par le Délégué à la Protection des Données

Protection contre les logiciels malveillants

Neo Financia déploie une stratégie de défense en profondeur contre les logiciels malveillants

Mesures préventives

- Solution EDR (Endpoint Detection and Response) : Déploiement sur 100% des postes et serveurs
- Filtrage web : Blocage des sites malveillants et des catégories à risque
- Protection de la messagerie : Filtrage avancé des emails et pièces jointes
- Durcissement des systèmes : Configuration restrictive limitant les vecteurs d'infection
- Application whitelisting : Restriction d'exécution aux applications autocisées
- Contrôle des supports amovibles : Restriction et scan automatique

Mesures de détection

- Scans antivirus : Analyse régulière et à l'accès
- Détection comportementale : Identification des activités suspectes
- Sandbox automatisée : Analyse dynamique des fichiers suspects
- Surveillance réseau : Détection des communications suspectes
- Centralisation des alertes : Intégration au SIEM pour corrélation
- Threat Intelligence : Utilisation de flux d'information sur les menaces

Mesures de réponse

- Isolation automatique : Quarantaine des systèmes suspectés d'infection
- Remédiation guidée : Procédures détaillées de nettoyage
- Restauration sécurisée : Reconstruction des systèmes compromis
- Investigation : Analyse forensique des incidents
- Partage d'information : Communication des loCs aux équipes concernées

Maintenance et mise à jour

- Mise à jour des signatures : Actualisation automatique toutes les 4 heures maximum
- Patch management : Déploiement accéléré des correctifs de sécurité critiques
- Tests de non-régression : Validation des mises à jour majeures
- Surveillance de l'efficacité : Métriques et audits des solutions déployées
- Veille technique : Suivi des évolutions et nouvelles menaces

Sauvegarde et restauration des données

Neo Financia implémente une stratégie robuste de sauvegarde et restauration pour protéger ses données critiques.

Politique de sauvegarde

Criticité

|Critique (données transactionnelles)|< 15 minutes|Continue (CDC + log shipping)|7 jours complet, 30 jours archives|Test hebdomadaire| |---|---|---|---|---| |Importante (données clients)|< 4 heures|Toutes les heures|30 jours complet, 1 an archives|Test bi-mensuel| |Standard (données opérationnelles)|> 4 heures < 24 heures|Quotidienne|30 jours|Test mensuel| |Faible (données analytiques)|> 24 heures < 72 heures|3 fois par semaine|15 jours|Test trimestriel|

Architecture de sauvegarde

Neo Financia applique le principe 3-2-1-1-0

- 3 copies des données : Original + 2 sauvegardes
- 2 types de supports différents : Stockage primaire + secondaire
- 1 copie hors site : Stockage géographiquement distant
- 1 copie immuable : Protection contre le ransomware (WORM - Write Once Read Many)
- 0 erreur : Validation systématique des sauvegardes

Technologies et méthodes

- Sauvegarde incrémentielle : Capture des modifications uniquement
- Snapshot des machines virtuelles : Points de restauration cohérents
- Réplication synchrone : Pour les données critiques (RTO < 15 min)
- Réplication asynchrone : Pour les données standard
- Archivage long terme : Conservation réglementaire (5-10 ans)
- Chiffrement : Protection des sauvegardes en transit et au repos
- Déduplication : Optimisation des volumes

Processus de restauration

- Procédures documentées : Instructions détaillées par type de restauration
- Tests réguliers : Exercices planifiés de récupération
- Restauration sélective : Capacité à récupérer des éléments individuels
- Restauration complète : Procédure de disaster recovery testée
- Autocisation formelle : Validation préalable des demandes de restauration
- Traçabilité : Documentation complète des opérations de restauration

Journalisation et surveillance

Neo Financia met en œuvre un dispositif complet de journalisation et de surveillance pour détecter les incidents et assurer la traçabilité des opérations :

Politique de journalisation

Type de logs	Périmètre	Contenu minimum	Rétention
Logs système	Serveurs, équipements réseau, systèmes d'exploitation	Événements système, erreurs, alertes, démarrage/arrêt	6 mois
Logs applicatifs	Applications métier, middlewares, API	Erreurs, transactions, performances, erreurs utilisateurs	12 mois
Logs de sécurité	Firewall, IDS/IPS, proxys, VPN, EDR	Tentatives d'intrusion, violations de politique, alertes	18 mois

Logs d'accès	Authentification, contrôle d'accès, actions privilégiées	Identité, timestamp, action, succès/échec, source	24 mois
Logs de transactions	Opérations financières, modifications de données sensibles	Détails complets de la transaction, utilisateur, timestamp	5 ans

Principes de journalisation

- Normalisation des formats : Standardisation pour faciliter l'exploitation
- Horodatage précis : Synchronisation NTP sur source fiable
- Intégrité : Protection contre la modification (append-only, signatures)
- Centralisation : Collecte dans un système SIEM centralisé
- Filtrage : Réduction du bruit et des données non pertinentes
- Corrélation : Mise en relation des événements pour détection avancée
- Confidentialité : Protection des données sensibles dans les logs

Surveillance opérationnelle

- Monitocing temps réel : Surveillance continue des indicateurs clés
- Tableaux de bord : Visualisation de l'état des systèmes
- Alertes automatisées : Notification des anomalies et dépassements de seuils
- Mesure des SLA : Suivi des niveaux de service
- Détection des anomalies : Identification des comportements inhabituels
- Surveillance applicative : APM (Application Performance Monitocing)
- Supervision de l'expérience utilisateur : RUM (Real User Monitocing)

Organisation de la surveillance

- Centre d'opérations sécurité (SOC) : Surveillance 24/7 des alertes de sécurité
- Centre d'opérations réseau (NOC) : Supervision infrastructure et performances
- Équipes d'astreinte : Rotation pour interventions hors heures
- Procédures d'escalade : Processus formalisé selon la gravité
- Reporting régulier : Communication des indicateurs aux parties prenantes

---

Gestion des vulnérabilités techniques

Neo Financia met en œuvre un processus continu de gestion des vulnérabilités techniques pour identifier et corriger les faiblesses de ses systèmes:

Identification des vulnérabilités

- Scans automatisés réguliers : Analyse de l'ensemble du parc (hebdomadaire minimum)
- Tests de pénétration : Évaluation approfondie par des experts (trimestrielle)
- Veille sur les vulnérabilités : Suivi des alertes et bulletins de sécurité
- Audit de configuration : Vérification de la conformité aux standards
- Bug bounty : Programme de récompense pour les découvertes externes
- Scan des applications : SAST, DAST et analyse de composition (SCA)

Évaluation et priorisation

- Classification CVSS : Évaluation basée sur le score standard
- Analyse de l'exposition : Prise en compte du contexte d'exploitation
- Impact business : Évaluation des conséquences potentielles
- Exploitabilité : Facilité de mise en œuvre de l'attaque
- Détermination des délais de correction : SLA interne par niveau de risque

Stratégie de remédiation

Niveau de risque	Délai de correction	Processus d'approbation	Mesures compensatoires
Critique (CVSS 9.0-10.0)	≤ 24h (production) ≤ 48h (autres env.)	Fast-track, notification COSEC	Obligatoires pendant correction
Élevé (CVSS 7.0-8.9)	≤ 7 jours	Validation RSSI	Recommandées
Moyen (CVSS 4.0-6.9)	≤ 30 jours	Processus standard	Au cas par cas
Faible (CVSS 0.1-3.9)	≤ 90 jours	Planification normale	Non requises

Cycle de vie des vulnérabilités

- Découverte : Identification initiale
- Qualification : Vérification et analyse
- Classification : Évaluation du risque
- Remédiation : Application du correctif ou mesure
- Vérification : Confirmation de la correction
- Clôture : Documentation finale

Gestion des exceptions

- Processus formel : Documentation complète des exceptions
- Justification : Motifs techniques ou business validés
- Mesures compensatoires : Contrôles alternatifs obligatoires
- Limitation dans le temps : Date d'expiration définie
- Approbation de haut niveau : Validation RSSI/COSEC selon criticité
- Surveillance renforcée : Monitocing spécifique des systèmes concernés

Configuration de sécurité des systèmes

Neo Financia maintient une approche structurée pour assurer la sécurité des configurations de ses systèmes d'information:

Standards de configuration

- Référentiels de base : CIS Benchmarks, NIST, guides ANSSI

- Modèles durcis : Templates pré-validés par technologie
- Documents de référence : Guides internes par type de système
- Principe de moindre fonctionnalité : Limitation aux services nécessaires
- Désactivation des services inutilisés : Réduction de la surface d'attaque
- Suppression des comptes par défaut : Élimination des vulnérabilités connues

Gestion des configurations

- Infrastructure as Code : Définition déclarative des configurations
- Automatisation : Déploiement standardisé et reproductible
- Configuration Management Database (CMDB) : Référentiel central des configurations
- Gestion des versions : Traçabilité des modifications
- Tests de conformité : Validation avant déploiement
- Contrôle de dérive : Détection des écarts par rapport aux standards

Mesures spécifiques par environnement

Type de système	Mesures spécifiques	Contrôles
Serveurs	- Durcissement OS selon CIS Level 2	
- Cloisonnement réseau		
- Privilèges minimaux		
Scan mensuel de conformité		
Bases de données	- Chiffrement transparent	
- Audit renforcé		
- Contrôles d'accès granulaires		
Audit trimestriel		

|Environnements cloud|-
Configuration via templates validés

- CSPM (Cloud Security Posture Management)
- Cloisonnement des tenants

Scan hebdomadaire, alertes temps réel		
Postes de travail	- Images standardisées	

- Gestion centralisée (MDM)
- Restriction des privilèges locaux |Vérification à la connexion| |Équipements réseau|-
  Configurations homologuées
- Accès via jumphost sécurisé
- Sauvegardes des configurations |Vérification quotidienne d'intégrité| |Conteneurs|-
  Images minimales validées
- Scanner de vulnérabilités intégré
- Politiques d'admission |Scan à chaque build et déploiement|

Surveillance et application des configurations

- Audit continu : Vérification automatisée de la conformité
- Remédiation automatique : Correction des dérives de configuration
- Reporting : Tableau de bord de conformité
- Revue périodique : Évaluation de l'efficacité des standards
- Mise à jour des référentiels : Adaptation aux évolutions technologiques

Gestion technique des secrets

Neo Financia a mis en place des mécanismes robustes pour gérer les secrets techniques (mots de passe, clés, certificats, tokens) :

Infrastructure de gestion des secrets

- Coffre-fort centralisé : Solution dédiée pour le stockage sécurisé
- Chiffrement fort : Protection des secrets au repos et en transit
- Séparation des rôles : Administration et utilisation distinctes
- Haute disponibilité : Architecture redondante et résiliente
- API sécurisée : Interface programmatique pour l'automatisation

Cycle de vie des secrets

- Génération sécurisée : Création selon les standards de robustesse

---

- Distribution contrôlée : Mécanismes sécurisés de transmission
- Rotation régulière : Renouvellement planifié ou événementiel
- Révocation d'urgence : Procédure de compromission
- Archivage sécurisé : Conservation histocique si nécessaire
- Destruction sécurisée : Effacement complet en fin de vie

Politiques spécifiques par type de secret

Type de secret	Durée maximale	Contrôles spécifiques
Comptes système & service	90 jours	Complexité élevée, accès restreint, journalisation
API Keys	60 jours	Limitation de portée, restriction par origine
Certificats TLS	1 an	Autocité de certification interne, inventaire complet
Clés de chiffrement	2 ans	HSM pour les clés critiques, séparation gestion/usage
Secrets cloud	45 jours	Intégration aux services natifs (KMS, Key Vault)
Tokens d'authentification	Session ou 8h max	Durée limitée, contexte unique, révocation instantanée

Intégration aux processus opérationnels

- Automatisation DevOps : Injection sécurisée dans les pipelines CI/CD
- Audit d'utilisation : Traçabilité complète des accès aux secrets
- Détection des fuites : Monitocing du code source et des journaux
- Accès d'urgence : Procédure break-glass avec approbation multiple
- Inventaire automatisé : Découverte et cartographie des secrets

Sécurité des communications

Principes fondamentaux

La sécurité des communications constitue un pilier essentiel de la protection globale des systèmes d'information de Neo Financia. En tant que néobanque opérant principalement à travers des canaux digitaux, l'institution doit garantir la confidentialité, l'intégrité et la disponibilité de toutes ses communications internes et externes, tout en assurant leur traçabilité.

Objectifs de la sécurité des communications :

- Assurer la protection des données en transit sur l'ensemble des réseaux
- Garantir la confidentialité des échanges entre les systèmes, les utilisateurs et les partenaires
- Préserver l'intégrité des informations pendant leur transmission
- Authentifier de manière fiable les parties communicantes

- Prévenir les intrusions et les accès non autocisés via les canaux de communication
- Assurer la disponibilité des services de communication critiques
- Permettre la traçabilité des échanges d'informations sensibles

Cette politique s'applique à l'ensemble des infrastructures réseau et moyens de communication utilisés par Neo Financia, qu'ils soient internes ou externes, filaires ou sans fil, sur site ou dans le cloud.

Architecture réseau sécurisée

Principes d'architecture

Neo Financia applique une approche de défense en profondeur dans la conception de son architecture réseau

- Segmentation multiniveau : Division du réseau en zones de sécurité distinctes
- Filtrage à chaque frontière : Contrôles entre les différentes zones
- Moindre privilège : Limitation des flux au strict nécessaire
- Défense en profondeur : Superposition de contrôles complémentaires
- Redondance : Élimination des points uniques de défaillance
- Invisibilité : Exposition minimale des services vers l'extérieur
- Monitocing : Surveillance complète des flux et anomalies

Zones de sécurité réseau

L'architecture réseau de Neo Financia est structurée en zones de sécurité distinctes

Zone	Description	Contrôles spécifiques	Usage
Internet / Externe	Réseaux publics non maîtrisés	Protection DDoS, surveillance avancée	Accès clients et partenaires
DMZ externe	Zone d'exposition contrôlée	WAF, IPS, filtrage applicatif	Services exposés (web, API Gateway)
Zone API	Couche d'orchestration des API	API Gateway, authentification forte	Exposition contrôlée des services internes
Zone applicative	Hébergement des applications métier	Micro-segmentation, flow control	Applications bancaires, services clients
Zone données	Stockage et traitement des données	Isolation stricte, contrôles d'accès renforcés	Bases de données, data lakes
Zone d'administration	Gestion des infrastructures	Bastions, PAM, surveillance renforcée	Administration technique

Zone utilisateur	Réseaux des postes de travail	NAC, filtrage des accès aux ressources	Collaborateurs internes
Zone partenaires	Interconnexions sécurisées	VPN dédiés, filtrage spécifique	Connexions avec Mangopay, Lemonway, etc.

Modèle de micro-segmentation :

En complément de cette segmentation principale, Neo Financia applique une micro-segmentation avancée, particulièrement dans les environnements cloud, basée sur :

- Identité et contexte des applications et services
- Classification des données traitées
- Niveau d'exposition et criticité
- Besoins d'interaction entre services

Cette approche permet un contrôle granulaire des communications, limitant drastiquement les mouvements latéraux en cas de compromission.

Contrôles de filtrage

Neo Financia déploie plusieurs niveaux de filtrage entre les différentes zones de sécurité

- Firewalls nouvelle génération (NGFW) : Filtrage évolué avec inspection applicative
- Web Application Firewalls (WAF) : Protection spécifique des applications web
- Systèmes de prévention d'intrusion (IPS) : Détection et blocage des attaques
- Proxys applicatifs : Contrôle et inspection du trafic spécifique
- Filtres anti-DDoS : Protection contre les attaques volumétriques
- Network Access Control (NAC) : Contrôle des connexions au réseau
- Filtrage par VM/Container : Rules de sécurité au niveau instance

Les règles de filtrage suivent plusieurs principes clés.

- Autocisation explicite des flux légitimes uniquement (deny by default)
- Granularité maximale dans la définition des règles
- Documentation complète de la justification business
- Processus formel d'approbation et de revue
- Audit périodique de pertinence (au moins semestriel)
- Suppression des règles temporaires à échéance

Sécurisation des communications

Chiffrement des communications

Neo Financia implémente une politique stricte de chiffrement des communications :

Type de communication	Standard minimum	Exigences complémentaires

Services web externes (Internet)	TLSv1.2 minimum obligatoire	- Certificate Extended Validation
- Certificats renouvelés tous les 12 mois		
- Certificate Transparency		
- HSTS avec preloading		
Communications internes critiques	TLSv1.2 minimum ou IPsec	- PKI interne avec validation stricte
- Authentification mutuelle obligatoire		
- Rotation des certificats tous les 6 mois		
API externes	TLSv1.2 minimum + jeton signé	- Signature des requêtes (JWS)
- Validité limitée des jetons (15min max)		
- Chiffrement de charge utile sensible (JWE)		
Connexions avec partenaires	VPN IPsec ou TLS	- Tunnel dédié par partenaire
- Authentification par certificat		
- Monitocing spécifique des tunnels		
Interconnexions Cloud	Liens privés chiffrés	- ExpressRoute/Direct Connect chiffré
- Isolation des flux par VLAN		

- Monitocing en temps réel		
Email	TLS opportuniste (STARTTLS)	- SPF, DKIM et DMARC obligatoires
- Chiffrement S/MIME pour emails sensibles		
- Anti-spoofing activé		
Communications administratives	SSH v2, RDP sur TLS	- Authentification par clé, pas de mot de passe
- Tunnel bastion obligatoire		
- Enregistrement des sessions		

Gestion des certificats

- Infrastructure à clé publique (PKI) : Gestion rigoureuse des autocités de certification
- Inventaire centralisé : Suivi de tous les certificats et dates d'expiration
- Génération sécurisée : Clés générées avec des paramètres robustes (RSA 4096+ ou ECC P-384+)
- Stockage protégé : Conservation des clés privées dans des HSM pour les services critiques
- Surveillance des expirations : Alertes préventives 60/30/15 jours avant échéance
- Procédure de rotation : Renouvellement sans impact sur la disponibilité des services
- Révocation d'urgence : Procédure rapide en cas de compromission

Protocoles et algorithmes autocisés

Protocoles et algorithmes approuvés par Neo Financia :

Protocoles de chiffrement :

- TLSv1.3 (privilégié)
- TLSv1.2 (compatible)
- IPsec avec IKEv2

- SSH v2

Algorithmes de chiffrement symétriques :

- AES-256-GCM (privilégié)
- AES-128-GCM
- ChaCha20-Poly1305

Algorithmes asymétriques :

- RSA 4096 bits minimum
- ECC avec P-384 ou P-521 (privilégié)
- Ed25519 pour SSH

Fonctions de hachage :

- SHA-384 (privilégié)
- SHA-256 (minimum)
- SHA-3 pour nouveaux systèmes

Protocoles et algorithmes interdits :

- SSL 2.0/3.0 et TLSv1.0/1.1
- RC4, DES, 3DES, Blowfish
- MD5, SHA-1
- RSA inférieur à 2048 bits
- Chiffrements faibles et modes non authentifiés (ECB, CBC sans HMAC)

- Diffie-Hellman avec des groupes inférieurs à 2048 bits

Protection périmétrique

Neo Financia met en œuvre une défense périmétrique multicouche pour protéger ses infrastructures exposées à Internet

Défense anti-DDoS

- Protection volumétrique : Filtrage des attaques massives au niveau réseau
- Protection applicative : Détection et mitigation des attaques ciblant la couche 7
- Capacité d'absorption : Dimensionnement pour résister aux pics de trafic
- Scrubbing centers : Redirection et nettoyage du trafic en cas d'attaque
- Plan de réponse : Procédures formalisées d'escalade et d'intervention
- Services tiers spécialisés : Contrat avec prestataire spécialisé anti-DDoS

Exposition minimale

- Limitation des services exposés : Exposition strictement limitée aux services nécessaires
- Reverse proxy obligatoire : Pas d'exposition directe des serveurs applicatifs
- Masquage d'informations : Suppression des bannières et informations techniques

- Segregation multi-tenants : Isolation des instances exposées
- Virtualisation inversée : Services exposés sur infrastructure dédiée

Filtrage avancé

- Web Application Firewall (WAF) : Protection contre les attaques applicatives web
- API Gateway sécurisée : Protection spécifique des API publiques
- Bot Management : Détection et contrôle des robots malveillants
- Inspection SSL/TLS : Analyse du trafic chiffré pour les connexions entrantes
- Règles adaptatives : Ajustement automatique selon le contexte de menace
- Protection "zero-day" : Détection comportementale des nouvelles menaces
- IP Reputation : Filtrage basé sur la réputation des adresses sources

Points de démarcation

- Architecture DMZ structurée : Zones tampons entre Internet et systèmes internes
- Cloisonnement par service : Isolation des différentes fonctions exposées
- Contrôles à chaque passage : Inspection des flux à chaque traversée de zone
- Surveillance renforcée : Monitocing spécifique des points d'entrée
- Proxys applicatifs : Médiation des protocoles entre zones

Accès distants sécurisés

Néo Financia sécurise les accès distants à ses systèmes par des mécanismes robustes

Solutions VPN

Type d'accès	Solution	Contrôles spécifiques	Usage
VPN collaborateurs	VPN SSL avec MFA	- Authentification forte obligatoire	
- Contrôle de santé du poste			
- Tunnel intégral ou split tunnel selon profil			
Télétravail, mobilité			
VPN administrateurs	VPN dédié sécurisé	- Double authentification	
- Accès limité aux adresses autocisées			
- Enregistrement intégral des sessions			
Administration d'urgence			

Accès partenaires	VPN site-à-site IPsec	- Tunnel dédié par partenaire	
- Filtrage granulaire des flux autocisés			
- Monitocing permanent des tunnels			
Connexion Mangopay, Lemonway			
Accès prestataires	Portail d'accès sécurisé	- Authentification dédiée par intervenant	
- Accès limité temporellement			
- Surveillance accrue des actions			
Maintenance, support			

Contrôles appliqués aux accès distants

- Authentification multi-facteurs : Obligatoire pour tous les accès distants
- Contrôle de conformité des postes : Vérification de l'état de sécurité avant connexion
- Segmentation des accès : Limitation aux seules ressources nécessaires
- Journalisation renforcée : Enregistrement détaillé des actions effectuées
- Détection des anomalies : Surveillance des comportements inhabituels
- Limitation temporelle : Sessions limitées dans le temps avec déconnexion automatique
- Filtrage géographique : Restrictions basées sur la localisation

Accès aux applications critiques

- Accès Zero Trust : Authentification et autocisation continues
- Passerelles d'application : Proxy applicatif avec authentification dédiée
- Virtualisation des applications : Publication sécurisée sans téléchargement local
- Isolation des sessions : Prévention des mouvements latéraux

---

- Contextualisation: Ajustement des accès selon le contexte (appareil, localisation, heure)

Sécurité des réseaux sans fil

Neo Financia implémente des contrôles spécifiques pour sécuriser ses réseaux sans fil.

Configuration des réseaux Wi-Fi

Réseau	Protocole	Authentification	Contrôles supplémentaires
Wi-Fi Corporate	WPA3-Enterprise	802.1X avec EAP-TLS	- Certificats matériels
- Intégration avec le NAC			
- Chiffrement individuel des sessions			
Wi-Fi BYOD	WPA3-Enterprise	802.1X avec authentification utilisateur	- Segmentation dédiée
- Accès limité aux ressources autocisées			
- Inspection du trafic sortant			
Wi-Fi Invités	WPA3-Personal	Portail captif avec code temporaire	- Isolation complète du Sl interne
- Sortie Internet filtrée			
- Limitation de bande passante			

Protection des réseaux sans fil

- Couverture maîtrisée : Limitation de la puissance d'émission aux limites physiques
- Détection de rogue AP : Surveillance et neutralisation des points d'accès non autocisés

- Inspection du trafic : Analyse du trafic sans fil pour détecter les menaces
- Rotation des clés : Renouvellement automatique des clés de chiffrement
- Détection d'attaques : Identification des tentatives de déauthentification, MITM, etc
- Sécurité physique : Protection des équipements réseau sans fil

Transfert sécurisé de l'information

Neo Financia encadre strictement les transferts d'information avec l'extérieur.

Politique d'échange de données

- Classification préalable : Évaluation du niveau de sensibilité des données à transférer
- Autocisation formelle : Validation obligatoire selon le niveau de sensibilité
- Canaux sécurisés dédiés : Utilisation de moyens appropriés selon la classification
- Chiffrement obligatoire : Protection des données sensibles pendant le transfert

---

- Traçabilité : Journalisation complète des transferts significatifs
- Contrôle d'intégrité : Vérification de l'intégrité des données transmises

Méthodes de transfert sécurisé

Niveau de sensibilité	Méthodes autocisées	Contrôles obligatoires
Public (PO)	Tous moyens standards	Validation de publication
Interne (P1)	Email, SFTP, HTTPS, portail sécurisé	Canal chiffré, authentification basique
Confidentiel (P2)	SFTP, portail sécurisé, API cryptée	- Chiffrement fort
- Authentification multi-facteurs		
- Traçabilité complète		
Critique (P3)	Canal dédié sécurisé, MFT chiffré	- Double chiffrement
- Validation avant et après transfert		
- Accusé de réception sécurisé		
-		

Journalisation détaillée		

Transferts avec les partenaires financiers

Neo Financia a établi des canaux de communication sécurisées avec ses principaux partenaires fintech

- Mangopay : API sécurisée avec authentification mutuelle par certificats, chiffrement TLS 1.3, signatures des transactions
- Lemonway : Tunnel VPN dédié avec authentification forte, APIs chiffrées, validation d'intégrité des messages
- Autres partenaires financiers : Connexions SFTP sécurisées avec authentification par clés, supervision dédiée

Chaque connexion avec un partenaire fait l'objet :

- D'une évaluation de sécurité préalable
- D'un contrat détaillant les exigences de sécurité
- D'une documentation technique précise
- D'une surveillance spécifique
- De tests réguliers de sécurité

Surveillance des réseaux

Neo-Financia assure une surveillance continue de ses infrastructures réseau.

Dispositifs de détection

- IDS/IPS : Détection et prévention d'intrusion aux points stratégiques
- NDR (Network Detection and Response) : Analyse comportementale du trafic

---

- Sondes réseau : Capteurs déployés dans les segments critiques
- Analyse de flux : Monitocing des modèles de trafic (NetFlow)
- Deep Packet Inspection : Inspection approfondie des communications sensibles
- Honeypots : Leurres pour détecter les activités malveillantes
- Surveillance DNS : Détection des tunneling et communications suspectes

Monitocina et alerte

- Surveillance 24/7 : Monitocing permanent par l'équipe SOC
- Corrélation d'événements : Analyse croisée des alertes via le SIEM
- Détection d'anomalies : Identification des écarts par rapport aux baseline
- Alertes en temps réel : Notification immédiate des incidents critiques
- Dashboards de sécurité : Visualisation de l'état de sécurité réseau
- Reporting régulier : Rapports quotidiens, hebdomadaires et mensuels

Gestion des incidents réseau

- Procédures d'intervention : Playbooks spécifiques par type d'incident
- Capacité d'isolation : Segmentation dynamique en cas d'attaque

- Équipe d'intervention : Ressources dédiées en cas d'incident
- Communication : Canaux sécurisés pour la gestion de crise
- Analyse post-incident : Investigation approfondie et retour d'expérience
- Amélioration continue : Adaptation des défenses selon les incidents observés

Séparation des réseaux

Neo-Financia implémente une séparation stricte des différents environnements réseau

Isolation des environnements

- Séparation production/hors-production : Isolation complète des environnements de production
- Cloisonnement développement/test/validation : Environnements distincts avec contrôles spécifiques
- Isolation des infrastructures cloud : Séparation entre les différents fournisseurs cloud (Azure, AWS, OVHcloud)
- Ségrégation des réseaux administratifs : Réseau de gestion isolé pour l'administration des systèmes
- Cloisonnement par classification : Séparation basée sur la sensibilité des données

Technologies de séparation

- VLAN : Segmentation logique du réseau local
- Firewalls physiques et virtuels : Contrôle des flux entre segments
- VRF (Virtual Routing and Forwarding) : Isolation au niveau routage
- VPC/VNET : Réseaux privés virtuels dans le cloud
- NSX/SDN : Micro-segmentation réseau définie par logiciel
- Proxys applicatifs : Rupture de flux entre zones de sécurité

Flux inter-environnements

- Contrôle strict : Limitation aux flux strictement nécessaires

---

- Zones de transit sécurisées : Points de passage contrôlés entre environnements
- Flux unidirectionnels : Direction des communications maîtrisée
- Inspection approfondie : Analyse du contenu des communications inter-zones
- Journalisation renforcée : Traçabilité complète des flux entre environnements

Acquisition, développement et maintenance des systèmes

Principes fondamentaux

L'intégration de la sécurité dans l'acquisition, le développement et la maintenance des systèmes est essentielle pour garantir que les applications et infrastructures de

Neo Financia répondent aux exigences de sécurité dès leur conception et tout au long de leur cycle de vie.

Objectifs de la sécurité dans le développement et la maintenance :

- Intégrer la sécurité dès la phase de conception des systèmes (Security by Design)
- Garantir que tous les développements internes et externes respectent les standards de sécurité
- S'assurer que les modifications apportées aux systèmes n'affectent pas leur niveau de sécurité
- Vérifier et valider la sécurité à chaque étape du cycle de développement
- Protéger les environnements de développement contre les compromissions
- Maintenir la sécurité des systèmes sur toute leur durée de vie
- Assurer la qualité et la sécurité des composants externes utilisés

Cette politique s'applique à l'ensemble des systèmes développés, acquis ou maintenus par Neo Financia, qu'ils soient réalisés en interne ou par des prestataires externes.

Sécurité dans le cycle de vie de développement

Modèle de cycle de vie sécurisé (S-SDLC)

Neo Financia a adopté un cycle de développement sécurisé intégrant la sécurité à chaque étape.

Phase	Activités de sécurité	Livrables	Responsables
Analyse des besoins	- Identification des exigences de sécurité		
- Classification des données traitées			
- Évaluation préliminaire des risques			
- Cahier des charges sécurité			
- Matrice de classification			
Chef de projet, Architecte sécurité			

|Conception|-
Modélisation des menaces (STRIDE/DREAD)

- Architecture de sécurité

- Choix des contrôles sécurité |-
  Document de modélisation
- Architecture sécurité validée
- Liste des contrôles

Architectes (applicatif et sécurité)			
Développement	- Application des standards de codage sécurisé		

- Revues de code orientées sécurité
- Tests unitaires sécurité
- Analyse statique (SAST) |-
  Code sécurisé
- Rapports d'analyse
- Documentation technique |Développeurs, Lead Developers| |Test|-
  Tests de sécurité dynamiques (DAST)
- Fuzzing et tests d'injection
- Tests de pénétration
- Vérification des vulnérabilités |-
  Rapports de test
- Liste des vulnérabilités
- Plan de remédiation |Testeurs, Équipe sécurité| |Déploiement|-
  Revue de sécurité pré-production
- Scan de vulnérabilités
- Configuration sécurisée
- Plan de durcissement |-
  Checklist déploiement
- Documentation d'exploitation
- Procédures de secours |DevOps, Équipe sécurité| |Maintenance|-
  Surveillance sécurité
- Gestion des vulnérabilités

- Application des correctifs
- Audits périodiques |-
  Rapports de surveillance
- Journal des correctifs
- Résultats d'audit |Équipe d'exploitation, Sécurité opérationnelle| |Retrait|-
  Plan de désactivation sécurisée
- Protection des données résiduelles |-
  Procédure de retrait
- Attestation de suppression |Chef de projet, Architecte, Sécurité|

- Révocation des accès et certificats

Modèle DevSecOps

Neo Financia a adopté l'approche DevSecOps avec un niveau de maturité actuel de 3/5, visant une progression à 4/5 dans les 24 prochains mois. Cette approche se caractérise par :

- Intégration continue (CI) : Tests de sécurité automatisés à chaque commit
- Déploiement continu (CD) : Processus automatisé incluant les validations de sécurité
- "Shift Left" Security : Déplacement des contrôles de sécurité au plus tôt dans le cycle
- Infrastructure as Code (IaC) : Définition et validation de l'infrastructure par code
- Automatisation des tests : Batterie de tests sécurité exécutés automatiquement
- Feedback rapide : Retour immédiat aux développeurs sur les problèmes de sécurité
- Collaboration étroite : Travail conjoint des équipes Dev, Sec et Ops

Pipeline CI/CD sécurisé

Neo Financia a implémenté un pipeline CI/CD avec les contrôles de sécurité suivants :

Pipeline DevSecOps Neo Financia :

flowchart LR Developpeur --> CommitReview["Commit\n+ Review"] CommitReview --> Build Build --> Test

CommitReview --> PreCommit["Pre-commit\nhooks"] Build --> SAST["SAST\nDeps scan"] Test --> DAST["DAST\nFuzzing"]

DAST --> SecurityGate["Security\nGate"] SecurityGate --> Deploy["Deploy\nCSPM"] Deploy --> Monitoc["Monitoc\nRASP"]

subgraph "Contrôles de sécurité" PreCommit SAST DAST SecurityGate Deploy Monitoc end

Les contrôles appliqués à chaque étape comprennent

Étape	Contrôles de sécurité	Outils
Pre-commit	- Détection de secrets (clés, mots de passe)	
Git hooks, linters, scanners légers		

| |-
Vérification de conformité au style

- Analyse de sécurité locale simple

Commit/Build	- Analyse statique (SAST)	

- Scan des dépendances (SCA)
- Vérification de conformité aux standards |SonarQube, OWASP Dependency Check|
|Test|-
Tests dynamiques (DAST)
- Fuzzing des API et interfaces
- Tests de sécurité automatisés |OWASP ZAP, tests personnalisés| |Security Gate|-
Validation des résultats de sécurité
- Application des règles d'acceptation
- Approbation formelle si nécessaire |Dashboard sécurité, workflow approbation|
|Deploy|-
Validation des configurations
- Scan de vulnérabilités pré-production
- Vérification des secrets et compliance |CSPM, scanners de vulnérabilités|
|Monitoc|-
Surveillance runtime (RASP)
- Détection d'anomalies comportementales
- Alertes de sécurité en temps réel |Solutions RASP, monitocing applicatif|

Exigences de sécurité des systèmes

Spécifications de sécurité

Neo Financia a défini des exigences de sécurité applicables à tous les développements.

Catégorie	Exigences	Applicabilité
Authentification	- MFA obligatoire pour les fonctions sensibles	
- Mécanismes anti-bruteforce		
- Gestion sécurisée des sessions		
- Authentification contextuelle adaptative		
Toutes les applications avec authentification		

|Autocisation|-
Contrôle d'accès par rôle (RBAC)

- Validation côté serveur obligatoire
- Principe du moindre privilège
- Séparation des tâches pour les opérations critiques

Toutes les applications multi-utilisateurs		
Protection des données	- Chiffrement des données sensibles (transit et repos)	

- Minimisation des données collectées
- Masquage des données sensibles à l'affichage
- Suppression sécurisée des données obsolètes |Applications traitant des données classifiées| |Validation des entrées|-
  Validation complète côté serveur
- Filtrage des caractères dangereux
- Protection contre les injections (SQL, XSS, etc.)
- Validation des fichiers uploadés |Toutes les applications avec saisie utilisateur| |Journalisation|-
  Traçabilité des actions sensibles

- Horodatage précis et fiable
- Protection des logs contre la modification
- Absence de données sensibles dans les logs |Toutes les applications critiques|
|APIs|-
Authentification forte pour toutes les API
- Rate limiting et anti-automation
- Validation des schémas de requêtes
- Gestion granulaire des tokens et scopes |Toutes les API internes et externes|
|Interface|-
Protection CSRF
- Headers de sécurité (CSP, X-Frame-Options, etc.)
- Gestion sécurisée des cookies
- Communications exclusivement HTTPS |Applications web et hybrides|

Règles de codage sécurisé

Neo Financia a établi un ensemble de règles de développement sécurisé adaptées à chaque langage et technologie.

- Standards généraux : Conformité aux principes OWASP ASVS niveau 2 (minimum) ou 3 (applications critiques)
- Guidelines par langage : Java Secure Coding Guidelines, JavaScript OWASP CheatSheet, etc
- Frameworks sécurisés : Utilisation privilégiée des frameworks validés par la sécurité
- Patterns sécurisés : Modèles de conception intégrant les bonnes pratiques de sécurité
- Anti-patterns : Documentation des pratiques à éviter avec alternatives sécurisées
- Librairies approuvées : Liste des bibliothèques validées par la sécurité

Ces règles sont documentées dans un référentiel accessible à tous les développeurs et font l'objet d'une formation obligatoire.

Bibliothèque de composants sécurisés

Neo Financia maintient une bibliothèque de composants pré-validés pour accélérer le développement sécurisé :

- Framework d'authentification : Implémentation validée des mécanismes d'authentification
- Module de gestion des sessions : Gestion sécurisée des sessions utilisateurs

- Composants de validation : Filtres et validateurs pour les différents types d'entrées
- Librairies cryptographiques : Implémentations validées des algorithmes cryptographiques
- Connecteurs sécurisés : Modules d'accès aux bases de données. APIs. etc
- Templates UI sécurisés : Composants d'interface intégrant les protections CSRF, XSS, etc

Chaque composant est documenté, testé et maintenu en intégrant les correctifs de sécurité dès leur disponibilité.

Environnement de développement sécurisé

Neo Financia applique des mesures spécifiques pour sécuriser ses environnements de développement

Sécurisation des environnements

- Isolation réseau : Séparation stricte des environnements de développement
- Contrôle d'accès : Accès limité aux développeurs autocisés
- Protection du code source : Système de gestion de versions sécurisé
- Données de test : Utilisation de jeux de données synthétiques ou anonymisés
- Configuration sécurisée : Durcissement des serveurs de développement
- Surveillance : Monitocing des activités suspectes

Postes développeurs

- Durcissement : Sécurisation des postes de travail des développeurs
- IDE sécurisé : Configuration sécurisée des environnements de développement
- Scan local : Outils d'analyse intégrés aux IDE
- Gestion des secrets : Utilisation d'un coffre-fort pour les secrets de développement
- Formation : Sensibilisation spécifique aux risques liés au développement

Gestion du code source

- Dépôt sécurisé : Système de gestion de versions avec contrôle d'accès granulaire
- Protection des branches : Restrictions sur les branches principales
- Revue de code : Processus obligatoire de revue par les pairs
- Intégrité du code : Signatures et vérification des commits
- Scan automatisé : Analyse du code à chaque commit
- Suivi des vulnérabilités : Intégration des outils de suivi des failles

Sécurité des API

Neo Financia accorde une importance particulière à la sécurisation de ses API, essentielles à son modèle d'affaires de néobanque:

Principes de sécurisation API

- Defense in Depth : Multiple couches de protection pour chaque API
- Zero Trust : Vérification systématique de chaque requête
- Least Privilege : Limitation des droits au strict nécessaire
- Secure by Default : Configuration restrictive par défaut
- Fail Secure : En cas d'erreur, blocage par défaut

Contrôles de sécurité API

Domaine	Contrôles implémentés
Authentification	- OAuth 2.0 avec OpenID Connect
- Authentification mutuelle TLS pour les API partenaires	
- Signatures API (JWT, HMAC)	
- Authentification contextuelle selon le risque	
Autocisation	- Scopes OAuth granulaires
- Vérification fine des permissions	
- Validation systématique côté serveur	
- Séparation des rôles (RBAC/ABAC)	
Protection des données	- Chiffrement TLS 1.3 obligatoire
- Tokenisation des données sensibles	
- Filtrage des données sensibles dans les réponses	
- Validation des schémas de données	
Protection contre les attaques	- Rate limiting adaptatif
- Protection contre l'énumération	

- Détection des attaques par force brute	

	- Validation des entrées côté serveur
---	---
Surveillance	- Logging détaillé des appels API
- Monitocing des comportements anormaux	
- Alertes sur les motifs d'attaque	
- Analyse de trafic en temps réel	

Gestion des API Open Banking

Néo Financia applique des mesures spécifiques pour ses API ouvertes aux partenaires fintech.

- Processus d'onboarding : Validation rigoureuse des partenaires API
- API Gateway dédiée : Infrastructure spécifique pour les API externes
- Sandbox sécurisée : Environnement de test isolé pour les partenaires
- Documentation sécurité : Guide d'implémentation sécurisée pour les partenaires
- Surveillance dédiée : Monitocing spécifique des API partenaires
- Limitations adaptatives : Quotas et throttling adaptés au profil de chaque partenaire
- Intégration avec Mangopay/Lemonway : Sécurisation spécifique des flux financiers

Tests de sécurité

Neo Financia a mis en place un programme complet de tests de sécurité pour ses applications et infrastructures

Types de tests implémentés

Type de test	Description	Fréquence	Responsable
SAST (Static Application Security Testing)	Analyse statique du code source pour identifier les vulnérabilités	À chaque commit	Automatisé (pipeline)

SCA (Software Composition Analysis)	Analyse des dépendances et bibliothèques tierces	À chaque build	Automatisé (pipeline)
DAST (Dynamic Application Security Testing)	Tests dynamiques sur l'application en fonctionnement	Hebdomadaire et avant déploiement	Automatisé + Équipe sécurité
IAST (Interactive Application Security Testing)	Analyse interactive pendant les tests fonctionnels	Durant phase de test	Équipe QA + Sécurité
Test de pénétration	Tests manuels approfondis par des experts	Trimestriel et avant lancement	Équipe interne + prestataires

---

Fuzzing	**Tests d'injection de données aléatoires/malformées**	**Mensuel pour les API critiques**	**Automatisé + Équipe sécurité**
Scan de vulnérabilités	Détection des vulnérabilités connues	Hebdomadaire	Équipe sécurité
Scan de configuration	Vérification des configurations sécurisées	Quotidien	Automatisé (CSPM)

Couverture des tests

- Applications critiques : 100% des fonctionnalités avec tous les types de tests
- Applications standard : SAST, SCA et DAST systématiques, pentest avant déploiement
- API exposées : Tests complets incluant fuzzing et tests d'authentification
- Infrastructure : Scan de vulnérabilités et de configuration
- Environnements cloud : CSPM continu et tests spécifiques clouc
- Mobiles : Tests spécifiques incluant analyse de l'application et communication

Gestion des résultats

- Centralisation : Consolidation des résultats dans une plateforme unique
- Priorisation : Classification selon criticité (CVSS) et contexte
- Déduplication : Élimination des doublons pour focus sur problèmes uniques
- Assignation : Attribution aux équipes responsables
- Suivi : Tracking de la résolution jusqu'à validation
- Reporting : Tableaux de bord et rapports de tendance
- Retour d'expérience : Analyse des causes racines pour amélioration continue

Gestion des données de test

Neo Financia applique des règles strictes pour la gestion des données utilisées en développement et test.

Principes de gestion des données

- Interdiction des données réelles : Proscription de l'utilisation de données de production dans les environnements non-productifs
- Anonymisation robuste : Techniques d'anonymisation irréversible si des données dérivées de production sont nécessaires
- Données synthétiques : Génération de jeux de données artificiels mais réalistes
- Validation juridique : Approbation DPO pour les méthodes d'anonymisation
- Contrôles d'accès : Protection renforcée des données de test
- Surveillance : Détection des fuites potentielles de données de production

Techniques d'anonymisation

Lorsque l'anonymisation est requise, Neo Financia utilise des techniques avancées.

- Masquage : Remplacement partiel des données (ex: XXXX XXXX XXXX 1234 pour les cartes)

- Tokenisation : Remplacement par des jetons sans relation avec l'origina
- Brouillage : Modification des données tout en conservant le format
- Randomisation : Remplacement par des valeurs aléatoires de même type
- Agrégation : Utilisation de données statistiques plutôt que individuelles
- Permutation : Mélange des valeurs entre différents enregistrements

Plateforme de données de test

- Infrastructure dédiée : Environnement spécifique pour la gestion des données de test
- Générateurs : Outils de création de données synthétiques
- Subsetting : Extraction d'échantillons représentatifs
- Versionning : Gestion des versions des jeux de données
- API de provisionnement : Services d'alimentation des environnements
- Validation : Contrôles de qualité et de représentativité

Acquisition et développement externe

Neo Financia applique des mesures spécifiques pour sécuriser les développements externes et l'acquisition de logiciels

Exigences pour les prestataires

- Clauses contractuelles : Obligations de sécurité dans les contrats
- Annexe sécurité : Détail des exigences techniques et organisationnelles
- Engagement de confidentialité : Protection des informations transmises
- Droit d'audit : Possibilité de vérifier les pratiques sécurité
- Certification : Exigence de certifications (ISO 27001) pour les prestataires critiques
- Propriété du code : Clarification des droits sur le code développé
- Processus de validation : Modalités de recette et d'acceptation

Évaluation des logiciels tiers

Avant l'acquisition ou l'utilisation d'un logiciel tiers, Neo Financia procède à une évaluation structurée

- Due diligence sécurité : Analyse approfondie des pratiques de sécurité de l'éditeur
- Analyse de vulnérabilités : Recherche de failles connues
- Scan de code : Analyse du code source quand disponible
- Test en environnement isolé : Validation préalable en sandbox
- Évaluation RGPD/conformité : Vérification des aspects juridiques et réglementaires
- Analyse des conditions de support : Réactivité sur les correctifs de sécurité
- Histocique de sécurité : Étude du track record de l'éditeur

Intégration sécurisée

- Configuration sécurisée : Application systématique des meilleures pratiques
- Moindre privilège : Limitation des droits accordés aux applications tierces
- Isolation : Cloisonnement des composants externes
- Surveillance spécifique : Monitocing renforcé des comportements

---

- Plan de secours : Stratégie de sortie en cas de problème
- Gestion des mises à jour : Processus de maintien à jour

Gestion des changements techniques

Néo Financia encadre strictement les modifications apportées aux systèmes en production

Processus de gestion des changements

- Demande : Expression formelle du besoin de changement
- Évaluation d'impact : Analyse des conséquences potentielles
- Évaluation sécurité : Revue spécifique des aspects sécurité
- Approbation : Validation formelle selon le niveau de risque
- Planification : Organisation de la mise en œuvre
- Test : Validation préalable en environnement de test
- Mise en œuvre : Déploiement contrôlé du changement
- Vérification : Contrôle post-déploiement
- Documentation : Mise à jour de la documentation
- Revue : Analyse de l'efficacité du changement

Changements d'urgence

- Processus accéléré : Circuit rapide pour les correctifs critiques
- Validation minimale : Tests essentiels pré-déploiement
- Documentation a posteriori : Formalisation après mise en œuvre
- Surveillance renforcée : Monitocing accru post-déploiement
- Revue post-incident : Analyse détaillée après stabilisation

Séparation des environnements

- Environnement de développement : Élaboration du code et tests unitaires
- Environnement de test : Validation fonctionnelle et technique
- Environnement de pré-production : Tests d'intégration et de charge
- Environnement de production : Exploitation des applications
- Contrôles de séparation : Isolation réseau, accès distincts, données séparées
- Promotion contrôlée : Processus formel de passage entre environnements

Gestion des incidents de sécurité

Principes fondamentaux

La gestion des incidents de sécurité constitue une composante essentielle du dispositif global de cybersécurité de Neo Financia. Elle vise à assurer une détection précoce, une réponse efficace et une résolution rapide des événements susceptibles d'affecter la confidentialité, l'intégrité ou la disponibilité des systèmes d'information et des données, tout en minimisant leur impact sur l'activité.

Objectifs de la gestion des incidents de sécurité :

- Détecter rapidement les incidents de sécurité avérés ou potentiels
- Répondre de manière coordonnée et efficace aux incidents
- Limiter l'impact opérationnel, financier et réputationnel des incidents
- Assurer la continuité des services essentiels pendant la gestion des incidents
- Respecter les obligations légales et réglementaires de notification
- Tirer les enseignements de chaque incident pour renforcer le dispositif de protection
- Maintenir la confiance des clients et des partenaires dans la capacité de Neo Financia à protéger leurs données

Cette politique s'applique à l'ensemble des incidents de sécurité, qu'ils affectent l'infrastructure interne, les services cloud, les applications métier ou les données, et concerne tous les collaborateurs, prestataires et partenaires.

Organisation et responsabilités

Structure organisationnelle

Neo Financia a mis en place une organisation dédiée pour la gestion des incidents de sécurité

- Security Operations Center (SOC) : Équipe de surveillance et détection 24/7
- Computer Emergency Response Team (CERT) : Équipe d'intervention et de résolution
- Cellule de crise cyber : Structure activée pour les incidents majeurs
- Coordinateur incidents : Rôle pivot assurant le suivi global des incidents

Rôles et responsabilités

Rôle	Responsabilités	Profil type
Analyste SOC	- Surveillance des alertes de sécurité	
- Qualification initiale des incidents		
- Déclenchement des procédures de réponse		
- Documentation des incidents		
Spécialiste sécurité opérationnelle		
Responsable CERT	- Coordination de la réponse technique	
- Affectation des ressources		
- Évaluation de l'impact technique		
Expert sécurité avec compétences en gestion d'incident		

| |• Validation des actions de remédiation| | | |---|---|---| |Intervenant CERT|- Analyse technique approfondie

- Containment et éradication
- Collecte des preuves
- Reconstruction des systèmes affectés |Technicien sécurité spécialisé par domaine| |Coordinateur d'incident|-
  Suivi global de l'incident
- Communication interne et reporting
- Coordination inter-équipes
- Maintien du journal des événements |Profil sécurité avec compétences en

coordination| |RSSI|-
Supervision stratégique

- Décision d'escalade en crise
- Communication vers la direction
- Interface avec les autocités |Responsable sécurité senior| |Directeur de crise|-
Pilotage de la cellule de crise
- Arbitrage des décisions stratégiques
- Validation du plan d'action global
- Reporting au COMEX |RSSI ou membre du COMEX selon gravité| |Responsable communication|-
Élaboration des messages
- Communication externe
- Relations médias
- Information clients |Directeur Communication| |Responsable juridique|-
Analyse des obligations légales
- Notifications réglementaires
- Gestion des aspects juridiques |Juriste spécialisé cybersécurité|

	• **Conseil sur la collecte de preuves**	
Délégué à la Protection des Données	- Évaluation de l'impact RGPD	
- Notification à la CNIL/ICO		
- Information des personnes concernées		
- Documentation RGPD de l'incident		
DPO		

Matrice RACI pour les incidents

Activité	Analyste SOC	CERT	Coordinateur	RSSI	DSI	Direction	Commun
Détection	R	C	I	I	I	-	-

Qualification	R	A	C	I	I	-	-
Analyse technique	C	R	I	A	C	-	-
Containment	I	R	I	A	C	I	-
Éradication	-	R	I	A	C	I	-
Communication interne	I	C	R	A	I	I	C
Communication externe	-	I	C	A	I	A	R
Notification réglementaire	-	I	C	A	I	I	I
Gestion de crise	I	C	C	R/A	C	A	C
Retour à la normale	I	R	C	A	C	I	I
Analyse post-	C	C	R	A	C	I	I

Légende: R = Responsible, A = Accountable, C = Consulted, I = Informec

Détection et signalement des incidents

Sources de détection

Neo Financia s'appuie sur de multiples sources pour détecter les incidents de sécurité.

- Outils de détection automatisés
- SIEM (Security Information and Event Management)
- EDR (Endpoint Detection and Response)
- NDR (Network Detection and Response)
- Systèmes de détection d'intrusion (IDS/IPS)
- Solutions de protection des données (DLP)
- Outils de surveillance cloud (CASB, CSPM)
- Alertes manuelles
- Signalements des collaborateurs
- Remontées des clients via le support
- Observations des équipes IT
- Notifications des partenaires

- Sources externes
- Services de Threat Intelligence
- CERT nationaux (CERT-FR, NCSC-UK)
- Communautés sectocielles (FS-ISAC)
- Notifications des fournisseurs

Processus de signalement

Neo Financia a établi des canaux dédiés pour le signalement des incidents :

- Pour les collaborateurs internes
- Portail intranet dédié (https://security.neofinancia.internal)
- Adresse email spécifique (cert@neofinancia.eu)
- Numéro d'astreinte sécurité (24/7)
- Application mobile de signalement
- Pour les clients
- Support client avec procédure d'escalade sécurité
- Formulaire web dédié aux signalements de sécurité
- Section sécurité dans l'application mobile
- Pour les partenaires et prestataires
- Point de contact défini dans les contrats
- Procédure de notification incluse dans les clauses
- Canal direct vers le CERT pour les partenaires critiques

Disponibilité des canaux

- Surveillance 24/7/365 par l'équipe SOC
- Astreinte sécurité permanente pour les incidents critiques
- Redondance des moyens de communication (téléphone, email, applications)
- Procédures dégradées en cas d'indisponibilité des canaux habituels

Classification et priorisation des incidents

Critères de classification

Neo Financia classifie les incidents de sécurité selon plusieurs dimensions

Type d'incident

- Atteinte à la confidentialité : Divulgation non autocisée d'informations

- Atteinte à l'intégrité : Altération non autocisée de données ou systèmes
- Atteinte à la disponibilité : Interruption de service ou d'accès
- Fraude : Utilisation malveillante des systèmes à des fins frauduleuses
- Malware : Infection par logiciel malveillant
- Accès non autocisé : Intrusion ou élévation de privilèges
- Ingénierie sociale : Phishing, usurpation d'identité, manipulation
- Attaque DoS : Déni de service

Périmètre concerné

- Applications critiques : Services bancaires core, paiements
- Services clients : Applications web/mobiles, interfaces client
- Infrastructure interne : Systèmes internes, réseau, postes de travail
- Environnements cloud : Azure. AWS. OVHcloud
- Services partenaires : Intégrations avec Mangopav. Lemonwav. etc.
- Données sensibles : Informations clients, données financières

Échelle de gravité

Néo-Financia utilise une échelle à 5 niveaux pour évaluer la gravité des incidents.

Niveau Désignation Critères Exemples SLA de réponse

Désignation

Critères

SLA de réponse

|1|Critique|-
Impact majeur sur les services critiques

- Atteinte à un volume important de données sensibles
- Risque significatif pour l'image ou la conformité
- Impact financier potentiel > 1M€ |-
  Compromission de la plateforme de paiement
- Exfiltration massive de données clients
- Attaque ciblée sur les systèmes core banking

Immédiat (< 15 min)				
2	Majeur	- Impact significatif sur des services importants		

- Atteinte à des données sensibles limitées
- Risque modéré pour l'image ou la conformité

- Impact financier potentiel 100k€-1M€ |-
  Compromission d'un serveur de production
- Fraude avérée via un canal digital
- Indisponibilité partielle d'un service client |< 1 heure| |3|Modéré|-
  Impact limité sur des services non critiques
- Atteinte potentielle à des données non sensibles
- Risque limité pour l'image ou la conformité
- Impact financier potentiel 10k€-100k€ |-
  Infection par malware sans propagation
- Tentative d'intrusion détectée et bloquée
- Vol d'équipement chiffré |< 4 heures| |4|Mineur|-
  Impact très limité sans conséquence sur les services
- Pas d'atteinte aux données sensibles
- Pas de risque pour l'image ou la conformité
- Impact financier potentiel < 10k€ |-
  Tentative de phishing générique
- Violation de politique sans conséquence
- Détection d'une vulnérabilité non exploitée |< 24 heures|

---

5 Information

- Événement de sécurité sans impact
- Alerte nécessitant une surveillance
- Aucun risque identifié à ce stade
- Tentative d'accès bloquée par défense périmétrique
- Comportement anormal isolé
- Alerte de bas niveau nécessitant analyse

< 72 heures

Matrice de priorisation

La priorisation des incidents combine la gravité avec l'urgence.

Gravité Urgence	Immédiate	Élevée	Moyenne	Basse
Critique (1)	P1	P1	P2	P2
Majeur (2)	P1	P2	P2	P3
Modéré (3)	P2	P3	P3	P4
Mineur (4)	P3	P3	P4	P4
Information (5)	P3	P4	P4	P4

Cette priorisation détermine le niveau de mobilisation et les processus applicables.

- P1 (Rouge) : Mobilisation immédiate, traitement prioritaire, escalade direction
- P2 (Orange) : Traitement prioritaire dans la journée, notification management
- P3 (Jaune) : Traitement planifié, notification équipe concernée
- P4 (Vert) : Traitement standard, suivi dans les processus habituels

Procédures de réponse aux incidents

Processus général de gestion des incidents

Neo Financia a établi un processus structuré en 6 phases pour la gestion des incidents de sécurité.

1. Détection et signalement

- Identification de l'incident potentiel
- Collecte des informations initiales
- Création de l'enregistrement d'incident

2. Qualification et triage

- Évaluation de la gravité et de l'urgence
- Classification et priorisation
- Escalade selon le niveau de priorité

---

3. Confinement et analyse

- Limitation de la propagation
- Protection des systèmes non affectés
- Investigation technique approfondie
- Détermination de l'étendue de l'impact

4. Éradication et remédiation

- Élimination de la cause racine
- Suppression des accès malveillants
- Application des correctifs nécessaires
- Renforcement des contrôles défaillants

5. Retour à la normale

- Restauration des systèmes et services
- Validation du bon fonctionnement
- Surveillance post-incident
- Fermeture formelle de l'incident

6. Analyse post-incident

- Revue détaillée de l'incident
- Identification des leçons apprises
- Définition des actions d'amélioration
- Documentation et partage des enseignements

Procédures spécifiques par type d'incident

Neo Financia a développé des playbooks spécifiques pour les principaux types d'incidents :

Type d'incident	Actions spécifiques	Équipes impliquées	Outils dédiés
Fuite de données	- Identification des données compromises		
- Fermeture du canal de fuite			
- Évaluation des impacts RGPD			
- Notification aux autocités si nécessaire			
- CERT			
- DPO			
- Juridique			
- DSI			

Solutions DLP, forensics			
Malware / Ransomware	- Isolation des systèmes infectés		
- Analyse du malware			
- Blocage des domaines C2			
- Restauration depuis backups sains			
- CERT			
- Équipe infrastructure			
- Équipe EDR			
EDR, sandbox, outils forensics			
Compromission de compte	- Blocage immédiat du compte		
- IAM team			
- CERT			
SIEM, IAM, UEBA			

|Attaque DDoS|-
Analyse des activités suspectes

- Reset des accès et credentials
- Vérification des systèmes accédés |-
  Équipe SOC

Solutions anti-DDoS, WAF			
- Activation des contre-mesures anti-DDoS			

- Traffic scrubbing

- Ajustement des règles de filtrage
- Communication vers les utilisateurs |-
  Équipe réseau
- SOC
- Prestataire anti-DDoS | |Fraude financière|-
  Blocage des transactions suspectes
- Traçage des flux financiers
- Contact des établissements destinataires
- Analyse des vecteurs d'attaque |-
  Équipe anti-fraude
- CERT
- Équipe métier
- Juridique |Outils anti-fraude, traçabilité| |Intrusion système|-
  Isolation du système compromis
- Recherche des IOCs
- Analyse des journaux
- Reconstruction sécurisée |-
  CERT
- Équipe système
- SOC |Outils forensics, EDR, SIEM| |Incident cloud|-
  Analyse des logs cloud spécifiques
- Revue des configurations IAM
- Isolation des ressources compromises
- Application des bonnes pratiques cloud |-
  Cloud Security team
- CERT
- Cloud Ops |CSPM, CWP, CASB|

Procédures d'escalade

Neo Financia a défini un processus d'escalade par niveau :

Niveau	Déclenchement	Intervenants	Actions
Niveau 1	Tous incidents	Équipe SOC et CERT	- Traitement standard selon playbooks
- Coordination technique			
- Résolution des incidents P3-P4			
Niveau 2	Incidents P2 et escalade N1	RSSI, responsables équipes concernées	- Coordination renforcée
- Allocation de ressources supplémentaires			
- Information du management			
Niveau 3 - Crise	Incidents P1 et escalade N2	Cellule de crise (RSSI, DSI, DG, Comm, Juridique)	- Activation de la cellule de crise
- Pilotage stratégique			
- Décisions de haut niveau			
- Communication externe			

Activation de la cellule de crise

- Déclenchement automatique pour tout incident P1
- Déclenchement sur décision du RSSI pour les incidents P2 évolutifs
- Composition adaptable selon la nature de l'incident

- Salle de crise physique et virtuelle disponible 24/7
- Moyens de communication dédiés et sécurisés
- Portail de crise pour centraliser les informations
- Procédures de relève pour les crises de longue durée

Conservation des preuves et investigation

Principes de collecte des preuves

Neo Financia applique les principes suivants pour la collecte et la préservation des preuves numériques :

- Non-altération : Préservation de l'intégrité des preuves
- Exhaustivité : Collecte complète des éléments pertinents
- Authenticité : Garantie de l'origine et de l'exactitude
- Traçabilité : Documentation de la chaîne de possession
- Reproductibilité : Méthodes permettant de répéter l'analyse
- Proportionnalité : Équilibre entre préservation et continuité d'activité

Techniques de collecte

Type de preuve	Méthode de collecte	Outils utilisés
Images disque	Copie forensique bit-à-bit	Outils forensiques professionnels
Mémoire vive	Capture de mémoire à chaud	Outils d'acquisition mémoire
Journaux système	Extraction et sauvegarde sécurisée	Scripts d'extraction, SIEM
Trafic réseau	Capture de paquets ciblée	Analyseurs de protocole, sondes
Données cloud	API forensiques cloud	Solutions CASB, outils cloud natifs
Artefacts malware	Extraction sécurisée, sandboxing	Solutions d'analyse de malware

Chaîne de conservation

Pour garantir l'admissibilité juridique des preuves, Neo Financia maintient une chaîne de conservation rigoureuse.

- Documentation initiale : Enregistrement des circonstances de collecte (date, heure, lieu, méthode, responsable)
- Hachage cryptographique : Calcul et enregistrement des empreintes numériques (SHA-256)
- Stockage sécurisé : Conservation dans un environnement à accès restreint et journalisé
- Registre des accès : Documentation de toute manipulation des preuves

- Scellés numériques : Protection contre la modification non autocisée
- Conservation longue durée : Archivage selon les exigences légales (minimum 1 an)

Investigation numérique

Neo Financia conduit les investigations selon une méthodologie structurée

- Analyse préliminaire : Évaluation rapide pour orienter l'investigation
- Hypothèses de travail : Formulation des scénarios possibles
- Plan d'investigation : Définition des étapes et ressources
- Analyse technique : Examen des preuves collectées
- Corrélation : Mise en relation des différents éléments
- Chronologie : Reconstitution de la séquence des événements
- Attribution : Identification des acteurs si possible
- Documentation : Rapport détaillé des conclusions

Communication et notification

Communication interne

Neo Financia a défini des processus de communication interne adaptés à chaque niveau d'incident :

|Équipes techniques concernées|-
Détails techniques complets

- Actions requises
- Indicateurs de compromission

Temps réel	**Outil de gestion d'incidents, chat sécurisé**		
Management intermédiaire	- Synthèse de l'incident		

- Impact sur les services
- Mesures en cours |Régulière (selon gravité)|Email sécurisé, réunions de suivi| |Direction générale|-
Résumé exécutif
- Impact business
- Risques associés
- Décisions requises |Points clés (P1-P2)|Rapports formels, briefings| |Ensemble

des collaborateurs|-
Information générale

- Consignes de sécurité
- Précautions à prendre |Si nécessaire (impact large)|Intranet, email, alertes|

Communication externe

La communication externe est strictement encadrée et coordonnée par la Direction de la Communication en lien avec le RSSI et la Direction Juridique :

- Clients
- Messages clairs et factuels sur l'impact
- Consignes pratiques et précautions
- Canaux multiples : app mobile, site web, email, SMS
- Ligne dédiée au support client en cas de crise
- Partenaires
- Information adaptée selon l'impact sur les services partagés
- Communication directe via les points de contact désignés
- Coordination des mesures conjointes si nécessaire
- Médias
- Communiqués de presse préparés selon des templates validés
- Porte-parole désignés et formés
- Validation juridique systématique
- Réactivité et transparence appropriée
- Autocités et régulateurs
- Respect strict des obligations légales de notification

- Format conforme aux exigences réglementaires
- Suivi des communications et mises à jour

Obligations de notification réglementaire

Neo Financia respecte les obligations légales de notification des incidents

Autocité	Type d'incident	Délai de notification	Responsable
CNIL (France)	Violation de données personnelles	72 heures maximum	DPO

ICO (UK)	Violation de données personnelles	48 heures maximum	DPO UK
ACPR (France)	Incident opérationnel significatif	24 heures maximum	RSSI + Conformité
FCA (UK)	Incident opérationnel significatif	24 heures maximum	Conformité UK
ANSSI (France)	Incident de sécurité significatif	24 heures maximum	RSSI
NCSC (UK)	Incident de sécurité significatif	24 heures recommandé	RSSI
BCE/BDF	Incident majeur de paiement	4 heures maximum	Responsable Paiements + RSSI

Des modèles de notification préapprouvés sont disponibles pour chaque autocité afin de garantir la conformité et la rapidité de réaction.

Analyse post-incident et retour d'expérience

Revue post-incident

Neo Financia conduit systématiquement une analyse approfondie après chaque incident significatif (P1-P2) et périodiquement pour les incidents mineurs regroupés :

- Objectifs de l'analyse
- Comprendre les causes profondes
- Évaluer l'efficacité de la réponse
- Identifier les améliorations possibles
- Partager les enseignements
- Processus d'analyse
- Collecte des informations factuelles
- Chronologie détaillée des événements

- Analyse des causes racines
- Évaluation de l'efficacité des mesures
- Identification des facteurs contributifs
- Participants
- Coordinateur d'incident
- Intervenants clés
- Représentants des équipes concernées
- Facilitateur neutre
- RSSI ou représentant

Méthodologie d'analyse des causes

Neo Financia applique une analyse structurée pour identifier les causes profondes

- Analyse des 5 pourquoi : Questionnement itératif pour remonter aux causes fondamentales
- Diagramme d'Ishikawa : Représentation des facteurs contributifs

- Analyse chronologique : Étude de la séquence des événements
- Analyse des écarts : Comparaison avec les processus attendus
- Examen des facteurs humains : Évaluation des aspects organisationnels et comportementaux

Documentation et partage

Les enseignements sont formalisés et partagés sous plusieurs formats.

- Rapport post-incident : Document détaillé comprenant
- Résumé exécutif
- Chronologie détaillée
- Analyse technique
- Causes identifiées
- Recommandations
- Plan d'action
- Fiches de retour d'expérience : Synthèses ciblées pour différentes audiences
- Base de connaissances : Alimentation de la base documentaire interne
- Sessions de partage : Présentations et discussions avec les équipes concernées

Amélioration continue

Chaque incident contribue à l'amélioration du dispositif de sécurité

- Plan d'action correctif : Mesures spécifiques pour adresser les vulnérabilités identifiées
- Mise à jour des procédures : Révision des playbooks et processus
- Adaptation des contrôles : Renforcement des mécanismes de protection
- Évolution de la formation : Intégration des enseignements dans les programmes de sensibilisation
- Suivi des indicateurs : Mesure de l'efficacité des améliorations

Un suivi formel des actions d'amélioration est réalisé par le RSSI et présenté régulièrement au COSEC.

Exercices et préparation

Programme d'exercices

Neo Financia maintient un programme d'exercices réguliers pour tester et améliorer sa capacité de réponse aux incidents.

Type d'exercice	Description	Fréquence	Participants
Table-top	Scénarios discutés en salle sans action technique	Trimestriel	Management, équipes cyber
Exercice fonctionnel	Test des procédures spécifiques en environnement contrôlé	Semestriel	Équipes techniques concernées
Simulation	Incidents simulés en	Semestriel	CERT, SOC,

technique	environnement de test		équipes IT
Exercice complet	Simulation réaliste avec tous les aspects	Annuel	Organisation complète
Red Team	Test adversarial avec équipe offensive	Annuel	Organisation complète (information limitée)

Scénarios d'exercice

Les exercices couvrent divers scénarios alignés sur les menaces pertinentes pour Neo Financia.

- Compromission d'API : Attaque ciblant les services bancaires ouverts
- Ransomware majeur : Infection touchant les systèmes critiques
- Fuite de données clients : Exfiltration d'informations sensibles
- Fraude sophistiquée : Attaque ciblant les systèmes de paiement
- Attaque de la supply chain : Compromission via un partenaire ou fournisseur
- Attaque DDoS massive : Indisponibilité des services en ligne
- Incident cloud majeur : Défaillance ou compromission d'un fournisseur cloud

Préparation et ressources

Neo Financia maintient un niveau de préparation élevé face aux incidents

- Kits de réponse aux incidents : Ressources prêtes à l'emploi
- Accès d'urgence : Procédures de break-glass pour les situations critiques
- Contrats de support : Assistance externe mobilisable rapidement
- Formation spécialisée : Équipes formées aux techniques d'intervention
- Surveillance proactive : Veille sur les menaces émergentes
- Coordination externe : Relations établies avec les CERT sectociels et nationaux

Continuité d'activité et résilience

Principes fondamentaux

La continuité d'activité et la résilience opérationnelle sont essentielles pour Neo Financia en tant que néobanque dont les services sont accessibles 24/7. Cette politique vise à garantir la disponibilité des services critiques en cas d'incident majeur, tout en respectant les exigences réglementaires spécifiques au secteur financier.

Objectifs de la continuité d'activité et de la résilience

- Assurer la continuité des services bancaires essentiels en toutes circonstances

- Minimiser l'impact des perturbations sur les clients et les opérations
- Permettre une reprise rapide et ordonnée après un incident
- Respecter les exigences réglementaires (DORA, ACPR, FCA)
- Renforcer la résilience globale de l'organisation face aux perturbations
- Protéger la réputation et la confiance des clients
- Limiter les impacts financiers des incidents majeurs

Cette politique s'applique à l'ensemble des activités, systèmes et ressources de Neo Financia, avec une attention particulière aux services critiques identifiés dans l'analyse d'impact métier.

Gouvernance et organisation

Structure de gouvernance

Neo Financia a mis en place une gouvernance spécifique pour la continuité d'activité et la résilience.

- Conseil d'Administration : Validation de la stratégie et des objectifs de résilience
- Comité des Risques : Supervision du dispositif de continuité
- Comité de Continuité d'Activité (CCA) : Pilotage opérationnel du dispositif
- Responsable du Plan de Continuité d'Activité (RPCA) : Coordination globale
- Correspondants PCA métiers : Relais dans chaque direction
- Cellule de Crise : Activation en cas d'incident majeur

Rôles et responsabilités

Fonction	Responsabilités principales
Responsable PCA (RPCA)	- Élaboration et maintenance de la stratégie de continuité
- Coordination des analyses d'impact métier	
- Pilotage du programme d'exercices	
- Reporting sur l'état de préparation	
Responsable des Plans de Secours Informatiques (RPSI)	- Conception des solutions techniques de reprise
- Maintien des capacités de reprise informatique	
- Tests techniques de reprise	

	• Coordination avec les fournisseurs cloud
---	---
Directeurs métiers	- Identification des activités critiques
- Validation des stratégies de continuité	
- Allocation des ressources nécessaires	
- Participation aux exercices	
Correspondants PCA	- Relais dans leur périmètre
- Maintien des procédures spécifiques	
- Formation des équipes	
- Participation aux tests	
Directeur de Crise	- Pilotage de la cellule de crise
- Prise de décisions stratégiques	
- Coordination globale des actions	
- Communication avec les instances dirigeantes	

Intégration avec la gestion des risques

Le dispositif de continuité d'activité est pleinement intégré au cadre global de gestion des risques

- Cartographie des risques opérationnels : Prise en compte des scénarios de continuité
- Indicateurs de risque partagés : KRIs communs et suivis de manière coordonnée
- Comitologie intégrée : Continuité d'activité traitée en Comité des Risques

- Reporting consolidé : Vision unifiée des risques opérationnels et de résilience
- Appétence au risque : Définition de seuils de tolérance pour les interruptions

Analyse d'impact sur l'activité (BIA)

Méthodologie d'analyse

Neo Financia conduit une analyse d'impact métier (Business Impact Analysis) structurée pour identifier les activités critiques et leurs besoins de continuité :

- Identification des processus : Cartographie complète des processus métier
- Évaluation des impacts : Analyse des conséquences d'une interruption
- Impact financier direct et indirect
- Impact client et réputationnel
- Impact réglementaire et contractuel
- Impact opérationnel interne
- Détermination des critères de criticité : Échelle d'évaluation standardisée
- Analyse des dépendances : Systèmes, ressources et fournisseurs associés

---

- 5. Définition des objectifs de continuité : RTO et RPO requis
- 6. Validation par les métiers : Confirmation par les propriétaires de processus

Classification des processus critiques

Les processus sont classifiés selon leur niveau de criticité pour l'activité.

Niveau	Description	RTO	RPO	Exemples
Critique (C1)	Processus vitaux dont l'interruption aurait un impact immédiat et majeur	< 15 min	< 15 min	- Authentification clients
- Paiements temps réel				
- Autorisation des cartes				
Essentiel (C2)	Processus dont l'interruption aurait un impact significatif au-delà de quelques heures	< 4 heures	< 1 heure	- Virements SEPA
- Consultation des comptes				
- Support client prioritaire				

Important (C3)	Processus dont l'interruption est tolérable jusqu'à une journée	< 24 heures	< 4 heures	- Ouverture de comptes
- Demande de crédit				
- Reporting client				
Standard (C4)	Processus pouvant être interrompus plusieurs jours sans impact majeur	< 72 heures	< 24 heures	- Reporting interne
- Fonctionnalités secondaires				
- Analyses marketing				

Ressources critiques identifiées

L'analyse d'impact a permis d'identifier les ressources critiques nécessaires à la continuité des services essentiels

Catégorie	Ressources critiques	Niveau de criticité
Systèmes applicatifs	- Plateforme d'authentification	
- Core banking system		
C1		

|-
Système de paiement

- APIs critiques
- Applications mobiles et web

Infrastructure	- Environnement Azure principal (70%)

- Environnement OVHcloud (20%)
- Infrastructure réseau
- Systèmes de base de données |C1| |Données|-
  Données clients
- Données transactionnelles
- Données de paiement
- Configuration des services |C1| |Partenaires externes|-
  Connexions Mangopay
- Intégration Lemonway
- Réseaux de paiement
- Fournisseurs d'identité |C1-C2| |Ressources humaines|-
  Équipe IT Ops
- Équipe sécurité
- Support client
- Management de crise |C1-C2|

Dépendances critiques

Neo Financia a cartographié les dépendances critiques entre ses systèmes et services

- Dépendances internes
- Chaîne de dépendance des applications et services
- Flux de données entre composants
- Interdépendances entre environnements cloud
- Dépendances externes
- Fournisseurs de services cloud (Azure, OVHcloud, AWS)
- Partenaires fintech (Mangopay, Lemonway)
- Prestataires de services de paiement
- Fournisseurs de télécommunications
- Fournisseurs d'énergie

Cette cartographie est maintenue à jour et sert de base à l'élaboration des stratégies de continuité.

Stratégie de continuité d'activité

Approche globale

Neo Financia a défini une stratégie globale de continuité d'activité basée sur les principes suivants

- Résilience intégrée : Conception des systèmes avec redondance native
- Redondance multi-niveaux : Application du principe N+1 minimum
- Diversité technologique : Réduction des risques de défaillance commune
- Indépendance géographique : Séparation des sites et infrastructures
- Approche multi-cloud : Répartition entre fournisseurs (Azure, OVHcloud, AWS)
- Dégradation gracieuse : Maintien des fonctions critiques en mode dégradé
- Restauration progressive : Priorisation des services selon leur criticité

Stratégies techniques

Pour atteindre ses objectifs de continuité, Neo Financia met en œuvre plusieurs stratégies complémentaires

Stratégie	Description	Cas d'application
Haute disponibilité	- Architecture redondante active-active	
- Élimination des points uniques de défaillance		
- Basculement automatique		
- Services critiques C1		
- Infrastructure réseau		
- Systèmes d'authentification		
Reprise après sinistre	- Sites de secours distincts	
- Réplication asynchrone		
- Procédures de basculement formalisées		
-		

Systèmes C1-C2		
- Bases de données transactionnelles		
- Applications métier		
Multi-cloud	- Répartition entre fournisseurs	
- Redondance inter-cloud		
- Capacité de migration		
- Services exposés aux clients		
- APIs critiques		
- Données clients		
Sauvegarde et restauration	- Stratégie 3-2-1-1-0	
- Sauvegardes fréquentes		
- Tests de restauration réguliers		
- Données transactionnelles		
- Configurations		
- Systèmes non critiques		

- Fonctionnalités minimales garanties		
- Priorisation des services essentiels		
- Réduction de la charge		
- Applications client		

- Services en cas de surcharge		
- Situation de crise majeure		

Architecture de résilience

L'architecture technique de Neo Financia intègre les principes de résilience suivants

flowchart TD A["Azure (70%)\nRegion 1"] <--> B["OVHcloud (20%)\nRegion FR"] <--> C["AWS (10%)\nRegion EU"] A --> D["API Gateway"] B --> E["API Gateway"] C --> F["API Gateway"] G["Clients/Partners"] <--> D <--> E <--> F D --> H["Applications\n(Active)"] E --> I["Applications\n(Active)"] F --> J["Applications\n(Standby)"] H <--> I <--> J H --> K["Données\n(Sync)"] I --> L["Données\n(Sync)"] J --> M["Données\n(Async)"] K <--> L <--> M

- Architecture multi-cloud : Répartition entre Azure (70%), OVHcloud (20%) et AWS (10%)
- Configuration active-active : Services critiques répartis entre plusieurs fournisseurs
- Réplication synchrone : Entre les sites principaux pour données critiques (RPO < 15 min)
- Réplication asynchrone : Vers les sites de secours pour les autres données
- Load balancing global : Répartition du trafic avec capacité de basculement
- Segmentation des services : Isolation des composants pour limiter la propagation des incidents
- Design for failure : Applications conçues pour résister aux défaillances d'infrastructure

Plans de continuité et de reprise

Structure des plans

Néo Financia a élaboré un ensemble de plans documentés et structurés.

- Plan de Continuité d'Activité (PCA) global : Document cadre définissant la stratégie et l'organisation
- Plans de Continuité Métier (PCM) : Procédures spécifiques à chaque direction
- Plans de Secours Informatique (PSI) : Procédures techniques de reprise des systèmes
- Plan de Gestion de Crise (PGC) : Modalités d'organisation et de communication en situation de crise
- Procédures opérationnelles : Instructions détaillées par système ou composant

Contenu des plans

Chaque plan comprend les éléments suivants :

- Objectifs et périmètre : Finalité et couverture du plan
- Scénarios couverts : Situations de crise anticipées
- Organisation et responsabilités : Rôles et intervenants
- Procédures d'activation : Critères et processus de déclenchement
- Procédures de basculement : Instructions techniques détaillées

- Procédures de retour à la normale : Modalités de reprise des activités standard
- Annuaire de crise : Contacts clés internes et externes
- Ressources nécessaires : Moyens humains, techniques et logistiques
- Communication : Modèles et canaux de communication

Scénarios de crise couverts

Les plans sont conçus pour répondre à différents scénarios de crise

Type de scénario	Description	Exemple d'impact	Stratégie principale
Incident technique majeur	Panne ou défaillance d'un système critique	Indisponibilité du core banking system	Basculement sur infrastructure redondante
Incident de sécurité	Compromission ou cyberattaque	Ransomware ou intrusion	Isolation, reconstruction des systèmes
Défaillance d'un fournisseur	Indisponibilité d'un prestataire critique	Panne Azure, indisponibilité Mangopay	Basculement vers fournisseur alternatif
Incident sur site	Sinistre affectant les locaux	Incendie, inondation, perte d'accès	Télétravail, site alternatif
Crise sanitaire	Pandémie ou problème de santé publique	Indisponibilité massive du personnel	Travail à distance, équipes réduites
Défaillance infrastructure	Coupure d'énergie, réseau, etc.	Perte des communications	Systèmes autonomes, redondance

Procédures de basculement

Neo Financia a élaboré des procédures de basculement détaillées

- Basculement automatique : Pour les systèmes en haute disponibilité
- Détection automatique des défaillances
- Basculement sans intervention humaine
- Vérification post-basculement
- Basculement semi-automatique : Pour les systèmes intermédiaires
- Détection automatique avec validation humaine
- Procédures d'activation simplifiées
- Scripts pré-approuvés
- Basculement manuel : Pour les systèmes complexes ou à risque
- Procédures étape par étape
- Points de contrôle et validation
- Tests préalables

Chaque procédure est documentée, testée et maintenue à jour. Les RTO/RPO (15 minutes pour les systèmes critiques) sont vérifiés lors des tests.

Tests et exercices

Programme de tests

Neo Financia maintient un programme complet de tests pour valider l'efficacité de ses plans.

Type de test	Description	Fréquence	Périmètre
Test unitaire	Vérification d'un composant spécifique	Mensuel	Composants techniques individuels
Test de basculement	Changement d'environnement technique	Trimestriel	Systèmes critiques par rotation
Test fonctionnel	Validation des processus métier	Semestriel	Processus critiques C1-C2
Exercice global	Simulation complète d'un scénario	Annuel	Organisation complète
Test de charge	Vérification des capacités	Semestriel	Infrastructure de secours
Test surprise	Exercice sans préavis	Annuel	Périmètre limité et maîtrisé

Les tests couvrent tous les scénarios de crise identifiés et sont planifiés pour minimiser l'impact sur les activités courantes.

Méthodologie des tests

Neo Financia suit une approche structurée pour la conduite des tests

1. Planification

- Définition des objectifs et critères de succès
- Élaboration du scénario et des injects
- Identification des participants et observateurs
- Évaluation des risques du test

2. Préparation

- Communication préalable (selon le type de test'
- Formation des participants si nécessaire
- Préparation des environnements techniques
- Mise en place des mécanismes d'observation

3. Exécution

- Déclenchement du test selon le scénario
- Déroulement des procédures prévues
- Collecte des observations et mesures
- Gestion des imprévus

4. Évaluation

- Mesure des temps de reprise effectifs
- Vérification des fonctionnalités
- Analyse des écarts par rapport aux attentes
- Identification des points forts et axes d'amélioration

5. Retour d'expérience

- Debriefing avec les participants
- Documentation des résultats
- Élaboration d'un plan d'action
- Mise à jour des procédures si nécessaire

Résultats et suivi

Les résultats des tests font l'objet d'un suivi rigoureux.

- Rapport de test : Documentation formelle des résultats et observations
- Plan d'action : Mesures correctives pour les anomalies identifiées
- Tableau de bord : Suivi des indicateurs de performance (RTO/RPO réels)
- Reporting : Communication aux instances de gouvernance
- Amélioration continue : Intégration des enseignements dans les plans

Les performances mesurées lors des tests permettent de valider le respect des objectifs de continuité (RTO/RPO < 15 minutes pour les systèmes critiques).

Évaluation et amélioration continue

Indicateurs de performance

Neo Financia a défini des indicateurs clés pour mesurer l'efficacité de son dispositif de continuité

Catégorie

Indicateur

Objectif

Fréquence de

		mesure	

Performance technique	Temps de reprise réel (RTO)	≤ 15 min pour systèmes C1	À chaque test
Performance technique	Perte de données maximale (RPO)	≤ 15 min pour données C1	À chaque test
Couverture	Taux de couverture des plans	100% des processus critiques	Trimestrielle
Maturité	Niveau de maturité PCA	Niveau 4/5	Annuelle
Préparation	Taux de réalisation du programme de tests	≥ 95%	Trimestrielle
Efficacité	Taux de succès des tests	≥ 90%	À chaque test
Actualisation	Âge moyen des procédures	< 12 mois	Trimestrielle
Formation	Taux de personnel formé	≥ 95% des rôles critiques	Semestrielle

Revue et audit

Le dispositif de continuité fait l'objet de revues périodiques.

- Revue interne : Évaluation complète annuelle par le RPCA
- Audit interne : Examen par l'Audit Interne tous les 2 ans
- Audit externe : Vérification par un prestataire spécialisé tous les 3 ans
- Revue réglementaire : Évaluation par les autorités de contrôle (ACPR, FCA)
- Certification : Validation selon la norme ISO 22301 (en cours)

Les résultats de ces évaluations sont présentés au Comité des Risques et au Conseil d'Administration

Amélioration continue

Neo Financia a mis en place un processus d'amélioration continue de son dispositif de continuité

1. Collecte des enseignements

- Résultats des tests et exercices
- Retours d'expérience post-incidents
- Audits et évaluations
- Veille sur les bonnes pratiques

2. Analyse des écarts

- Identification des points faibles
- Analyse des causes racines
- Benchmark avec les standards

- Évaluation des risques résiduels

3. Priorisation des actions

- Classification par niveau de risque
- Évaluation coût/bénéfice
- Alignement avec les objectifs stratégiques
- Faisabilité et ressources requises

4. Mise en œuvre

- Plan d'action formalisé
- Attribution des responsabilités
- Allocation des ressources
- Suivi de l'avancement

5. Validation

- Vérification de l'efficacité des actions
- Tests de validation
- Mise à jour des indicateurs
- Communication des résultats

Conformité réglementaire

Exigences applicables

Neo Financia assure la conformité de son dispositif de continuité avec les exigences réglementaires :

Référentiel	Exigences principales	Application
DORA (Digital Operational Resilience Act)	- Tests de résilience numérique	
- Gestion des risques liés aux tiers		
- Notification des incidents majeurs		
- Stratégie de résilience documentée		
Exigences intégrées dans le dispositif global		
ACPR (France)	- Analyse d'impact sur les activités	
- Stratégie de continuité formalisée		
- Tests réguliers documentés		

- Reporting des incidents		
Conformité totale vérifiée annuellement		
FCA (Royaume-Uni)	- Operational resilience framework	
- Impact tolerance for important business services		
- Testing and mapping		
- Self-assessment		
Dispositif spécifique pour l'entité UK		

|EBA Guidelines|-
ICT and security risk management

- Outsourcing arrangements
- Management of operational and security risks

Intégré dans les politiques de sécurité		
ISO 22301	- Système de management de la continuité d'activité	

- Analyse d'impact et évaluation des risques
- Stratégies de continuité
- Procédures et tests |Certification en cours (prévue Q3 2025)|

Reporting réglementaire

Neo Financia assure un reporting régulier aux autorités de contrôle :

- ACPR/BCE : Reporting annuel sur le dispositif de continuité
- FCA : Self-assessment document annuel
- Notification des incidents : Procédure de déclaration dans les 24h des incidents majeurs
- Rapport d'exercice : Communication des résultats des tests majeurs
- Cartographie des risques : Mise à jour annuelle partagée avec les régulateurs

Documentation et formation

Gestion documentaire

Neo Financia maintient une documentation complète et structurée de son dispositif de continuité.

- Politique de continuité d'activité : Document cadre validé par le CA
- Stratégie de continuité : Orientations globales et principes directeurs
- Plans de continuité et de reprise : Documentation opérationnelle
- Procédures techniques : Instructions détaillées par système
- Résultats des tests : Rapports et plans d'action
- Matrice des responsabilités : Rôles et contacts

Cette documentation est

- Stockée dans un référentiel sécurisé avec contrôle d'accès
- Disponible en version électronique et papier (pour les documents critiques)
- Accessible hors ligne en cas de crise majeure
- Révisée au minimum annuellement ou après chaque changement significatif
- Soumise à un contrôle de version rigoureux

Programme de formation

Neo Financia a établi un programme de formation adapté aux différents profils :

Public	Contenu	Fréquence	Format
Tous collaborateurs	- Principes de base de la continuité		
- Consignes générales en cas de crise			
- Rôles et responsabilités			
À l'embauche + annuelle	E-learning, communications		
Acteurs PCA identifiés	- Procédures spécifiques à leur rôle		
- Utilisation des outils de crise			
- Communication en situation de crise			

Semestrielle	Ateliers pratiques, exercices		
Équipes techniques	- Procédures de reprise détaillées		
- Opérations en mode dégradé			
- Séquence de restauration			
Trimestrielle	Formation technique, hands-on		
Cellule de crise	- Gestion de crise avancée		
- Prise de décision sous pression			
- Communication de crise			
Semestrielle	Simulations, exercices de crise		
Management	- Enjeux stratégiques		
- Gouvernance de la continuité			
- Responsabilités légales			
Annuelle	Présentations, table-top exercises		

L'efficacité des formations est évaluée lors des exercices et tests, avec un objectif de 95% des acteurs capables d'exécuter leurs missions en situation de crise.

Conformité

Principes fondamentaux

La conformité constitue un élément fondamental de la politique de sécurité des systèmes d'information de Neo Financia. En tant que néobanque opérant dans plusieurs juridictions (France, UE, Royaume-Uni), Neo Financia doit se conformer à un ensemble complexe d'exigences légales, réglementaires et contractuelles relatives à la sécurité de l'information.

Objectifs de la politique de conformité :

- Identifier et respecter l'ensemble des exigences légales et réglementaires applicables
- Mettre en œuvre les contrôles nécessaires pour assurer la conformité
- Prévenir les violations de conformité et leurs conséquences (sanctions, atteinte à la réputation)
- Démontrer la diligence et l'engagement de Neo Financia envers ses obligations
- Adapter le dispositif de conformité aux évolutions réglementaires
- Intégrer les exigences de conformité dans les processus métier et techniques
- Assurer une traçabilité complète des actions de mise en conformité

Cette politique s'applique à l'ensemble des activités, systèmes et processus de Neo Financia, ainsi qu'à tous les collaborateurs, prestataires et partenaires ayant accès à ses systèmes d'information.

Cadre réglementaire

Cartographie des principales réglementations

Neo Financia est soumise à un ensemble de réglementations en matière de sécurité de l'information, dont les principales sont :

Domaine	Réglementations	Principales exigences	Périmètre d'application
Résilience numérique	- DORA (Digital Operational Resilience Act)		
- NIS2 (Network and Information Security Directive)			
- Gestion des risques informatiques			
- Tests de résilience opérationnelle			
- Gestion des incidents			
- Contrôle des prestataires de services			
Activités dans l'UE			
Protection des données	- RGPD (Règlement Général		

	sur la Protection des Données)		
- UK GDPR et Data Protection Act 2018			
- Protection des données personnelles			
- Droits des personnes concernées			
- Notification des violations de données			
UE et Royaume-Uni			

	• **Analyse d'impact relative à la protection des données**
Services de paiement	• DSP2 (Directive sur les Services de Paiement 2)
• PSD2 (Payment Services Directive 2) au Royaume-Uni	
• RTS (Regulatory Technical Standards) de l'ABE	• Authentification forte du client (SCA)
• Sécurité des canaux de communication	
• Gestion des incidents de sécurité majeurs	
• Open Banking sécurisé	UE et Royaume-Uni
Réglementation bancaire	• Exigences de l'ACPR (France)
• Guidelines EBA sur la gouvernance interne	
• FCA Handbook (Royaume-Uni)	• Gouvernance des risques opérationnels
• Contrôle interne	

• Continuité d'activité	
• Protection des fonds des clients	France et Royaume-Uni
Lutte contre la fraude	• LCB-FT (Lutte Contre le Blanchiment et le Financement du Terrorisme)
• UK AML Regulations	
• Directive (UE) 2018/843 (5ème directive anti-blanchiment)	• KYC (Know Your Customer)
• Surveillance des transactions	
• Déclarations de soupçon	
• Conservation des données	UE et Royaume-Uni
Normes sectorielles	• PCI-DSS (Payment Card Industry Data Security Standard)
• ISO/IEC 27001	
• SWIFT Customer Security Programme (CSP)	• Protection des données de cartes de paiement
• Système de management de la sécurité de l'information	
• Sécurité des infrastructures de messagerie financière	Mondial

Veille réglementaire

Neo Financia a mis en place un dispositif de veille réglementaire pour anticiper et s'adapter aux évolutions du cadre normatif :

- Sources surveillées

- Publications officielles (JOUE, JORF, législation UK)
- Communications des autorités de contrôle (CNIL, ANSSI, ACPR, FCA, ICO, etc.)
- Associations professionnelles (FBF, UK Finance, etc.)
- Cabinets d'avocats spécialisés
- Services de veille spécialisés

Processus de veille

- Identification des textes pertinents
- Analyse d'impact sur les activités de Neo Financia
- Diffusion ciblée aux parties prenantes concernées
- Planification des actions de mise en conformité
- Suivi des échéances réglementaires

Comitologie

- Revue mensuelle des évolutions réglementaires en Comité Conformité
- Point trimestriel au COSEC sur les impacts sécurité
- Reporting semestriel au Comité des Risques

Organisation de la conformité

Structure et responsabilités

Neo Financia a établi une organisation claire pour assurer la gestion de la conformité en matière de sécurité de l'information:

Fonction	Responsabilités
Directeur de la Conformité	- Supervision globale du dispositif de conformité
- Reporting aux instances de gouvernance	
- Interface avec les régulateurs	
- Validation des politiques de conformité	
Responsable Conformité Sécurité	- Coordination des actions de mise en conformité sécurité
- Analyse des exigences réglementaires liées à la sécurité	
- Suivi des plans de remédiation	
- Préparation des reportings réglementaires	
RSSI	- Mise en œuvre des exigences de sécurité réglementaires

- Définition des contrôles techniques	
- Évaluation de la conformité des solutions techniques	
- Coordination des audits de sécurité réglementaires	
Délégué à la Protection des Données (DPO)	- Conseil sur la conformité au RGPD/UK GDPR

	- Tenue du registre des traitements
- Pilotage des analyses d'impact (AIPD)	
- Gestion des relations avec les autorités de protection	
---	---
Compliance Officers (par entité)	- Application des exigences locales (France, UK)
- Adaptation des politiques aux spécificités régionales	
- Suivi des contrôles de conformité locaux	
- Reporting local	
Correspondants Conformité (par direction)	- Relais des exigences de conformité
- Identification des besoins spécifiques	
- Suivi des actions de mise en conformité	
- Remontée des alertes	

- Pilotage des analyses d'impact (AIPD)
- Application des exigences locales (France, UK)
- Reporting local

Comitologie

La gouvernance de la conformité s'appuie sur plusieurs comités :

Comité de Conformité

- Fréquence
- Participants

Mensuelle

- Participants : Directeur Conformité, RSSI, DPO, Compliance Officers, Risques
- Missions : Suivi des projets de conformité, validation des positions, arbitrages
- Missions

Comité RGPD

- Fréquence

Rimestrielle

- Participants
- Participants : DPO, RSSI, Juridique, représentants métiers
- Missions : Suivi des actions RGPD, validation des AIPD, gestion des incidents
- Missions

Comité de Sécurité (COSEC)

- Fréquence

Mensuelle

- Participants

RSSI, DSI, Conformité, métiers

- Missions : Volet sécurité de la conformité, suivi des contrôles techniques
- Missions

Comité des Risques

- Fréquence

Trimesterielle

- Participants : Conseil d'administration, COMEX, fonctions de contrôle
- Participants
- Missions : Supervision des risques de non-conformité, validation des approches
- Missions

Gestion des exigences de conformité

Processus d'identification et de suivi

Neo Financia a mis en place un processus structuré pour gérer les exigences de conformité.

Identification des exigences

- Analyse des textes réglementaires applicables

- Extraction des obligations spécifiques
- Classification par domaine et niveau de criticité
- Mise à jour du référentiel d'exigences

2. Évaluation des impacts

- Analyse de l'impact sur les systèmes et processus existants
- Identification des écarts (gap analysis)
- Évaluation des ressources nécessaires
- Définition des priorités

3. Planification

- Élaboration des plans d'action
- Attribution des responsabilités
- Définition des jalons et échéances
- Allocation des ressources

4. Mise en œuvre

- Adaptation des politiques et procédures
- Implémentation des contrôles techniques
- Formation des équipes
- Documentation des actions réalisées

5. Vérification

- Contrôles de conformité
- Tests d'efficacité
- Audits internes et externes
- Revue de la documentation

6. Reporting

- Suivi de l'avancement des plans d'action
- Reporting aux instances de gouvernance
- Communication aux autorités de contrôle
- Mise à jour du statut de conformité

Référentiel des exigences de conformité

Neo Financia maintient un référentiel centralisé des exigences de conformité

Structure du référentiel

- Classification par source réglementaire
- Identification unique de chaque exigence
- Description détaillée de l'obligation
- Lien vers les textes de référence
- Criticité et échéance applicable
- Contrôles associés
- État de conformité actuel
- Actions en cours
- Responsables désignés

Mise à jour du référentiel

- Intégration des nouvelles exigences sous 30 jours
- Révision complète semestrielle

- Processus de validation des modifications
- Historisation des changements
- Accessibilité et diffusion
- Plateforme GRC centralisée
- Accès sécurisé selon les responsabilités
- Extraction de rapports personnalisés
- Alertes automatiques sur les échéances

Contrôles de conformité

Cadre de contrôle

Neo Financia a défini un cadre de contrôle complet pour vérifier sa conformité aux exigences de sécurité.

Niveau de contrôle	Description	Responsables	Fréquence
Contrôles de 1er niveau	- Autocontrôles par les équipes opérationnelles		
- Vérifications intégrées aux processus			
- Points de contrôle dans les chaînes d'opérations			
Équipes opérationnelles, managers	Quotidienne à mensuelle		

Contrôles de 2ème niveau	- Contrôles indépendants par les fonctions de contrôle		
- Vérifications ciblées sur les risques majeurs			
- Tests de conformité approfondis			
Conformité, RSSI, Risques	Mensuelle à trimestrielle		
Contrôles de 3ème niveau	- Audits internes		
- Évaluations globales			
- Vérifications de l'efficacité du dispositif			
Audit interne	Annuelle ou sur demande		
Contrôles externes	- Audits externes indépendants		
- Certification par tiers			
- Inspections réglementaires			
Auditeurs externes, régulateurs	Annuelle ou pluriannuelle		

Plans de contrôle spécifiques

Des plans de contrôle spécifiques sont établis pour les principales réglementations.

Plan de contrôle RGPD/UK GDPR

- Vérification de la conformité des traitements
- Contrôle des mesures de sécurité des données personnelles
- Validation des processus d'exercice des droits
- Revue des transferts internationaux
- Audit des procédures de violation de données

Plan de contrôle DSP2/PSD2

- Test de l'authentification forte client (SCA)
- Vérification des mécanismes de sécurité des API
- Contrôle des procédures de gestion des fraudes
- Audit des processus de notification d'incidents

Plan de contrôle PCI-DSS

- Scans de vulnérabilité trimestriels
- Tests de pénétration annuels
- Revue des contrôles de sécurité des données cartes
- Vérification de la segmentation réseau
- Audit complet pré-certification

Plan de contrôle DORA/NIS2

- Test de résilience des systèmes critiques
- Vérification des mesures de gestion des risques
- Contrôle des dispositifs de surveillance
- Audit de la gestion des fournisseurs

Gestion des non-conformités

Neo Financia a mis en place un processus formel pour traiter les non-conformités identifiées.

1. Identification et documentation

- Enregistrement détaillé de la non-conformité
- Classification par niveau de gravité
- Analyse des causes racines
- Évaluation des impacts potentiels

2. Plan de remédiation

- Définition des actions correctives
- Attribution des responsabilités
- Établissement d'un calendrier
- Allocation des ressources nécessaires

3. Mesures d'atténuation

- Mise en place de contrôles compensatoires
- Actions immédiates pour limiter les risques
- Communication aux parties prenantes

4. Suivi et reporting

- Suivi régulier de l'avancement
- Validation de l'efficacité des actions

- Reporting aux instances de gouvernance
- Notification aux autorités si nécessaire

5. Clôture et retour d'expérience

- Vérification finale de la remédiation
- Documentation des enseignements
- Mise à jour des contrôles préventifs
- Partage des bonnes pratiques

Niveaux de gravité des non-conformités :

- Critique : Non-conformité majeure exposant à des sanctions importantes ou à des risques significatifs
- Élevée : Non-conformité importante nécessitant une action corrective rapide
- Moyenne : Non-conformité à traiter dans un délai raisonnable
- Basse : Non-conformité mineure ou technique avec impact limité

Protection des données personnelles

Gouvernance des données personnelles

Neo Financia a mis en place une gouvernance spécifique pour la protection des données personnelles

Organisation

- Délégué à la Protection des Données (DPO) enregistré auprès de la CNIL et de l'ICC
- Équipe Protection des Données dédiée
- Réseau de correspondants dans chaque direction
- Comité RGPD bimestrie

Documentation

- Politique de protection des données personnelles
- Registre des traitements
- Cartographie des flux de données
- Procédures d'exercice des droits
- Mentions d'information et modèles de consentement
- Processus clés
- Privacy by Design & by Default dans tous les projets
- Analyse d'impact relative à la protection des données (AIPD)
- Gestion des demandes d'exercice de droits
- Notification des violations de données
- Encadrement des transferts hors UE/UK

Mesures de protection des données

Neo Financia a déployé des mesures techniques et organisationnelles pour protéger les données personnelles.

Mesures mises en œuvre

|Minimisation des données|-
Collecte limitée aux données strictement nécessaires

- Durées de conservation définies et appliquées
- Processus de purge et d'archivage automatisés
- Anonymisation des données pour les analyses | |---|---| |Contrôles d'accès|-
  Accès aux données personnelles sur principe du besoin d'en connaître
- Authentification forte pour les accès aux données sensibles
- Journalisation des accès aux données personnelles
- Revue régulière des droits d'accès | |Sécurité des données|-
  Chiffrement des données sensibles au repos et en transit
- Cloisonnement des environnements
- Protection renforcée des bases de données clients
- Masquage des données en environnements non-productifs | |Gestion des incidents|-
  Procédure de gestion des violations de données
- Outils de détection des fuites de données
- Processus de notification CNIL/ICO (72h)
- Communication aux personnes concernées si nécessaire | |Gestion des tiers|-
  Due diligence des sous-traitants
- Clauses contractuelles de protection des données
- Audit des sous-traitants critiques
- Encadrement des transferts internationaux |

Analyse d'impact relative à la protection des données (AIPD)

Neo Financia conduit systématiquement des AIPD pour les traitements à risque élevé.

Critères de déclenchement

- Traitement de données sensibles à grande échelle
- Profilage avec effet juridique ou impact significatif
- Surveillance systématique à grande échelle
- Innovations technologiques présentant des risques
- Croisement de données de sources multiples

Méthodologie

- Description systématique du traitement
- Évaluation de la nécessité et de la proportionnalité
- Identification et analyse des risques

- Définition des mesures pour atténuer les risques
- Documentation complète de l'analyse

Validation et suivi

- Revue par le DPC
- Validation par le Comité RGPD
- Mise à jour annuelle ou en cas de changement significatil
- Consultation préalable de la CNIL/ICO si risque résiduel élevé

Sécurité dans les obligations contractuelles

Exigences pour les tiers

Néo Financia intègre des exigences de sécurité et de conformité dans ses relations contractuelles

Clauses types de sécurité

- Engagement de conformité aux réglementations applicables
- Mesures de sécurité minimales requises
- Gestion et notification des incidents
- Droits d'audit et de contrôle
- Confidentialité et protection des données
- Conditions de réversibilité et de fin de contrat

Annexes de sécurité spécifiques

- Exigences détaillées adaptées à la nature du service
- Niveaux de service (SLA) pour la sécurité
- Processus de gestion des vulnérabilités
- Modalités d'intervention en cas d'incident
- Plan de contrôles périodiques

Contrats avec les partenaires fintech

- Exigences renforcées pour Mangopay et Lemonway
- Sécurisation des API et des flux de données
- Procédures conjointes de gestion d'incident
- Tests de sécurité réguliers
- Partage d'informations sur les menaces

Gestion des fournisseurs de cloud

Des dispositions spécifiques encadrent les relations avec les fournisseurs cloud (Azure, OVHcloud, AWS)

Due diligence pré-contractuelle

- Évaluation de la conformité réglementaire
- Vérification des certifications (ISO 27001, SOC 2, etc.)
- Analyse des conditions de service et SLA

- Revue des modalités de fin de service et de portabilité

Contrôles contractuels

- Clauses RGPD complètes (conformes aux exigences EDPB)
- Engagement de localisation des données
- Niveaux de service pour la sécurité et la disponibilité

- Procédures d'escalade et de gestion de crise
- Conditions de sous-traitance et chaîne de responsabilité

Surveillance continue

- Revue trimestrielle des performances sécurité
- Monitoring des incidents de sécurité
- Évaluation périodique des mesures de sécurité
- Audit annuel de conformité

Audit et évaluation de la conformité

Programme d'audit

Neo Financia maintient un programme d'audit complet pour évaluer sa conformité en matière de sécurité.

Type d'audit	Périmètre	Fréquence	Réalisé par
Audit interne de conformité	Évaluation globale de la conformité sécurité	Annuelle	Équipe d'Audit Interne
Audit RGPD	Conformité aux exigences de protection des données	Annuelle	Équipe DPO + Audit Interne
Audit PCI-DSS	Conformité au standard PCI-DSS	Annuelle	QSA (Qualified Security Assessor) externe
Audit ISO 27001	Conformité au système de management de la sécurité	Semestrielle (interne), Annuelle (certification)	Auditeurs internes, Organisme certificateur
Audit DSP2/PSD2	Exigences de sécurité des services de paiement	Annuelle	Équipe Conformité + experts externes
Audit réglementaire	Inspection des autorités de contrôle	Périodique (selon les autorités)	ACPR, FCA, CNIL, ICO, etc.

Méthodologie d'audit

Néo Financia suit une approche structurée pour la conduite des audits de conformité

1 Planification

- Définition du périmètre et des objectifs
- Identification des référentiels applicables
- Élaboration du plan d'audit détaillé
- Sélection des auditeurs compétents

2. Préparation

- Collecte de la documentation
- Élaboration des questionnaires et points de contrôle

- Organisation des entretiens
- Communication aux parties prenantes

3. Exécution

- Revue documentaire approfondie
- Entretiens avec les responsables
- Tests de conformité
- Observations et collecte de preuves

4. Analyse et reporting

- Évaluation des constats
- Identification des non-conformités
- Élaboration du rapport d'audit
- Présentation des résultats

5. Suivi

- Élaboration du plan d'action
- Suivi de la mise en œuvre
- Vérification de l'efficacité des actions
- Clôture des recommandations

Certifications

Neo Financia maintient plusieurs certifications pour démontrer sa conformité

ISO/IEC 27001:2022

- Périmètre : Système global de management de la sécurité de l'information
- Statut : Certification obtenue, maintenue depuis 2023
- Audit de surveillance annuel, recertification tous les 3 ans
- PCI-DSS v4.0
- Périmètre : Infrastructure de traitement des données de cartes
- Statut : Conformité attestée, renouvelée annuellement
- Audits trimestriels de vulnérabilité, audit annuel complet
- SOC 2 Type II
- Périmètre : Contrôles relatifs à la sécurité, disponibilité et confidentialité

- Statut : Rapport obtenu, renouvelé annuellement
- Évaluation continue sur une période de 12 mois
- Certification GDPR (CNIL)
- Périmètre : Gouvernance des données personnelles
- Statut : En cours de préparation, obtention prévue Q2 2026

Reporting et communication

Reporting interne

Neo Financia a mis en place un dispositif de reporting interne sur la conformité

Destinataire

Contentu

Fréquence

Format

|Conseil d'Administration|-
Situation globale de conformité

- Risques majeurs de non-conformité
- Résultats des audits significatifs
- Évolutions réglementaires majeures

Semestrielle	**Rapport de synthèse stratégique**		
Comité des Risques	- Tableau de bord de conformité		

- Suivi des plans d'action majeurs
- Incidents de conformité significatifs
- Résultats des contrôles et audits |Trimestrielle|Rapport détaillé avec métriques| |COMEX|-
  Points d'attention opérationnels
- Projets de conformité en cours
- Impacts business des évolutions réglementaires
- Ressources et priorités |Trimestrielle|Présentation exécutive| |Directions métiers|-
  Conformité spécifique à leur périmètre
- Actions à mettre en œuvre
- Résultats des contrôles de leur domaine

- Évolutions réglementaires impactantes |Mensuelle|Tableau de bord opérationnel|

Reporting réglementaire

Neo Financia assure un reporting régulier aux autorités de contrôle

- Rapports réglementaires périodiques
- Rapport annuel sur le contrôle interne (ACPR)
- Questionnaire sur la sécurité des systèmes d'information (ACPR)
- Reporting annuel de sécurité (FCA)
- Rapport annuel du DPO (CNIL)
- Notifications d'incidents
- Notification des incidents de paiement majeurs (ACPR/BCE)
- Notification des violations de données (CNIL/ICO)
- Notification des incidents de sécurité significatifs (ANSSI/NCSC)
- Communications spécifiques
- Réponses aux demandes d'information des régulateurs
- Déclaration des nouveaux traitements à risque
- Demandes d'avis ou d'autorisation préalables

Gestion des relations avec les régulateurs

Neo Financia maintient un dialogue constructif avec les autorités de contrôle

Principes d'interaction

- Transparence et coopération
- Réactivité aux demandes
- Communication proactive
- Documentation complète et précise

Processus d'interaction

- Points de contact désignés par autorité
- Procédure de validation des communications officielles
- Préparation et accompagnement des inspections
- Suivi des engagements pris

Participation active

- Groupes de travail sectoriels
- Consultations publiques

- Forums professionnels
- Initiatives de partage d'information

Formation et sensibilisation à la conformité

Programme de formation

Neo Financia a déployé un programme complet de formation à la conformité

Public	Contenu	Format	Fréquence
Tous collaborateurs	- Sensibilisation générale à la conformité		
- Protection des données personnelles			
- Sécurité de l'information			
- Signalement des incidents			
E-learning, vidéos, communications	À l'embauche + Annuelle		
Management	- Responsabilités en matière de conformité		
- Pilotage des contrôles			
- Gestion des risques de non-conformité			
- Promotion de la culture conformité			
Sessions présentielles, workshops	Semestrielle		

|Équipes IT et développement|-
Security & Privacy by Design

- Exigences réglementaires techniques
- Tests de conformité

- Standards de développement sécurisé

Formation technique, ateliers pratiques	**Semestrielle**		
Équipes produit et marketing	- Conformité des produits et services		

- Protection des données dans le marketing
- Règles de communication financière
- Traitement loyal des clients |Sessions spécifiques, cas pratiques|Semestrielle| |Correspondants conformité|-
Formation approfondie sur les réglementations
- Techniques d'évaluation et de contrôle
- Remontée et traitement des alertes
- Documentation et suivi |Formation spécialisée, certification|Initiale + Trimestrielle|

Sensibilisation continue

Neo Financia maintient un programme de sensibilisation continue à la conformité

Communications régulières

- Newsletter mensuelle sur la conformité
- Articles sur l'intranet
- Alertes sur les évolutions réglementaires
- Campagnes thématiques (RGPD, sécurité, etc.)

Événements

- Semaine de la conformité annuelle
- Webinaires trimestriels
- Sessions de questions-réponses
- Interventions d'experts externes

Outils pédagogiques

- Guides pratiques par thématique
- FAQ et base de connaissances
- Cas concrets et retours d'expérience

- Modules d'auto-évaluation

Mesure de l'efficacité

L'efficacité des actions de formation et de sensibilisation est régulièrement évaluée.

- Indicateurs quantitatifs
- Taux de participation aux formations (objectif : ≥95%)
- Scores aux évaluations (objectif : ≥80%)
- Nombre d'incidents liés à la méconnaissance des règles
- Taux de conformité lors des contrôles
- Évaluations qualitatives
- Enquêtes de perception
- Tests pratiques (simulations)
- Entretiens avec les correspondants
- Retours des audits
- Amélioration continue
- Analyse des résultats
- Identification des lacunes
- Adaptation du programme
- Renforcement ciblé si nécessaire

Sécurité des services bancaires digitaux

Principes fondamentaux

La sécurité des services bancaires digitaux constitue un enjeu critique pour Neo Financia, dont le modèle d'affaires repose entièrement sur les canaux numériques. Cette politique vise à garantir le plus haut niveau de protection des services proposés aux 2 millions de clients de la néobanque, tout en préservant une expérience utilisateur fluide et intuitive.

Objectifs de la sécurité des services bancaires digitaux :

- Protéger les données financières et personnelles des clients
- Garantir l'intégrité et la confidentialité des transactions
- Assurer une disponibilité maximale des services digitaux
- Prévenir les fraudes et les utilisations non autorisées
- Respecter les exigences réglementaires spécifiques aux services financiers
- Maintenir la confiance des clients dans les services digitaux
- Assurer l'évolutivité sécurisée des services face aux innovations

Cette politique s'applique à l'ensemble des services bancaires digitaux proposés par Neo Financia, incluant l'application mobile, les interfaces web, les APIs, les services de paiement, ainsi que tous les processus de support associés.

Authentification et gestion des identités clients

Politique d'authentification

Neo Financia applique une approche d'authentification forte, multifactorielle et adaptative pour ses services bancaires digitaux:

|Niveau de sensibilité|Type d'opération|Méthode d'authentification|Exemples| | |---|---|---|---| |Niveau 1 (Standard)|Consultation d'informations générales|Authentification simple + session sécurisée|-
Consultation du solde

- Historique des transactions
- Informations sur les produits | |Niveau 2 (Sensible)|Opérations à impact modéré|Authentification forte (2 facteurs)|-
Virements vers bénéficiaires enregistrés
- Modification des paramètres non critiques
- Souscription à des services complémentaires | |Niveau 3 (Critique)|Opérations à haut risque|Authentification forte renforcée (2+ facteurs) + analyse de risque|-
Ajout d'un nouveau bénéficiaire
- Virements de montants élevés
- Modification des données personnelles sensibles
- Modification des paramètres de sécurité | |Niveau 4 (Très critique)|Opérations exceptionnelles|Authentification multi-niveaux + validation hors bande + contrôle manuel|-
Virements internationaux de montants importants
- Demandes de crédit
- Changement d'appareil principal
- Réinitialisation complète des accès |

Méthodes d'authentification

Neo Financia propose plusieurs méthodes d'authentification, adaptées aux besoins et préférences des clients.

Identifiants primaires

- Identifiant unique + mot de passe respectant les meilleures pratiques
- Politique de complexité des mots de passe (12 caractères minimum, combinaison de types)
- Stockage sécurisé (hachage avec sel, algorithmes robustes)
- Renouvellement en cas de suspicion de compromission

Authentification biométrique

- Reconnaissance faciale (avec détection de vivacité)
- Empreinte digitale
- Reconnaissance vocale (pour certaines opérations téléphoniques)
- Traitement local sur l'appareil, sans stockage centralisé des données biométriques

Facteurs complémentaires

- Codes à usage unique (OTP) par SMS
- Application d'authentification (TOTP)
- Notifications push sécurisées
- Validation sur appareil secondaire
- Questions de sécurité dynamiques (pour récupération uniquement)

Authentification adaptative

Neo Financia utilise une approche d'authentification adaptative, ajustant le niveau de sécurité en fonction du contexte.

Facteurs d'analyse de risque

- Appareil utilisé (connu/inconnu, caractéristiques techniques`
- Localisation et géolocalisation
- Comportement de navigation et d'utilisation
- Historique des transactions
- Modalités de connexion
- Horodatage et fréquence des connexions

Adaptations dynamiques

- Demande de facteurs d'authentification supplémentaires
- Limitation temporaire des opérations sensibles
- Alertes en temps réel au client
- Surveillance renforcée de la session

- Vérifications supplémentaires par les équipes anti-fraude

Gestion du cycle de vie des identités clients

Neo Financia a établi un processus sécurisé pour gérer l'ensemble du cycle de vie des identités clients.

1. Enrôlement et vérification d'identité

- Processus d'identification conforme à la réglementation KYC
- Vérification des documents d'identité (contrôles automatisés et manuels)
- Vérification des données personnelles auprès de sources tierces
- Détection des tentatives d'usurpation d'identité
- Enrôlement multi-canal sécurisé (application, web, vidéo)

2. Attribution des accès

- Création d'identifiants uniques

- Distribution sécurisée des informations d'accès initiales
- Enrôlement des dispositifs d'authentification
- Définition des limites opérationnelles initiales

3. Gestion des modifications

- Processus sécurisé de mise à jour des données d'identité
- Validation renforcée des changements critiques
- Traçabilité complète des modifications
- Notification des changements au client

4. Réinitialisation et récupération

- Procédure multi-étapes de réinitialisation des credentials
- Vérification d'identité renforcée
- Délais de sécurité et alertes pour prévenir les abus
- Assistance dédiée pour les cas complexes

5. Révocation et suppression

- Désactivation immédiate sur demande du client
- Désactivation temporaire en cas de suspicion de fraude
- Archivage sécurisé des données selon les obligations légales
- Suppression définitive à l'issue des délais réglementaires

Sécurité des transactions

Protection des transactions

Neo Financia met en œuvre des mesures de sécurité spécifiques pour garantir l'intégrité, la confidentialité et la non-répudiation des transactions financières :

- Chiffrement de bout en bout
- Chiffrement TLS 1.3 obligatoire pour toutes les communications
- Chiffrement supplémentaire des données sensibles au niveau applicatif
- Rotation régulière des clés de chiffrement
- Mise en œuvre de Perfect Forward Secrecy

- Intégrité des données
- Signatures électroniques des transactions
- Contrôles de cohérence systématiques
- Comparaison des montants en lettres et en chiffres
- Vérification des totaux de contrôle
- Validation des transactions
- Authentification forte du client (SCA) conforme DSP2
- Confirmation explicite des opérations sensibles
- Délais de validation pour les opérations à risque
- Notifications en temps réel
- Traçabilité
- Journalisation immuable de toutes les transactions
- Horodatage sécurisé
- Conservation des preuves de transaction
- Piste d'audit complète et inaltérable

Limites et contrôles

Neo Financia applique un système de limites et de contrôles pour réduire les risques liés aux transactions

Type de limite	Description	Paramétrage
Limites de montant	- Plafonds par transaction	
- Plafonds journaliers		
- Plafonds hebdomadaires		
- Plafonds mensuels		
- Limites par défaut selon profil client		
- Personnalisation possible (avec validation)		
-		

Limites renforcées pour nouveaux bénéficiaires		
- Augmentation temporaire possible		
Restrictions géographiques	- Zones autorisées par défaut	
- Restrictions par pays à risque		
- Cohérence géographique des opérations		
- Blocage par défaut hors UE		
- Activation temporaire sur demande		
- Alertes sur transactions inhabituelles		
Contrôles temporels	- Délais entre opérations sensibles	
- Périodes d'activation des services		
- Temporisation des opérations à risque		
- Délai de 24h pour nouveaux bénéficiaires		
- Exécution différée des virements importants		
- Validation en deux temps des opérations critiques		
Restrictions par type d'opération	- Activation/désactivation de fonctionnalités	
- Restrictions par canal		

- Limites spécifiques par service		
- Paiements en ligne activables/désactivables		
- Virements internationaux sur opt-in		
- Retraits personnalisables		

Gestion des bénéficiaires

La gestion des bénéficiaires de virements fait l'objet de mesures de sécurité spécifiques

Processus d'ajout sécurisé

- Authentification forte systématique
- Délai de sécurité entre l'ajout et le premier virement (24h par défaut)
- Notification immédiate au client (email, push)
- Validation par un second canal pour les ajouts sensibles

Contrôles de validité

- Vérification automatique des coordonnées bancaires (IBAN)

- Contrôle de cohérence nom/IBAN (quand disponible)
- Détection des bénéficiaires suspects
- Vérification des sanctions et listes noires

Protection contre la fraude

- Détection des modifications multiples de bénéficiaires
- Alerte sur les motifs inhabituels de virement
- Analyse comportementale des patterns d'ajout
- Contrôles renforcés pour les bénéficiaires internationaux

Gestion des modifications

- Traçabilité des modifications
- Historique des bénéficiaires
- Processus sécurisé de suppression
- Protection contre la modification en masse

Sécurité des applications mobiles

Principes de sécurité

L'application mobile Neo Financia, utilisée par 80% de la clientèle active, est conçue selon les principes de sécurité suivants :

Principes fondamentaux de sécurité mobile :

- Security by design : Sécurité intégrée dès la conception de l'application
- Defense in depth : Multiples couches de contrôles sécurité complémentaires
- Zero trust : Vérification systématique de l'identité et du contexte de chaque requête
- Least privilege : Limitation des permissions au strict nécessaire
- Data minimization : Limitation des données stockées localement
- Secure by default
- Secure by default : Configuration restrictive par défaut

Sécurité du code et de l'application

Neo Financia assure la sécurité de son application mobile par une approche complète.

Développement sécurisé

- Bonnes pratiques de codage sécurisé (OWASP MASVS L2)
- Revue de code systématique et pair-programming
- Tests de sécurité automatisés dans la CI/CD
- Analyse statique et dynamique du code

Protection du code

- Obfuscation du code
- Anti-tampering (détection de modification)
- Anti-debugging et anti-reverse engineering
- Détection des environnements compromis (jailbreak/root)
- Intégrité de l'application

- Signature cryptographique des versions
- Vérification de l'intégrité au démarrage
- Détection des modifications non autorisées
- Distribution exclusive via stores officiels

Gestion des sessions

- Tokens sécurisés à durée limitée
- Renouvellement régulier des jetons d'authentification
- Déconnexion automatique après inactivité (5 minutes par défaut)
- Invalidation à distance des sessions

Sécurité des données sur l'appareil

Néo Financia protège les données stockées sur les appareils mobiles

Minimisation des données locales

- Stockage local limité au strict nécessaire

- Absence de données sensibles en clair
- Nettoyage automatique des données temporaires
- Effacement complet à la désinstallation

Chiffrement des données

- Chiffrement de toutes les données persistantes
- Utilisation des API de sécurité natives (Keystore/Keychain)
- Stockage sécurisé des clés cryptographiques
- Protection contre l'extraction des données

Protection contre les fuites de données

- Prévention des captures d'écran sur les vues sensibles
- Désactivation du copier-coller pour les données critiques
- Mode incognito pour les informations sensibles
- Effacement automatique du presse-papiers

Gestion multi-appareils

- Enrôlement sécurisé des appareils
- Limitation du nombre d'appareils actifs simultanément
- Désenregistrement à distance
- Inventaire des appareils consultable par le client

Sécurité des communications

Les communications entre l'application mobile et les serveurs de Neo Financia sont protégées par :

Chiffrement des communications

- TLS 1.3 avec suite de chiffrement forte
- Certificate pinning pour prévenir les attaques Man-in-the-Middle
- Chiffrement supplémentaire au niveau applicatif pour les données sensibles
- Vérification des certificats

Sécurité des requêtes

- Jetons d’authentification à courte durée de vie
- Signatures des requêtes sensibles

- Nonces pour prévenir les rejeux
- Validation stricte des entrées côté serveur

Protection contre les menaces réseau

- Détection des proxys et outils d'interception
- Mécanismes anti-replay
- Détection des anomalies réseau
- Vérification de l'intégrité des réponses

Sécurité des services web

Architecture sécurisée

La plateforme web Neo Financia (20% des transactions) repose sur une architecture conçue pour la sécurité.

Défense en profondeur

- Architecture multi-couches avec séparation des responsabilités
- Filtrage progressif des requêtes
- Plusieurs niveaux de validation et de contrôle
- Cloisonnement des environnements front-end et back-end

Infrastructures dédiées

- Serveurs web exposés en DMZ
- Séparation des serveurs de présentation et d'application
- Protection périmétrique renforcée (WAF, IPS)
- Flux unidirectionnels vers les systèmes internes

Haute disponibilité

- Architecture redondante active-active
- Répartition de charge avec contrôles de santé
- Isolation des défaillances
- Basculement automatique inter-sites

Sécurité de l'interface web

Neo Financia applique les meilleures pratiques de sécurité pour son interface web

Sécurité du transport

- HTTPS obligatoire (TLS 1.3)
- En-têtes de sécurité HTTP complets
- HSTS avec preloading
- OCSP Stapling pour la vérification de certificats
- Protection contre les attaques web
- Content Security Policy (CSP) stricte
- Protection CSRF robuste (tokens par session/action)
- Défenses XSS (encodage, validation, sanitization)
- Contrôles contre l'injection de code (SQL, OS, etc.)
- Protection contre le clickjacking (X-Frame-Options)

Sécurité des sessions

- Cookies sécurisés (Secure, HttpOnly, SameSite=Strict)

- Identifiants de session aléatoires et complexes
- Renouvellement de session après authentification
- Délai d'inactivité paramétrable (10 minutes par défaut)
- Invalidation des sessions parallèles suspectes

Protection du client

- JavaScript obfusqué et minifié
- Validation côté client complémentaire (non exclusive)
- Protection contre l'extraction de données sensibles
- Détection des extensions navigateur malveillantes

Optimisation pour la sécurité mobile

Le site responsive de Neo Financia intègre des mesures spécifiques pour la sécurité des accès mobiles

Responsive security design

- Adaptation des contrôles de sécurité au facteur de forme
- Simplification de l'interface pour réduire les risques
- Masquage intelligent des données sensibles
- Optimisation pour les écrans tactiles (minimisation des erreurs)

Contrôles adaptatifs

- Détection de l'environnement de navigation
- Adaptation de l'authentification selon le contexte
- Limitation intelligente des fonctionnalités à risque
- Navigation guidée pour réduire les erreurs
- Intégration web-application
- App-links sécurisés pour redirection vers l'application native
- Mécanismes de transfert sécurisé de sessior
- Cohérence des contrôles entre canaux

API et Open Banking sécurisé

Gouvernance des API

Neo Financia a mis en place une gouvernance spécifique pour ses API, essentielles à son modèle de néobanque.

- Organisation
- Équipe dédiée API Security
- Comité API mensuel impliquant sécurité, développement et métier
- Processus d'approbation des nouvelles API
- Documentation centralisée et contrôlée
- Gestion du cycle de vie
- Processus formalisé de conception sécurisée
- Revue de sécurité obligatoire avant exposition
- Versioning strictement contrôlé
- Dépréciation et fin de vie gérées
- Monitoring et reporting
- Surveillance continue des usages

- Alertes sur comportements anormaux

- Reporting mensuel d'activité et de sécurité
- Tableau de bord temps réel des API

Architecture API sécurisée

L'architecture API de Neo Financia a été conçue pour une sécurité maximale :

Architecture multi-niveaux

- Gateway API centralisée avec contrôles de sécurité uniformes
- Proxy d'API avec inspection approfondie
- API management pour la gestion des droits et quotas
- Backend API sécurisé et isolé

Classification des API

- API publiques (Open Banking, partenaires externes)
- API partenaires (Mangopay, Lemonway, intégrations spécifiques)
- API internes (applications propres de Neo Financia)
- API administratives (gestion interne)

Segmentation et isolation

- Séparation physique et logique par type d'AP
- Cloisonnement des environnements
- Flux unidirectionnels contrôlés
- Limitation de la surface d'exposition

Sécurité des API ouvertes

Neo Financia applique des mesures de sécurité spécifiques pour ses API Open Banking et partenaires

Contrôle de sécurité	Mise en œuvre
Authentification	- OAuth 2.0 avec OpenID Connect
- Certificats clients mutuels (mTLS) pour les connexions partenaires	
- API keys + secrets pour identification des applications	
- Authentification multi-niveaux (app + utilisateur final)	
Autorisation	- Scopes OAuth granulaires et spécifiques

- Consentement explicite et limité dans le temps	
- Validation côté serveur systématique	
- Séparation des rôles et permissions	
Protection des données	- TLS 1.3 obligatoire
- Chiffrement supplémentaire au niveau message (JWE)	
- Signatures des requêtes (JWS)	

	• Vérification d'intégrité des payloads
---	---
Limitation et contrôle	- Rate limiting adaptatif (par client, IP, utilisateur)
- Quotas d'utilisation par service	
- Détection des comportements anormaux	
- Mise en quarantaine automatique en cas d'abus	
Validation des entrées	- Validation stricte des schémas (OpenAPI/Swagger)
- Filtrage des entrées	
- Protection contre les injections	
- Limitation de taille des requêtes	

Gestion des partenaires API

Neo Financia a mis en place un processus rigoureux pour la gestion des partenaires utilisant ses API.

1. Onboarding sécurisé

- Vérification approfondie des partenaires (due diligence)
- Évaluation de la maturité sécurité
- Signature de contrats avec clauses de sécurité
- Attribution d'un niveau de confiance

2. Provisionnement

- Création d'identifiants spécifiques
- Limitation aux seules API nécessaires
- Configuration des quotas et limitations
- Documentation personnalisée et support d'intégration

3. Surveillance spécifique

- Monitoring dédié par partenaire
- Alertes personnalisées
- Détection des anomalies d'usage
- Rapports réguliers d'activité

4. Gestion du cycle de vie

- Revue périodique des accès
- Rotation des secrets
- Gestion des évolutions d'API
- Procédure de révocation d'urgence

Conformité DSP2/Open Banking

Neo Financia assure la conformité de ses API Open Banking aux exigences réglementaires.

- Standards implémentés

- Conformité aux RTS EBA (Regulatory Technical Standards)

- Implémentation des standards STET (France)
- Compatibilité avec Open Banking UK
- Alignement sur les standards Berlin Group NextGenPSD2

Exigences spécifiques DSP2

- Authentification forte du client (SCA)
- Gestion des exemptions à la SCA
- Interfaces dédiées pour TPP (Third Party Providers)
- Mécanisme de secours (fallback)
- Surveillance réglementaire
- Monitoring des taux de disponibilité (>99.5%)
- Reporting des performances aux régulateurs
- Documentation publique des API
- Environnement de test accessible aux TPF

Détection et prévention des fraudes

Stratégie anti-fraude

Neo Financia a développé une approche multi-niveaux pour la détection et la prévention des fraudes

Principes de la stratégie anti-fraude

- Défense multicouche : Contrôles à différents niveaux du parcours client
- Analyse en temps réel : Détection des fraudes pendant les opérations
- Analyse différée : Détection des patterns complexes sur historique
- Approche basée sur les risques : Intensité des contrôles adaptée au niveau de risque
- Intelligence collective : Partage d'information sur les menaces
- Amélioration continue : Adaptation constante aux nouvelles menaces

Dispositif de détection

Neo Financia déploie un dispositif complet de détection des fraudes :

Système de surveillance temps réel

- Analyse comportementale des transactions
- Scoring de risque dynamique
- Moteur de règles expert
- Détection d'anomalies par machine learning
- Profilage client et adaptation contextuelle

Surveillance des canaux d'accès

- Détection des appareils suspects
- Identification des tentatives d'usurpation
- Analyse des patterns de navigation
- Identification des réseaux à risque (Tor, VPN connus)
- Device fingerprinting avancé

Contrôles spécifiques par type de fraude

- Détection de SIM swapping
- Prévention de l'ingénierie sociale
- Identification des mules financières
- Détection des tentatives d'usurpation d'identité
- Protection contre les attaques par script automatisé

Analyse post-transaction

- Revue des transactions à risque
- Analyse de réseaux de transactions suspectes
- Détection des patterns émergents

- Corrélation d'événements multi-canaux

Procédures d'intervention

Neo Financia a défini des procédures d'intervention en cas de suspicion de fraude

Niveau de risque	Actions automatiques	Actions humaines
Faible	- Surveillance accrue	
- Journalisation renforcée		
- Marquage pour analyse ultérieure		
- Analyse périodique des tendances		
- Ajustement des règles si nécessaire		
Moyen	- Notification au client	
- Demande de confirmation secondaire		
- Authentification renforcée		
- Temporisation de l'opération		
- Revue par l'équipe fraude dans les 4h		
- Contact client si nécessaire		
- Ajustement du profil de risque		
Élevé	- Blocage préventif de l'opération	
- Alerte au client (SMS, push, email)		
- Limitation temporaire de certains services		

- Enregistrement d'une alerte		
- Analyse prioritaire (<30 minutes)		
- Contact proactif du client		
- Décision de déblocage ou confirmation		
- Documentation détaillée du cas		
Critique	- Blocage complet du compte	
- Déconnexion des sessions actives		
- Révocation des tokens d'accès		
- Alerte immédiate au SOC		
- Intervention immédiate de l'équipe fraude		
- Contact d'urgence client		
- Investigation approfondie		
- Signalement aux autorités si confirmé		

# Éducation et prévention		

Neo Financia développe des actions préventives et éducatives pour limiter les risques de fraude.

- Information des clients
- Guide de bonnes pratiques de sécurité
- Alertes sur les fraudes émergentes
- Communications ciblées selon les profils
- Centre de ressources sécurité dans l'application

- Outils préventifs
- Paramétrage des limites de transaction
- Gestion des alertes personnalisées
- Contrôle des canaux actifs
- Validation supplémentaire activable
- Prévention ciblée
- Accompagnement renforcé des clients vulnérables
- Alertes contextuelles dans les parcours à risque
- Campagnes de sensibilisation thématiques
- Conseils personnalisés basés sur les habitudes

Gestion des mises à jour et de l'évolution

Gestion des versions

Neo Financia applique un processus rigoureux pour la gestion des versions de ses services digitaux.

- Politique de versioning
- Versioning sémantique (Major.Minor.Patch)
- Documentation des changements (changelog)
- Rétrocompatibilité garantie pour les mises à jour mineures
- Période de transition pour les changements majeurs
- Cycles de mise à jour
- Applications mobiles : cycle de 4 semaines pour les nouvelles fonctionnalités
- Correctifs de sécurité : déploiement accéléré (< 72h pour critiques)
- Backend : déploiement continu avec tests de non-régression
- Notification proactive des mises à jour de sécurité
- Fin de support
- Politique de support clairement définie
- Support des trois dernières versions majeures minimum
- Notification aux utilisateurs des versions obsolètes
- Migration assistée vers les versions supportées

Intégration de la sécurité dans l'évolutior

Neo Financia intègre la sécurité à toutes les étapes d'évolution de ses services digitaux :

- Security by Design
- Revue de sécurité dès la conception

- Threat modeling systématique pour les nouvelles fonctionnalités
- Évaluation d'impact pour chaque évolution significative
- Validation des exigences de sécurité en phase de conception

DevSecOps

- Tests de sécurité automatisés dans la pipeline CI/CD
- Analyse statique et dynamique du code
- Scan des dépendances
- Security gates à chaque étape

Validation pré-production

- Tests de pénétration complets avant déploiement majeur
- Analyse de vulnérabilités
- Revue de code des composants critiques
- Validation par l'équipe sécurité

Déploiement sécurisé

- Déploiement progressif (canary release)
- Surveillance renforcée post-déploiement
- Capacité de rollback rapide
- Validation post-déploiement

Surveillance de l'expérience client

Neo Financia maintient un équilibre entre sécurité et expérience utilisateur.

Mesure de l'impact

- Suivi des indicateurs de friction (drop-off, temps d'exécution)
- Analyse des retours clients sur les contrôles de sécurité
- Tests d'utilisabilité des mécanismes de sécurité
- Évaluation comparative avec les standards du marché

Optimisation progressive

- Ajustement des contrôles selon le feedback
- Simplification des parcours sécurisés
- Amélioration de l'ergonomie des mécanismes d'authentification
- Personnalisation des contrôles selon les préférences utilisateur

Sécurité contextuelle

- Adaptation dynamique du niveau de sécurité selon le contexte
- Réduction des frictions pour les opérations standard

- Renforcement ciblé pour les actions sensibles
- Apprentissage des habitudes pour minimiser les contrôles redondants

Innovation et évolutions

Veille technologique et anticipation

Neo Financia maintient une veille active sur les innovations en matière de sécurité bancaire digitale.

Sources surveillées

- Évolutions réglementaires (DSP3, DORA, eIDAS 2.0)

- Standards émergents (FIDO, OAuth 2.1, etc.)
- Travaux académiques et recherche
- Innovations des acteurs du marché
- Évolutions des écosystèmes mobiles (iOS, Android)
- Processus d'évaluation
- Lab d'innovation sécurité
- POC (Proof of Concept) des technologies prometteuses
- Grille d'évaluation multicritère (sécurité, UX, coût, maturité)
- Tests utilisateurs des innovations
- Roadmap d'intégration
- Planification des évolutions technologiques
- Alignment avec la stratégie globale
- Préparation des migrations
- Maintien de la compatibilité

Technologies émergentes

Neo Financia évalue et expérimente plusieurs technologies émergentes pour renforcer la sécurité de ses services

Technologie	Applications potentielles	Statut
FIDO2/WebAuthn	- Authentification sans mot de passe	
- Validation des transactions		
- Simplification de l'authentification forte		

En déploiement (Q3 2025)		
Analyse comportementale (eBiometrics)	- Authentification continue invisible	
- Détection des fraudes comportementales		
- Réduction des frictions d'authentification		
POC en cours		
Quantum-resistant cryptography	- Préparation à la menace quantique	
- Sécurisation des données à long terme		
- Chiffrement des communications sensibles		
Évaluation en laboratoire		
Self-sovereign identity (SSI)	- Contrôle utilisateur sur ses données d'identité	
- Simplification des processus KYC		
- Réduction des risques de vol d'identité		
Participation à des consortiums		

AI/ML for security

- Détection avancée des fraudes
- Prédiction des menaces
- Adaptation dynamique des contrôles

Déploiement partiel

- Adaptation dynamique des contrôles

Collaboration et partenariats

Neo Financia s'engage dans plusieurs initiatives collaboratives pour améliorer la sécurité de l'écosystème financier digital:

Partenariats industriels

- Participation aux groupes de travail sectoriels (FBF, UK Finance)
- Collaboration avec les fintechs spécialisées en sécurité
- Partage d'information sur les menaces
- Développement de standards communs
- Coopération avec les autorités
- Participation aux exercices de cybersécurité sectoriels
- Partage d'information avec les CERT nationaux
- Collaboration avec les forces de l'ordre sur la fraude
- Contribution aux consultations réglementaires
- Innovation ouverte
- Programme de bug bounty
- Collaboration avec la recherche académique
- Participation aux hackathons de sécurité
- Publication des bonnes pratiques

Sécurité cloud

Principes fondamentaux

La sécurité cloud constitue un pilier essentiel de la stratégie de cybersécurité de Neo Financia, en tant que néobanque opérant principalement sur des infrastructures cloud. Cette politique établit les principes, contrôles et responsabilités permettant de sécuriser efficacement les ressources cloud, tout en tirant parti de la flexibilité et de l'innovation offertes par ces technologies.

Objectifs de la sécurité cloud:

- Établir un cadre de gouvernance adapté aux spécificités des environnements cloud
- Définir clairement les responsabilités entre Neo Financia et ses fournisseurs cloud
- Garantir une sécurité homogène à travers les différents environnements cloud utilisés
- Protéger les données et workloads hébergés dans le cloud contre les menaces
- Assurer la conformité aux exigences réglementaires spécifiques aux services financiers
- Permettre l'innovation tout en maintenant un niveau de risque acceptable

---

- Établir les bases d'une architecture cloud résiliente et sécurisée

Cette politique s'applique à l'ensemble des ressources cloud utilisées par Neo Financia, qu'il s'agisse des environnements Azure (70%), OVHcloud (20%) ou AWS (10%), et couvre tous les modèles de déploiement (IaaS, PaaS SaaS).

Stratégie multi-cloud

Approche globale

Neo Financia a adopté une stratégie multi-cloud réfléchie, visant à optimiser les avantages tout en maîtrisant les risques associés:

- Diversification des fournisseurs : Répartition des charges entre plusieurs fournisseurs pour réduire les risques de dépendance
- Spécialisation des usages : Utilisation des forces spécifiques de chaque fournisseur selon les besoins métier
- Résilience accrue : Capacité à maintenir les services en cas de défaillance d'un fournisseur
- Optimisation des coûts : Flexibilité dans le choix des solutions les plus économiques selon les cas d'usage
- Conformité géographique : Adaptation aux exigences de localisation des données selon les juridictions

Répartition des environnements

Fournisseur	Pourcentage	Cas d'usage principaux	Régions utilisées
Microsoft Azure	70%	- Core banking system	
- Applications critiques			
- Analyse de données			
- Services d'authentification			
- France Central (principal)			
- France South (secondaire)			
- West Europe (DR)			
- UK South (services UK)			
OVHcloud	20%	- Systèmes non critiques	
- Environnements de développement			
- Stockage de données archivées			

- Services spécifiques France			
- Roubaix (principal)			
- Gravelines (secondaire)			
- Strasbourg (archivage)			
Amazon Web Services	10%	- Analyses avancées	
- Services spécifiques UK			
- Capacité de débordement			
- Tests de nouvelles technologies			
- EU-West-1 (Ireland)			
- EU-West-2 (London)			
- EU-Central-1 (Frankfurt)			

# Principes d'architecture multi-cloud			

- Conception hybride : Architecture permettant la mobilité des charges entre environnements
- Abstraction des dépendances : Réduction des couplages forts avec les services spécifiques
- Standardisation : Utilisation de formats, protocoles et interfaces standardisés
- Automatisation : Infrastructure as Code (IaC) pour tous les environnements
- Surveillance unifiée : Vue consolidée de la sécurité à travers tous les clouds
- Contrôles harmonisés : Cohérence des politiques de sécurité sur toutes les plateformes

Modèle de responsabilité partagée

Principes de partage des responsabilités

Neo Financia applique le modèle de responsabilité partagée en adaptant sa mise en œuvre aux différents types de services cloud:

graph TD subgraph "Responsabilité Neo Financia" A1["Données clients"] A2["Accès et identités"] A3["Applications"] A4["Configuration des services cloud"] end

subgraph "Responsabilité partagée (varie selon le modèle)" B1["Runtime, middleware"] B2["Système d'exploitation"] B3["Virtualisation"] B4["Réseau (configuration)"] end

subgraph "Fournisseur Cloud" C1["Matériel physique"] C2["Réseau (infrastructure)"] C3["Datacenters"] end

subgraph "Types de services" D1["IaaS"] D2["PaaS"] D3["SaaS"] end

Matrice de responsabilités détaillée

Couche	IaaS	PaaS	SaaS
Données clients et contenu	Neo Financia	Neo Financia	Neo Financia
Gestion des accès et identités	Neo Financia	Neo Financia	Neo Financia

---

Applications	Neo Financia	Neo Financia	Fournisseur
Configuration de sécurité	Neo Financia	Neo Financia	Partagée
Système d'exploitation	Neo Financia	Fournisseur	Fournisseur
Middleware, runtime	Neo Financia	Fournisseur	Fournisseur
Virtualisation, conteneurs	Fournisseur	Fournisseur	Fournisseur
Réseaux	Partagée	Fournisseur	Fournisseur
Infrastructure physique	Fournisseur	Fournisseur	Fournisseur

Contrôles à implémenter par Neo Financia

En fonction du modèle de service utilisé, Neo Financia met en œuvre des contrôles spécifiques

Modèle	Contrôles obligatoires
IaaS	- Durcissement des systèmes d'exploitation
- Gestion des patchs et vulnérabilités	
- Configuration des pare-feu et sécurité réseau	
-	

Chiffrement des données	
- Gestion des secrets et des clés	
- Surveillance complète de la pile applicative	
PaaS	- Sécurisation des déploiements d'applications
- Configuration sécurisée des services	
- Gestion des identités et des accès	
- Chiffrement des données	
- Surveillance des activités et alertes	
- Tests de sécurité des applications	
SaaS	- Configuration des contrôles d'accès
- Protection des données sensibles	
- Gestion de l'authentification (SSO, MFA)	
- Surveillance des activités utilisateurs	
- Évaluation de la conformité des fournisseurs	
- Plans de continuité et de sortie	

# Gouvernance cloud	

Organisation et responsabilités

Neo Financia a établi une structure de gouvernance spécifique pour ses environnements cloud.

- Cloud Security Board : Comité décisionnel sur les aspects sécurité cloud
- Composition : RSSI, DSI, Cloud Architects, Responsables Cloud de chaque direction
- Fréquence : Réunion mensuelle, reporting trimestriel au COSEC
- Missions : Validation des architectures de référence, politiques cloud, exceptions
- Cloud Center of Excellence (CCoE) : Équipe d'experts multi-disciplinaire
- Composition : Architectes, Sécurité, Ingénieurs cloud, Finance, Conformité
- Missions : Développement des standards, bonnes pratiques, formation
- Cloud Security Team : Équipe dédiée au sein de la direction Sécurité
- Composition : 5 spécialistes en sécurité cloud
- Missions : Conception et implémentation des contrôles, évaluation continue
- Cloud Custodians : Relais dans chaque équipe produit
- Missions : Application des standards, contrôles de premier niveau

Politiques et standards

La gouvernance cloud s'appuie sur un référentiel documentaire complet.

Document	Contenu	Public cible	Fréquence de mise à jour
Stratégie Cloud	Vision, objectifs, approche multi-cloud, modèles d'adoption	Direction, Management	Annuelle
Politique de Sécurité Cloud	Exigences de sécurité, standards minimum, conformité	Équipes IT, Sécurité	Annuelle
Architectures de référence	Modèles sécurisés par fournisseur et cas d'usage	Architectes, Développeurs	Semestrielle
Règles de configuration	Paramètres techniques détaillés par service	Équipes Cloud Ops	Trimestrielle
Procédures opérationnelles	Instructions détaillées pour les tâches courantes	Équipes Opérations	Continue
Matrice de contrôles	Correspondance entre exigences et implémentations	Sécurité, Conformité	Trimestrielle

Processus de validation cloud

Neo Financia a établi un processus formel pour l'adoption de nouveaux services cloud.

1. Qualification initiale : Évaluation préliminaire du service

- Analyse des besoins et cas d'usage
- Vérification de la compatibilité avec la stratégie
- Identification des risques potentiels

2. Évaluation de sécurité : Analyse approfondie des aspects sécurité

- Revue des mécanismes de sécurité disponibles
- Analyse des certifications et conformité
- Évaluation des contrôles compensatoires nécessaires

3. Validation d'architecture : Conception du modèle d'intégration

- Élaboration de l'architecture cible
- Définition des contrôles de sécurité
- Validation par le Cloud Security Board
- Phase pilote : Déploiement contrôlé à petite échelle
- Implémentation dans un environnement restreint
- Tests de sécurité spécifiques
- Mesure de l'efficacité des contrôles
- Homologation : Validation formelle pour utilisation
- Bilan des tests et retours pilote
- Documentation des configurations approuvées
- Ajout au catalogue des services autorisés

Sécurité de l'infrastructure cloud

Sécurité réseau cloud

Neo Financia applique une approche de défense en profondeur pour son infrastructure réseau cloud :

Segmentation avancée

- Isolation stricte des environnements (production, test, développement)
- Séparation par niveau de sensibilité des données
- Micro-segmentation pour les workloads critiques
- Segmentation par fonctionnalité métier

Contrôles de flux

- Principe du moindre privilège pour toutes les communications
- Règles restrictives par défaut (deny-all par défaut)
- Documentation et justification de chaque règle de flux
- Revue périodique (trimestrielle) des règles
- Protection périmétrique
- Pare-feu nouvelle génération (NGFW) virtuels
- Web Application Firewall (WAF) pour les services exposés
- Protection DDoS native et renforcée
- Détection d'intrusion (IDS/IPS) en ligne

Connectivité sécurisée

- Liaisons privées dédiées avec les fournisseurs (ExpressRoute, Direct Connect)
- Tunnels VPN site-à-site redondants pour les connexions secondaires
- Chiffrement de tout le trafic inter-régions

- Accès des administrateurs via jumphost et bastion sécurisés

Architecture de référence

Neo Financia a défini des architectures de référence pour chaque fournisseur cloud :

Architecture standard Azure (exemple) :

flowchart TD subgraph "Azure Region" subgraph "Azure Virtual Network" FrontendSubnet["Frontend\nSubnet"] ServicesSubnet["Services\nSubnet"] BackendSubnet["Backend\nSubnet"]

FrontendNSG["NSG/\nFirewall"] ServicesNSG["NSG/\nFirewall"] BackendNSG["NSG/\nFirewall"]

FrontendSubnet --> FrontendNSG ServicesSubnet --> ServicesNSG BackendSubnet --> BackendNSG end

ServiceEndpoints["Service Endpoints / Private Link"]

PaaSServices["PaaS Services (SQL, Storage, KeyVault, etc.)"]

Azure_Virtual_Network --> ServiceEndpoints ServiceEndpoints --> PaaSServices end

Caractéristiques clés

- Séparation en couches (frontend, services, données)
- Filtrage à chaque niveau
- Accès privé aux services PaaS (Private Link/Endpoint)
- Points de contrôle sécurisés entre zones

Sécurisation des services managés

Neo Financia applique des contrôles spécifiques pour les services managés (PaaS)

Type de service	Contrôles obligatoires	Bonnes pratiques
Bases de données managées	- Accès privé uniquement (Private Link/Endpoint)	
- Chiffrement transparent des données		
- Authentification forte (IAM + MFA)		
- Journalisation complète des accès et requêtes		
- Rotation automatique des clés de chiffrement		
- Déploiement multi-régions pour la résilience		
-		

Protection des données sensibles (Dynamic Data Masking)		
Stockage d'objets	- Blocage de l'accès public par défaut	
- Chiffrement systématique (SSE avec CMEK)		
- Signatures d'accès temporaires (SAS)		
- Stratégie de rétention et protection contre la suppression		
- Versioning pour les objets critiques		
- Réplication géographique pour la durabilité		
- Analyse de malware automatique		
Services applicatifs	- HTTPS obligatoire, TLS 1.2+ uniquement	
- Identités managées pour l'authentification		
- Restrictions IP pour l'administration		
- Isolation réseau (intégration VNET)		
- Web Application Firewall activé		
- Autoscaling avec limites définies		
- Surveillance des performances et anomalies		

Gestion des identités et des accès cloud

Architecture IAM cloud

Neo Financia a implémenté une architecture IAM centralisée et cohérente.

- Fédération d'identité
- Source d'autorité unique (Azure AD)
- Fédération avec tous les fournisseurs cloud
- Single Sign-On (SSO) pour tous les services
- Centralisation de l'authentification multifacteur
- Modèle de privilèges
- Principe du moindre privilège strictement appliqué
- Modèle RBAC (Role-Based Access Control) standardisé
- Définition de rôles personnalisés restrictifs
- Attribution temporaire pour les accès critiques (JIT)
- Séparation des environnements

- Tenants/comptes dédiés par environnement
- Séparation stricte production/non-production
- Identités techniques distinctes par environnement
- Cloisonnement entre fournisseurs cloud

Modèle de gestion des accès

Neo Financia a structuré la gestion des accès cloud selon le modèle suivant

Niveau d'accès	Description	Contrôles spécifiques
Accès de gouvernance	Administration des souscriptions, facturation, politiques globales	- Nombre d'utilisateurs strictement limité
- MFA obligatoire pour toute action		
- Révision mensuelle des droits		
- Audit détaillé de toutes les actions		

Accès administrateur	Gestion de l'infrastructure et des services techniques	- Accès Just-In-Time (sessions limitées)
- Attribution par workflow formel		
- Enregistrement des sessions		
- Approbation N+2 pour la production		
Accès opérationnel	Exploitation quotidienne des services	- Rôles prédéfinis restrictifs
- Ségrégation des tâches (SoD)		
- Revue trimestrielle des droits		
- Attribution par workflow standard		
Accès développement/test	Développement et test des applications	- Limité aux environnements non-production
- Isolation par projet ou équipe		
- Contrôles de coûts et quotas		
- Impossibilité d'accéder à la production		
Accès service	Interactions entre services et applications	- Utilisation d'identités managées
-		

Éviter les secrets statiques		

- Limitation précise des périmètres d’accès		
- Rotation automatique des identifiants		

Authentification et accès privilégiés

Neo Financia applique des exigences strictes pour l'authentification aux environnements cloud :

Authentification des utilisateurs

- MFA obligatoire pour tous les accès aux environnements cloud
- MFA renforcé (FIDO2, certificats) pour les accès sensibles
- Authentification contextuelle (localisation, appareil, comportement)
- SSO avec limitation des sessions (8h maximum)

Gestion des accès privilégiés (PAM)

- Accès just-in-time pour tous les rôles administratifs
- Workflow d'approbation multi-niveaux
- Journalisation renforcée et surveillance en temps réel
- Sessions administratives limitées à 2h maximum
- Enregistrement vidéo des sessions privilégiées

Accès d'urgence (break-glass)

- Comptes d'urgence sous double-contrôle
- Stockage sécurisé des informations d'accès (coffre physique)
- Processus formel d'activation avec validation RSSI
- Audit post-utilisation obligatoire

Protection des données dans le cloud

Classification et localisation

Néo Financia applique une politique stricte concernant la localisation des données dans le cloud.

Classification	Exigences de localisation	Contrôles supplémentaires

P3 - Critique	- Stockage exclusivement en France	
- Fournisseurs qualifiés SecNumCloud pour les données les plus sensibles		
- Réplication limitée au territoire national		
- Chiffrement renforcé avec clés gérées par Neo Financia		
- Isolation complète des autres données		
- Audits réguliers de localisation		
P2 - Confidentiel	- Stockage principal en France	
- Réplication possible dans l'UE uniquement		
- Chiffrement obligatoire (CMEK)		
- Ségrégation logique stricte		

	- Données britanniques dans datacenters UK	
- Vérification de conformité RGPD		
---	---	---

P1 - Interne	- Stockage principal en UE	
- Réplication possible Europe et UK		

- Éviter les transferts hors zone		
- Chiffrement standard		
- Contrôles d'accès adaptés		
- Journalisation des accès		
P0 - Public	- Aucune restriction géographique	
- Préférence pour solutions optimisées en coût		
- Contrôle d'intégrité		
- Protection contre la modification non autorisée		

Stratégie de chiffrement cloud

Neo Financia implémente une stratégie de chiffrement complète pour les environnements cloud

Principes fondamentaux

- Chiffrement systématique des données au repos et en transit
- Contrôle des clés adapté à la sensibilité des données
- Séparation des rôles pour la gestion des clés
- Rotation régulière des clés cryptographiques

Modèles de gestion des clés

- BYOK (Bring Your Own Key) : Clés gérées par Neo Financia dans les HSM cloud
- HYOK (Hold Your Own Key) : Clés conservées on-premises pour les données critiques
- CSEK (Customer-Supplied Encryption Keys) : Clés fournies lors de l'utilisation
- Clés gérées par le fournisseur : Pour les données non sensibles uniquement

Infrastructure de gestion des clés

- Utilisation de services HSM certifiés (FIPS 140-2 Level 3 minimum)
- Architecture multi-régions pour la haute disponibilité
- Sauvegarde sécurisée et procédures de restauration testées
- Journalisation complète des opérations sur les clés

Matrice de chiffrement par classification :

Classification	Au repos	En transit	Gestion des clés
P3 - Critique	AES-256 (double chiffrement)	TLS 1.3 avec PFS	HYOK (clés on-premises)
P2 - Confidentiel	AES-256	TLS 1.3 avec PFS	BYOK
P1 - Interne	AES-256	TLS 1.2+	CSEK ou BYOK

Cycle de vie des données cloud

Neo Financia gère le cycle de vie complet des données dans le cloud.

Création/Ingestion

- Classification automatique à la création
- Application des contrôles de chiffrement
- Vérification de la localisation appropriée

Stockage

- Application des politiques de rétention
- Contrôles d'accès basés sur la classification
- Surveillance des accès et modifications

Utilisation/Traitement

- Contrôles de sécurité lors du traitement
- Anonymisation/pseudonymisation pour les analyses
- Prévention des fuites de données (DLP)

Partage/Transmission

- Canaux sécurisés et chiffrés
- Autorisation formelle pour les partages externes
- Création d'accès temporaires pour les partenaires

Archivage

- Transition vers stockage à long terme
- Maintien des métadonnées et contrôles
- Validation périodique de l'intégrité

Suppression

- Effacement sécurisé conforme aux normes
- Destruction des clés de chiffrement
- Certification d'effacement pour les données critiques

Sécurité des workloads cloud

Sécurisation des machines virtuelles

Néo-Financia applique les contrôles suivants pour les machines virtuelles dans le cloud

Durcissement des systèmes

- Images de base durcies et pré-validées
- Configuration selon CIS Benchmarks
- Application automatisée des correctifs de sécurité
- Désactivation des services non essentiels

Gestion des accès

- Authentification par clés SSH uniquement (Linux)
- MFA obligatoire pour RDP (Windows)

- Accès via bastions dédiés
- Pas d'adresse IP publique directe

Protection en temps réel

- EDR cloud-native sur toutes les instances
- Anti-malware nouvelle génération
- Surveillance comportementale
- Détection des modifications non autorisées

Surveillance et journalisation

- Collecte centralisée des journaux
- Surveillance des performances et activités
- Détection des comportements anormaux
- Alertes en temps réel pour les incidents

Sécurité des conteneurs

Pour les workloads conteneurisés, Neo Financia implémente.

Sécurité des images

- Utilisation d'images de base minimales
- Scan automatique des vulnérabilités
- Signatures d'images obligatoires
- Registre privé sécurisé avec contrôle d'accès

Orchestration sécurisée

- Configuration durcie des clusters Kubernetes
- Isolation réseau entre pods et namespaces
- Application de politiques de sécurité
- Limites de ressources et quotas

Runtime protection

- Surveillance comportementale en temps réel
- Détection d'activités suspectes
- Application de politiques d'admission
- Isolation renforcée des conteneurs

Secret management

- Gestion centralisée des secrets
- Identités managées pour l'authentification
- Rotation automatique des credentials
- Isolation des secrets par namespace

Sécurité des services serverless

Pour les architectures serverless, Neo-Financia met en œuvre

Contrôles d'accès

- Identités managées pour l'authentification
- Attribution précise des permissions
- Isolation des environnements
- Accès aux ressources via réseaux privés

Sécurité du code

- Analyse statique (SAST) systématique
- Limitation des dépendances
- Validation des entrées rigoureuse
- Contrôle des bibliothèques tierces

Configuration sécurisée

- Définition de timeouts appropriés
- Limitation des privilèges d'exécution
- Isolation renforcée entre fonctions
- Paramétrage adapté à la charge

Journalisation et observabilité

- Traçabilité complète des exécutions
- Monitoring des performances
- Détection des comportements anormaux
- Alertes sur erreurs répétées

Surveillance et gestion des incidents cloud

Logging et monitoring

Neo Financia a implémenté une stratégie complète de surveillance de ses environnements cloud

Architecture de surveillance

- Collecte centralisée dans un SIEM unifié
- Normalisation des formats de logs cross-cloud
- Rétention adaptée à la criticité (12-24 mois)
- Architecture multi-niveaux pour optimiser les coûts

Sources de journaux

- Journaux d'infrastructure (plateformes, services, réseaux)
- Journaux d'identité et accès (authentification, autorisation)
- Journaux de sécurité (alertes, détection)
- Journaux de conformité (contrôles, audit)
- Journaux applicatifs (performance, erreurs)

Détection des menaces

- Règles de détection spécifiques cloud
- Détection des comportements anormaux (UEBA
- Corrélation cross-cloud des événements
- Intégration des flux de threat intelligence

Détection et réponse aux incidents

Neo Financia a adapté ses processus de gestion des incidents au contexte cloud

Phase	Actions spécifiques cloud	Outils
Préparation	- Playbooks dédiés aux incidents cloud	
- Runbooks automatisés		

	- Formation spécifique des équipes	
- Accès d'urgence pré-configurés		
- Portail de documentation		
- Environnement forensics cloud		

| --- | --- | --- |

Détection	- Surveillance multi-cloud 24/7	
- Détection des menaces spécifiques cloud		
- Alertes sur configurations dangereuses		
- SIEM unifié		
- CSPM (Cloud Security Posture Management)		
- CWP (Cloud Workload Protection)		
Confinement	- Isolation réseau automatisée	
- Suspension des accès compromis		
- Snapshot des ressources affectées		
- Automatisation cloud (Azure Runbooks, AWS Lambda)		
- IAM emergency		
- Outils de quarantaine		
Éradication	- Reconstruction immaculée des ressources	
- Rotation des secrets et credentials		
- Correction des failles de configuration		
- Infrastructure as Code		

- Outils de remédiation		
- Key Vault/Secrets Manager		
Récupération	- Déploiement immaculé via pipelines	
- Validation des contrôles de sécurité		
- Tests de non-régression		
- CI/CD pipelines		
- Outils de validation		
- Scanners de vulnérabilités		
Post-Incident	- Analyse cloud-forensics	
- Revue des lacunes de sécurité		
- Amélioration des contrôles cloud		
- Outils d'analyse forensique cloud		
- Benchmark frameworks		
- Outils de modélisation des menaces		

Gestion du Shadow IT cloud

Neo Financia a implémenté un programme de détection et de gestion du Shadow IT cloud

Détection proactive

- Scanning du trafic réseau sortant
- Surveillance des DNS et certificats
- Solutions CASB pour identifier les services non autorisés
- Programme de divulgation volontaire

Évaluation et triage

- Classification des services détectés par niveau de risque

- Évaluation de la conformité réglementaire
- Analyse des données potentiellement exposées
- Identification des besoins métier sous-jacents

Remédiation

- Processus d'intégration au catalogue officie
- Migration vers alternatives approuvées
- Accompagnement des utilisateurs
- Approche pédagogique plutôt que punitive

Prévention

- Catalogue de services cloud approuvés
- Processus accéléré d'évaluation des nouveaux services
- Sensibilisation et formation des utilisateurs
- Contrôles techniques (filtrage, CASB)

Conformité et gestion des risques cloud

Exigences réglementaires

Neo Financia doit se conformer à plusieurs cadres réglementaires concernant ses activités cloud

Réglementation	Implications principales	Mesures spécifiques
DORA		
(Digital Operational		
Resilience Act)	- Gestion des risques liés aux tiers (CSP)	
- Test de résilience opérationnelle		
- Plan de continuité cloud		
- Stratégie de sortie		
- Due diligence renforcée des fournisseurs		
-		

Tests de basculement inter-cloud		
- Architecture multi-cloud active		
- Monitoring résilience 24/7		
RGPD	- Localisation des données personnelles	
- Sécurité du traitement		
- Sous-traitance et responsabilités		
- Transferts internationaux		
- Mapping des données dans le cloud		
- Chiffrement et pseudonymisation		
- Clauses contractuelles renforcées		
- Contrôles de localisation		
EBA Guidelines		
(Outsourcing		
Arrangements)	- Gouvernance des services externalisés	
- Évaluation et due diligence		
- Droit d'audit		

- Registre des services cloud		
- Classification des services critiques		
- Clauses d'audit renforcées		

	• Plans de sortie	• Tests de réversibilité
---	---	---
NIS2	• Mesures de sécurité pour entités essentielles • Gestion des incidents • Chaîne d'approvisionnement sécurisée • Notification des incidents	• Framework de contrôles aligné NIS2 • Procédures de notification adaptées • Évaluation des fournisseurs cloud • Surveillance renforcée
SecNumCloud (pour données critiques)	• Souveraineté des données sensibles • Contrôle par des entités européennes • Protection contre législations extra-européennes	• Utilisation de clouds qualifiés • Isolation des données critiques • Contrôles juridiques renforcés

Évaluation des risques cloud

Neo Financia a adapté son approche de gestion des risques au contexte cloud.

- Risques spécifiques cloud identifiés
- Perte de gouvernance et contrôle

- Dépendance aux fournisseurs (vendor lock-in)
- Défaillance d'isolation multi-tenants
- Compromission des interfaces de gestior
- Protection insuffisante des données
- Résilience des services cloud
- Dérive des configurations et compliance
- Méthode d'évaluation
- Identification des services cloud critiques
- Évaluation des contrôles disponibles
- Analyse des écarts (gap analysis)
- Attribution de niveaux de risque résiduels
- Plan de traitement priorisé
- Fréquence et déclencheurs
- Évaluation complète annuelle
- Réévaluation lors de changements majeurs
- Analyse ad hoc pour nouveaux services
- Revue après incidents significatifs

Stratégie de sortie cloud

Neo Financia a développé une stratégie complète pour gérer la sortie d'un fournisseur cloud :

Scénarios de sortie

- Fin de relation commerciale planifiée
- Défaillance du fournisseur
- Changement réglementaire
- Dégradation de service inacceptable
- Incident de sécurité majeur

Mesures préventives

- Architecture agnostique (minimisation des dépendances spécifiques)
- Documentation des dépendances techniques
- Clauses contractuelles (assistance, transition)
- Conservation des compétences internes

Plan de sortie

- Procédures détaillées de migration
- Identification des destinations alternatives
- Mécanismes d'extraction des données
- Séquence de transition par priorité
- Estimations des délais et coûts

Test du plan

- Exercices partiels périodiques
- Vérification des procédures d'extraction
- Validation des formats d'exportation
- Simulation des scénarios critiques

Cette stratégie est formellement documentée, régulièrement mise à jour, et validée par le RSSI et la DSI.

Gestion des fournisseurs cloud

Évaluation et sélection

Neo Financia suit un processus rigoureux pour la sélection de ses fournisseurs cloud :

1. Définition des exigences

- Spécifications fonctionnelles et techniques
- Exigences de sécurité et conformité
- Niveaux de service attendus
- Contraintes réglementaires

2. Due diligence

- Évaluation de la solidité financière
- Analyse des certifications (ISO 27001, SOC 2, etc.)
- Audit de sécurité si possible
- Vérification des références
- Évaluation de la maturité opérationnelle

3. Évaluation des risques

- Analyse d'impact sur l'activité
- Identification des risques spécifiques
- Évaluation des contrôles disponibles

- Détermination du risque résiduel

4. Contractualisation

- Clauses de sécurité détaillées
- SLA adaptés aux besoins critiques
- Exigences de reporting et transparence
- Droit d'audit et de contrôle

- Conditions de sortie et réversibilité

Surveillance et gouvernance continue

Neo-Financia assure un suivi continu de ses fournisseurs cloud.

Suivi des performances

- Tableau de bord des SL A
- Mesure continue de la disponibilité
- Suivi des incidents et problèmes
- Évaluation des temps de résolution

Revue de sécurité

- Analyse des rapports d'audit tiers
- Exercice du droit d'audit
- Suivi des vulnérabilités et correctifs
- Évaluation continue des risques

Gouvernance formalisée

- Comités de suivi trimestriels
- Revue annuelle approfondie
- Gestion des changements fournisseurs
- Coordination de la roadmap
- Plans d'amélioration
- Identification des axes d'amélioration
- Définition d'objectifs partagés
- Suivi des actions correctives
- Mise à jour des exigences

Protection des données

Principes fondamentaux

La protection des données constitue un pilier essentiel de la stratégie globale de sécurité de Neo Financia. En tant qu'institution financière digitale traitant des données sensibles pour ses 2 millions de clients, Neo Financia s'engage à assurer le plus haut niveau de protection des données personnelles et financières, conformément aux réglementations applicables et aux attentes de ses clients.

Objectifs de la protection des données :

- Garantir la conformité aux réglementations sur la protection des données (RGPD, UK GDPR, sectorielles'

- Protéger les données personnelles et financières contre tout accès, utilisation ou divulgation non autorisés
- Respecter les droits des personnes concernées sur leurs données
- Assurer la transparence des traitements de données réalisés
- Minimiser la collecte de données au strict nécessaire (principe de minimisation)

- Intégrer la protection des données dès la conception des services (Privacy by Design)
- Maintenir la confiance des clients dans la capacité de Neo Financia à protéger leurs données

Cette politique s'applique à l'ensemble des données personnelles et sensibles traitées par Neo Financia, que ce soit pour ses clients, prospects, collaborateurs ou partenaires, dans tous ses sites (Paris, Lyon, Londres) et sur toutes ses plateformes technologiques.

Cadre réglementaire

Neo Financia opère dans un environnement réglementaire complexe, particulièrement en matière de protection des données, en raison de sa présence dans plusieurs juridictions et du caractère sensible des données financières traitées

Principales réglementations applicables

Réglementation	Champ d'application	Principales exigences	Impact pour Neo Financia
Règlement Général sur la Protection des Données (RGPD)	Traitement des données personnelles des résidents de l'UE	- Base légale pour tout traitement	
- Droits des personnes concernées			
- Mesures techniques et organisationnelles			
- Notification des violations			
- Analyses d'impact			
S'applique à l'ensemble des activités en France et aux clients européens			
UK GDPR / Data Protection Act 2018	Traitement des données personnelles des résidents du Royaume-Uni	- Similaire au RGPD avec spécificités britanniques	
- Régime spécifique de transferts internationaux post-Brexit			

S'applique aux opérations britanniques et aux clients UK			
Directive sur les Services de Paiement (DSP2)	Services de paiement et accès aux comptes	- Exigences d'authentification forte	
Impact sur les processus d'authentification et le partage de données			

		• Sécurité des données de paiement • Règles d'accès via API	
Règlement elDAS	Identification électronique et services de confiance	• Signature électronique • Identification et authentification	Impacte les processus d'onboarding et de contractualisation
Code monétaire et financier	Exigences sectorielles bancaires	• Secret bancaire • Conservation des données • Lutte anti-blanchiment	Exigences spécifiques pour les données financières
Digital Operational Resilience Act (DORA)	Résilience opérationnelle numérique pour le secteur financier	• Gestion des risques liés aux TIC • Tests de résilience • Signalement d'incidents	Renforce les exigences de protection des données en cas d'incident

Autres référentiels

En complément du cadre réglementaire, Neo Financia s'appuie sur plusieurs standards et bonnes pratiques

- ISO 27701 : Extension de l'ISO 27001 spécifique à la gestion des informations de confidentialité
- Standards de sécurité PCI DSS : Pour la protection des données de cartes de paiement
- Recommandations de la CNIL : Guides et référentiels sectoriels
- Recommandations de l'ICO : Guidelines britanniques pour la protection des données
- Lignes directrices du Comité Européen de la Protection des Données (EDPB) : Interprétations officielles du RGPD

Gouvernance des données personnelles

Organisation et responsabilités

Neo Financia a mis en place une organisation dédiée pour assurer la protection des données :

Fonction	Responsabilités
Délégué à la Protection des Données (DPO)	- Supervision de la conformité au RGPD
- Point de contact pour les autorités de contrôle	
- Conseil et formation en interne	
- Supervision des analyses d'impact	

Data Protection Officer UK	- Traitement des demandes des personnes concernées
---	---
	- Gestion de la conformité spécifique au UK GDPR
- Point de contact pour l'ICO au Royaume-Uni	
- Coordination avec le DPO Groupe	
Privacy Champions (par direction)	- Relais du DPO dans chaque département
- Promotion de la culture de protection des données	
- Identification des nouveaux traitements	

Comité Data Privacy	- Supervision de la stratégie protection des données
- Arbitrage des questions complexes	
- Validation des grandes orientations	
- Revue trimestrielle de la conformité	
Direction Juridique	- Support pour les aspects légaux
- Révision des contrats	
- Veille réglementaire conjointe avec le DPO	
RSSI et équipe cybersécurité	- Mise en œuvre des mesures techniques de protection
- Gestion des incidents de sécurité impliquant des données personnelles	
- Tests de sécurité et audits	
Data Governance Officer	- Gestion de la qualité des données
- Cartographie des flux de données	
- Coordination avec la protection des données	

Rapports hiérarchiques et indépendance

- Le DPO est rattaché directement au Comité Exécutif pour garantir son indépendance
- Le DPO communique directement au Comité des Risques du Conseil d'Administration sur base trimestrielle
- Le DPO UK rapporte fonctionnellement au DPO Groupe et hiérarchiquement à la Direction UK
- Le Comité Data Privacy est présidé par un membre du COMEX (Directeur de la Conformité)

Indépendance du DPO :

Conformément à l'article 38 du RGPD, Neo Financia garantit que le DPO :

- Est associé à toutes les questions relatives à la protection des données
- Dispose des ressources nécessaires à l'exercice de ses missions
- Agit en toute indépendance et sans recevoir d'instructions
- Ne peut être sanctionné pour l'exercice de ses missions
- A un accès direct au plus haut niveau de la direction

Principes de traitement des données personnelles

Neo Financia s'engage à respecter les principes fondamentaux de la protection des données dans tous ses traitements

Principe	Description	Mise en œuvre
Licéité, loyauté et transparence	Les données sont traitées de manière licite, loyale et transparente vis-à-vis de la personne concernée	- Base juridique identifiée pour chaque traitement
- Notices d'information claires et accessibles		
- Processus de consentement explicite		
Limitation des finalités	Les données sont collectées pour des finalités déterminées, explicites et légitimes	- Documentation des finalités dans le registre
- Vérification de la compatibilité des usages		
- Information préalable sur les finalités		
Minimisation des données	Seules les données adéquates, pertinentes et limitées au nécessaire	- Revue critique

	sont collectées	de chaque donnée collectée
- Suppression des champs non essentiels		
- Contrôle lors de la conception des formulaires		

Exactitude	Les données sont exactes et tenues à jour	- Procédures de mise à jour régulière
- Validation des données critiques		
- Interface permettant la mise à jour par les clients		
---	---	---
Limitation de conservation	Les données sont conservées pour une durée limitée	- Politique de rétention documentée
- Purge automatisée des données obsolètes		
- Archivage intermédiaire conforme		
Intégrité et confidentialité	Les données sont protégées contre tout traitement non autorisé ou illicite	- Chiffrement des données sensibles
- Contrôles d'accès stricts basés sur le besoin d'en connaître		
-		

Mesures de sécurité techniques et organisationnelles		
Responsabilité (Accountability)	Capacité à démontrer la conformité aux principes	- Documentation complète des traitements
- Traçabilité des décisions		
- Audits réguliers de conformité		

Bases légales des traitements

Neo Financia identifie et documente systématiquement la base légale de chaque traitement.

Base légale	Cas d'utilisation	Exemples chez Neo Financia
Consentement	Lorsque la personne concernée donne explicitement son accord pour un traitement spécifique	- Marketing ciblé
- Cookies non essentiels		
- Participation à des études		
Exécution d'un contrat	Lorsque le traitement est nécessaire à l'exécution d'un contrat avec la personne concernée	- Gestion du compte bancaire
- Exécution des opérations de paiement		

Obligation légale	Lorsque le traitement est imposé par la loi	- Gestion des

		crédits et épargnes
---	---	---
		- KYC et lutte anti-blanchiment
- Déclarations réglementaires		
- Conservation légale des données		
Intérêt vital	Protection d'intérêts vitaux	- Rarement utilisé
- Situations d'urgence médicale		
Mission d'intérêt public	Exécution d'une mission d'intérêt public	- Non applicable aux activités courantes
Intérêts légitimes	Lorsque le traitement est nécessaire aux intérêts légitimes poursuivis, sous réserve des droits fondamentaux	- Prévention de la fraude
- Sécurité des systèmes d'information		
- Marketing direct simple (clients existants)		
- Amélioration des services		

Attention aux intérêts légitimes :

Tout traitement basé sur l'intérêt légitime doit faire l'objet d'un test de mise en balance (LIA - Legitimate Interest Assessment) documenté qui démontre que :

- L'intérêt poursuivi est légitime
- Le traitement est nécessaire pour atteindre cet objectif
- Les droits des personnes ne prévalent pas sur cet intérêt

Ces analyses sont validées par le DPO avant tout nouveau traitement.

Droits des personnes concernées

Catalogue des droits

Neo Financia garantit l'exercice effectif des droits des personnes concernées sur leurs données personnelles

Droit	Description	Mise en œuvre	Exceptions
Droit d'information	Être informé sur le traitement de ses données de manière claire et transparente	- Politique de confidentialité	
- Notices d'information contextuelles			
- Information par couches			
Information déjà connue, impossibilité, effort disproportionné			
Droit d'accès	Obtenir une copie de ses données et des informations sur leur traitement	- Portail client self-service	
- Procédure de demande formalisée			
- Vérification d'identité sécurisée			
Demandes manifestement			

infondées ou excessives			
Droit de rectification	Faire corriger les données inexactes ou compléter les données incomplètes	- Interface de modification en ligne	
- Procédure de vérification des modifications sensibles			
Données historiques nécessaires (ex: transactions passées)			
Droit à l'effacement	Obtenir la suppression de ses données sous certaines conditions	- Processus de suppression défini	
- Vérification des obligations légales de conservation			
Obligations légales, défense juridique, intérêt public			
Droit à la limitation	Restreindre temporairement le traitement de ses données	- Mécanisme de gel des traitements	
- Conservation avec restriction d'usage			
Motifs d'intérêt public importants			

Droit à la portabilité	**Récupérer ses données dans un format structuré et les transférer**	**• Export de données au format standard (CSV, JSON) • API Open Banking pour les données financières**	**Traitements non basés sur le consentement ou le contrat**
Droit	S'opposer au	• Opt-out simple	Motifs légitimes

d'opposition	traitement de ses données, notamment pour le marketing	pour le marketing • Procédure d'évaluation des oppositions	impérieux, obligations légales
Droit relatif à la décision automatisée	Ne pas faire l'objet d'une décision basée uniquement sur un traitement automatisé	• Possibilité d'intervention humaine • Explicabilité des décisions automatisées	Nécessaire au contrat, autorisé par la loi, consentement explicite

Gestion des demandes d'exercice des droits

Neo Financia a mis en place un processus structuré pour traiter les demandes d'exercice des droits

1. Réception

- Canaux multiples : espace client, email dédié, formulaire web, courrier postal
- Centralisation auprès de l'équipe DPC
- Enregistrement systématique dans l'outil de suivi des demandes

2. Vérification d'identité

- Procédure sécurisée d'authentification
- Niveau de vérification adapté à la sensibilité des données
- Utilisation de l'authentification existante dans l'espace client

3. Analyse et traitement

- Qualification de la demande
- Vérification des exceptions applicables
- Collecte des données concernées
- Mise en œuvre technique de la réponse

4. Réponse

- Transmission sécurisée des informations
- Format adapté et compréhensible
- Documentation des actions réalisées

5. Suivi et clôture

- Enregistrement de la réponse fournie

- Mesure des délais de traitement
- Conservation des preuves de traitement

Les demandes sont traitées dans un délai d'un mois, extensible de deux mois supplémentaires en cas de demande complexe ou nombreuse, avec information de la personne concernée.

Mesures d'information des personnes

Neo Financia adopte une approche transparente et multicouche pour informer les personnes sur le traitement de leurs données:

- Politique de confidentialité globale
- Document complet disponible sur le site web et l'application
- Structure claire et langage accessible
- Version PDF téléchargeable
- Historique des versions conservé
- Notices d'information contextuelles
- Informations spécifiques lors de la collecte des données
- Format adapté au contexte (formulaire, application mobile)
- Précision des finalités spécifiques
- Centre de préférences de confidentialité
- Interface dédiée dans l'espace client
- Gestion centralisée des consentements
- Tableau de bord des données détenues
- Communications régulières
- Mises à jour sur les pratiques de données
- Information en cas de modification significative des traitements
- Section dédiée dans les communications périodiques

Registre des activités de traitement

Conformément à l'article 30 du RGPD, Neo Financia maintient un registre complet et à jour de ses activités de traitement.

Structure du registre

Le registre est structuré selon les catégories suivantes.

Section	Contenu
Identification du traitement	- Nom et description du traitement
- Direction responsable	
- Référent métier et DPO	
- Date de création et mises à jour	

Acteurs et responsabilités	- Responsable de traitement
- Co-responsables éventuels	

- Sous-traitants impliqués	
- Destinataires des données	
---	---
Caractéristiques du traitement	- Finalités détaillées
- Base légale et justification	
- Nécessité et proportionnalité	
- Processus de collecte	
Catégories de données	- Liste des données traitées
- Catégories particulières éventuelles	
- Source des données	
- Volumétrie approximative	
Personnes concernées	- Catégories de personnes
- Estimation du nombre	
- Vulnérabilités éventuelles	
Cycle de vie des données	- Durées de conservation
- Critères de détermination	
- Processus d'archivage	
- Méthode de suppression	
Mesures de sécurité	- Contrôles techniques

- Mesures organisationnelles	
- Niveau de sécurité global	
Transferts hors UE	- Pays destinataires
- Garanties appropriées	
- Documentation des transferts	

- Nécessité d'une AIPD	
- Référence à l'AIPD réalisée	
- Résultat de l'analyse préliminaire	

Gestion et maintenance du registre

- Outil dédié : Solution GRC (Governance, Risk & Compliance) centralisée
- Processus de mise à jour : Révision annuelle et lors de tout changement significatif
- Responsabilités : DPO (propriétaire), Privacy Champions (contributeurs)
- Procédure d'ajout : Workflow de validation pour les nouveaux traitements
- Contrôle qualité : Audit périodique de complétude et d'exactitude
- Documentation complémentaire : Liens vers les documents associés (AIPD, contrats, etc.)

Intégration dans le processus de développement :

Tout nouveau projet ou évolution significative d'un service existant déclenche systématiquement une revue du registre des traitements:

- Phase d'initiation : Questionnaire préliminaire de traitement de données
- Phase de conception : Fiche de traitement détaillée et analyse de conformité
- Phase de validation : Intégration formelle au registre des traitements
- Phase de déploiement : Vérification finale de conformité
- Phase de revue : Contrôle post-implémentation après 3 mois

Analyses d'impact relatives à la protection des données (AIPD)

Processus d'évaluation préliminaire

Neo Financia a mis en place un processus systématique pour déterminer la nécessité d'une AIPD.

- Nature des données (sensibles, financières, à grande échelle)
- Portée du traitement (nombre de personnes, volume de données)
- Contexte du traitement (personnes vulnérables, usage innovant)
- Finalités du traitement (profilage, décisions automatisées)
- Technologies employées (IA, reconnaissance biométrique, loT)
- Présence dans les listes de l'autorité de contrôle
- Score élevé : AIPD obligatoire
- Score intermédiaire : Revue détaillée par le DPC
- Score faible : AIPD non requise (avec documentation)

Méthodologie des AIPD

Neo Financia utilise une méthodologie structurée pour la réalisation des AIPD, inspirée des recommandations de la CNIL et de l'ICO:

Étape	Activités	Livrables	Intervenants
Cadrage	- Description détaillée du traitement		
- Périmètre de l'analyse			
- Contexte du traitement			
- Identification des parties prenantes			
Document de cadrage validé	DPO, Métier, RSSI		
Évaluation de la nécessité et de la proportionnalité	- Analyse des finalités		
- Évaluation des bases légales			
- Minimisation des données			
- Qualité et exactitude			
- Durées de conservation			

Matrice de nécessité/proportionnalité	DPO, Métier, Juridique		
Identification des menaces et évaluation des risques	- Recensement des sources de risques		
- Identification des événements redoutés			
- Évaluation de la gravité			
- Évaluation de la vraisemblance			
- Détermination du niveau de risque			
Cartographie des risques	DPO, RSSI, Métier		
Mesures de traitement des risques	- Identification des mesures existantes		
- Évaluation de leur efficacité			
- Définition des mesures complémentaires			
- Réévaluation des risques résiduels			
Plan de traitement des risques	DPO, RSSI, Métier, IT		

|Validation et documentation|-
Formalisation du rapport AIPD

- Avis des personnes concernées ou représentants
- Validation par les responsables
- Consultation préalable si nécessaire

Rapport AIPD validé	**DPO, Direction métier, COMEX si risque élevé**		
Mise en œuvre et suivi	- Implémentation des mesures définies		

- Suivi du plan d'action
- Revue périodique de l'AIPD |Tableau de bord de suivi|DPO, RSSI, Métier|

Consultation préalable

Lorsqu'une AIPD révèle un risque résiduel élevé malgré les mesures prévues, Neo Financia met en œuvre la procédure de consultation préalable de l'autorité de contrôle :

1. Préparation du dossier complet incluant :
   - Rapport d'AIPD détaillé
   - Description des responsabilités (RT, ST, etc.)
   - Finalités et moyens du traitement
   - Mesures et garanties prévues
   - Coordonnées du DPO
2. Soumission à l'autorité compétente (CNIL ou ICO)
3. Suivi des échanges et demandes complémentaires
4. Adaptation du projet selon les recommandations reçues
5. Documentation des décisions prises

Le traitement n'est mis en œuvre qu'après réception de l'avis de l'autorité ou expiration du délai de huit semaines sans réponse.

Protection des données dès la conception et par défaut

Principes du Privacy by Design

Neo Financia intègre la protection des données dès la conception de ses services, produits et processus, en appliquant les principes suivants :

|Proactivité plutôt que réactivité|Anticipation et prévention des problèmes de vie privée avant qu'ils ne surviennent|-
Intégration du DPO dès la phase d'idéation

- Privacy Champions dans les équipes produit
- Checklist Privacy by Design en amont des projets | |---|---|---| |Protection par défaut|Les paramètres les plus protecteurs sont appliqués automatiquement|-
  Paramètres de confidentialité restrictifs par défaut
- Opt-in explicite pour les usages non essentiels
- Minimisation des données affichées/partagées | |Protection intégrée|La confidentialité fait partie intégrante de la conception|-
  Architecture technique orientée protection des données
- Documentation des choix de conception

- Sécurité et confidentialité indissociables | |Fonctionnalité complète|Somme positive et non compromis (gagnant-gagnant)|-
  Équilibre entre expérience utilisateur et protection
- Solutions innovantes conciliant les deux aspects
- Tests d'utilisabilité incluant la dimension privacy | |Sécurité de bout en bout|Protection tout au long du cycle de vie des données|-
  Chiffrement de bout en bout quand approprié
- Traçabilité complète des accès aux données
- Destruction sécurisée en fin de vie | |Visibilité et transparence|Ouverture sur les pratiques et processus|-
  Documentation claire et accessible
- Interfaces montrant l'utilisation des données |

		• Journal des accès consultable par l'utilisateur
Respect de la vie privée de l'utilisateur	L'intérêt de l'individu est central	• Contrôle effectif par l'utilisateur
• Feedback des utilisateurs intégré		
• Options de confidentialité granulaires		

Intégration dans le cycle de développement

La protection des données est intégrée à chaque étape du cycle de développement des produits et services

Phase	**Activités liées à la protection des données**	**Livrables**
Idéation	- Consultation précoce du DPO	
- Identification préliminaire des enjeux de données		
- Brainstorming sur les approches privacy-friendly		

Note d'orientation privacy		
Cahier des charges	- Définition des exigences de protection des données	
- Identification des données nécessaires		
- Questionnaire Privacy by Design complété		
Cahier des charges avec section privacy		
Conception	- Workshop privacy avec les parties prenantes	
- Data mapping détaillé		
- Évaluation préliminaire AIPD		
- Choix des technologies privacy-enhancing		
- Cartographie des flux de données		
- Spécifications privacy		
- AIPD si nécessaire		
Développement	- Application des design patterns privacy	
- Implémentation des contrôles techniques		
- Revue de code orientée privacy		
- Tests unitaires des fonctions de privacy		
- Code respectant les exigences		

- Documentation technique		
Test	- Tests spécifiques privacy	
- Validation des paramétrages par défaut		
Rapport de test privacy		

|Déploiement|-
Vérification pré-production

- Mise à jour du registre des traitements
- Validation finale du DPO
- Information des utilisateurs |-
  Certificat de conformité privacy
- Communication de lancement | |---|---|---| |-
  Vérification des notices d'information
- Test des mécanismes de consentement |-
  Vérification des notices d'information
- Test des mécanismes de consentement | |Maintenance|-
  Audits périodiques de conformité
- Surveillance des indicateurs privacy
- Mise à jour selon l'évolution réglementaire
- Gestion des demandes des personnes concernées |Rapport de surveillance continue|

Mesures techniques et organisationnelles

Neo Financia implémente un ensemble de mesures pour assurer la protection des données par conception et par défaut

Mesures techniques

- Pseudonymisation des données dès que possible
- Anonymisation pour les usages statistiques
- Chiffrement des données sensibles (transport et stockage)
- Cloisonnement logique des données
- Contrôles d'accès granulaires basés sur les rôles et le contexte
- Journalisation des accès et modifications

- Purge automatique des données à l'expiration des durées de conservation
- Protection contre l'extraction massive de données

Mesures organisationnelles

- Formation Privacy by Design des équipes produit et IT
- Processus de validation privacy intégré au workflow de développement
- Privacy Champions dans chaque équipe produit
- Revues périodiques des paramétrages de confidentialité
- Documentation des choix de conception liés à la privacy
- Tests d'intrusion spécifiques à la protection des données

Exemples de technologies privacy-enhancing déployées :

- Differential Privacy : Pour l'analyse des comportements sans identifier les individus
- Federated Learning : Pour les modèles prédictifs sans centraliser les données
- Secure Multi-Party Computation : Pour le partage sécurisé d'analyses avec des partenaires
- Zero-Knowledge Proofs : Pour la vérification sans révélation de données (ex: éligibilité crédit)

- Privacy-Preserving Record Linkage : Pour le matching client sans identifiants directs

Transferts de données hors UE

Cartographie des transferts

Neo Financia maintient une cartographie détaillée des transferts de données personnelles en dehors de l'UE/EEE

Pays destination	Type de données	Finalité du transfert	Base du transfert	Destinataire
Royaume-Uni	Données clients, transactions	Opérations de la filiale UK	Décision d'adéquation	Neo Financia UK
États-Unis	Données techniques limitées	Support technique, cloud services	CCT avec garanties supplémentaires	Fournisseurs SaaS et cloud
Suisse	Données KYC	Vérification d'identité	Décision d'adéquation	Prestataire verification
Inde	Données de support limités	Support niveau 2 (hors horaires)	CCT avec mesures techniques	Centre de support externe

Mécanismes de transfert

Neo Financia utilise plusieurs mécanismes pour encadrer juridiquement les transferts hors UE.

Mécanisme	Usage et mise en œuvre
Décisions d'adéquation	- Utilisé pour les transferts vers les pays reconnus (UK, Suisse, etc.)
- Veille sur l'évolution des décisions	
- Documentation des flux concernés	
Clauses Contractuelles Types (CCT)	- Modèles 2021 systématiquement implémentés
- Annexes complétées avec les détails des traitements	
- Inclusion dans tous les contrats pertinents	
- Processus de validation juridique	
Règles d'entreprise contraignantes (BCR)	- Non utilisées actuellement
---	
	- Évaluation en cours pour transferts groupe
---	---
Dérogations de l'article 49	- Utilisé exceptionnellement pour des cas spécifiques
- Documentation détaillée des circonstances	
- Approbation DPO obligatoire	
- Minimisation des données transférées	

Évaluations d'impact des transferts (TIA)

Suite à l'arrêt Schrems II, Neo Financia conduit des évaluations d'impact des transferts pour tout transfert hors UE ne bénéficiant pas d'une décision d'adéquation :

1. Analyse du transfert
   - Cartographie détaillée des données
   - Chaîne complète des sous-traitants
   - Modalités techniques du transferl
2. Évaluation du cadre juridique du pays tiers
   - Législation en matière d'accès gouvernemental
   - Pouvoirs des autorités de surveillance
   - Recours disponibles pour les personnes concernées
   - Utilisation des analyses EDPB et ressources externes
3. Évaluation des risques spécifiques
   - Sensibilité des données transférées
   - Volume et fréquence des transferts
   - Secteur d'activité et attractivité des données
   - Format des données (chiffrées, pseudonymisées)
4. Mesures supplémentaires
   - Techniques : chiffrement, pseudonymisation, fragmentation
   - Contractuelles : engagements de transparence, assistance juridique
   - Organisationnelles : processus de notification, audits
5. Conclusion documentée
   - Évaluation finale du niveau de protection
   - Justification des mesures retenues
   - Validation par le DPO et la Direction Juridique
   - Monitoring et revue périodique

Post-Brexit : attention particulière au Royaume-Uni

Bien que bénéficiant actuellement d'une décision d'adéquation, les transferts vers le Royaume-Uni font l'objet d'une vigilance spécifique :

- Veille renforcée sur l'évolution réglementaire UK
- Plan de contingence en cas de remise en cause de la décision d'adéquation

---

- Documentation détaillée des flux transfrontaliers
- Maintien de contrats avec CCT en complément (approche de précaution)
- Revue annuelle dédiée aux transferts UK/UE

Gestion des violations de données

Détection et qualification

Neo Financia a mis en place un dispositif complet pour détecter et qualifier les violations de données personnelles.

Sources de détection

- Alertes automatisées des systèmes de sécurité (DLP, SIEM, EDR)
- Signalements des collaborateurs via le canal dédié
- Remontées des clients ou partenaires
- Veille externe (dark web, forums)
- Alertes des autorités ou organismes de sécurité

Processus de qualification

- Analyse initiale par l'équipe de sécurité et le DPC
- Vérification de l'implication de données personnelles
- Évaluation préliminaire de la gravité
- Détermination du type de violation (confidentialité, intégrité, disponibilité)
- Documentation des éléments factuels

Gestion et notification

Une fois une violation de données personnelles confirmée, Neo Financia suit un processus structuré.

1. Confinement et remédiation

- Mesures immédiates pour limiter l'impact
- Préservation des preuves
- Actions correctives techniques

2. Évaluation d'impact

- Détermination de la nature et du périmètre exact
- Identification des données et personnes concernées
- Analyse des conséquences potentielles
- Évaluation des risques pour les droits et libertés des personnes

3. Décision de notification

- Analyse du seuil de risque (CNIL/ICO)
- Consultation de la Direction Juridique
- Validation par le RSSI et le DPO
- Information du Comité Exécutif pour les cas significatifs

4. Notification à l'autorité de contrôle (si requise)

- Préparation du dossier complet
- Soumission à la CNIL/ICO dans les 72h
- Compléments d'information si nécessaire
- Suivi des échanges avec l'autorité

---

5. Communication aux personnes concernées (si requise`

- Rédaction d'un message clair et transparent
- Validation par la Communication et le Juridique
- Mise en place des canaux de contact dédiés
- Suivi des réactions et questions

Critères d'évaluation du risque

Neo Financia utilise une matrice d'évaluation pour déterminer si une violation doit être notifiée :

Critère	Faible	Moyen	Élevé
Type de données	Données non sensibles, publiques	Données personnelles standard	Données sensibles, financières, d'identification
Volume	Quelques personnes	Groupe limité (<1000)	Volume important (>1000)
Facilité d'identification	Données anonymisées	Données pseudonymisées	Données directement identifiantes
Gravité des conséquences	Contrariété mineure	Impact limité mais réel	Préjudice significatif (financier, réputation)
Caractéristiques des personnes	Pas de vulnérabilité particulière	Vulnérabilité modérée	Personnes vulnérables
Niveau d'exposition	Accès interne limité	Accès externe limité	Accès large non contrôlé

La combinaison de ces facteurs détermine le niveau de risque global et donc les obligations de notification

- Risque faible : Documentation interne uniquement
- Risque moyen : Notification à l'autorité de contrôle
- Risque élevé : Notification à l'autorité et aux personnes concernées

Documentation et suivi

- Registre des violations : Documentation de toutes les violations, y compris celles non notifiées
- Dossier d'investigation : Conservation des preuves et analyses
- Plan de remédiation : Mesures correctives mises en place
- Retour d'expérience : Analyse des causes racines et enseignements
- Suivi des notifications : Traçabilité des échanges avec les autorités
- Revue périodique : Analyse des tendances et adaptation des contrôles

Coordination avec la gestion des incidents de sécurité

La gestion des violations de données s'intègre au processus plus large de gestion des incidents de sécurité.

- Équipe conjointe RSSI/DPO pour l'évaluation initiale
- Processus d'escalade harmonisé
- Double qualification (incident de sécurité / violation de données)
- Traitement coordonné des actions correctives

- Partage des leçons apprises entre les équipes

Mesures de sécurité spécifiques aux données personnelles

En complément des mesures de sécurité générales décrites dans la PSSI, Neo Financia applique des contrôles spécifiques pour les données personnelles :

Contrôles techniques

Catégorie	Mesures implémentées
Chiffrement	- Chiffrement des données sensibles au repos (AES-256)
- Chiffrement en transit systématique (TLS 1.3)	
- Gestion sécurisée des clés (HSM)	
- Chiffrement des sauvegardes	
Pseudonymisation	- Séparation des identifiants directs dans les tables
- Tokenisation des données sensibles	
- Hash pour les comparaisons sans accès direct	
- Données de test toujours pseudonymisées	
Contrôle d'accès	- Authentification forte pour les données personnelles
- Ségrégation des rôles et responsabilités	
- Accès aux données sensibles sur justification	
-	

Revue trimestrielle des accès aux données personnelles	
Journalisation et surveillance	- Traçabilité de tous les accès aux données personnelles
- Enregistrement des modifications et exports	
- Alertes sur les comportements anormaux (UEBA)	
- Surveillance dédiée aux données sensibles	

Protection des endpoints	- DLP sur les postes de travail
- Restriction des supports amovibles	
- Chiffrement des postes et mobiles	
- Limitations des téléchargements selon le contexte	
---	---
Architecture de données	- Minimisation des flux de données personnelles
- Segmentation des bases de données sensibles	
- Politique de réplication restrictive	
- Restrictions d'accès géographiques	

Contrôles organisationnels

Catégorie	Mesures implémentées

Procédures formalisées	- Procédures de gestion du cycle de vie des données
- Protocoles d'accès aux données sensibles	
- Processus de validation des extractions	
- Règles de partage interne et externe	
Formation et sensibilisation	- Programme spécifique pour les manipulateurs de données
- Formations avancées pour les équipes data	
- Certification obligatoire pour accès privilégiés	
- Sensibilisation ciblée par profil de risque	
Tests et audits	- Tests d'intrusion ciblés sur les systèmes de données personnelles
- Audits de conformité RGPD annuels	
- Vérification du respect des durées de conservation	
- Revue des mesures de sécurité par type de données	
Gestion des tiers	- Due diligence approfondie des sous-traitants
- Clauses contractuelles détaillées (art. 28 RGPD)	
-	

Audit des sous-traitants critiques	
- Limitation des accès aux données strictement nécessaires	
Surveillance continue	- Monitoring des flux de données personnelles
- Détection des données personnelles non déclarées	

- Surveillance de la conformité aux politiques	
- Alertes sur les anomalies de traitement	

Traitement des catégories particulières de données

Neo Financia applique des mesures renforcées pour les catégories particulières de données (données sensibles au sens de l'article 9 du RGPD):

- Données biométriques (utilisées pour l'authentification optionnelle)
- Stockage uniquement des modèles, jamais des données brutes
- Chiffrement renforcé avec clés individuelles
- Conservation sur le terminal utilisateur quand possible
- Alternative systématiquement proposée
- Consentement explicite documenté
- Données de santé (limitées aux informations d'assurance)
- Cloisonnement strict dans des bases spécifiques
- Accès nominal avec justification obligatoire
- Double validation pour tout export
- Chiffrement spécifique de bout en bout
- Données judiciaires (vérifications KYC)
- Accès restreint à l'équipe conformité
- Séparation des données dans un environnement sécurisé
- Conservation limitée à la durée légale obligatoire
- Journalisation renforcée de tous les accès

Conformité et amélioration continue

Programme d'audit

Neo Financia a mis en place un programme d'audit complet pour évaluer sa conformité en matière de protection des données:

Type d'audit	Périmètre	Fréquence	Responsable
Audit interne de conformité RGPD	Évaluation globale du dispositif de protection des données	Annuel	Audit interne avec DPO
Audit technique de sécurité des données	Tests des mesures techniques de protection	Semestriel	Équipe sécurité
Audit des sous-traitants	Évaluation des principaux sous-traitants	Annuel (par rotation)	DPO + Achats
Revue des droits d'accès	Vérification des habilitations aux données personnelles	Trimestriel	DSI + DPO

Audit externe	Évaluation indépendante par un cabinet spécialisé	Tous les 2 ans	Prestataire externe
Test de conformité métier	Vérification des pratiques par direction	Annuel (par rotation)	DPO + Privacy Champions

Indicateurs de performance (KPIs)

Neo Financia suit un ensemble d'indicateurs pour mesurer l'efficacité de son dispositif de protection des données

Catégorie	Indicateurs	Cible	Fréquence
Conformité	- Taux de complétion du registre des traitements		
- Taux de réalisation des AIPD requises			
- Pourcentage de recommandations d'audit mises en œuvre			
- 100%			
- 100%			
- ≥90%			
Trimestriel			

Droits des personnes	- Délai moyen de traitement des demandes		
- Taux de demandes traitées dans les délais			
- Taux de satisfaction des demandeurs			
- ≤ 15 jours			
- ≥ 95%			
- ≥ 90%			
Mensuel			
Formation	- Pourcentage d'employés formés		
- Score moyen aux tests de connaissance			
- Taux de participation aux rappels			
- 100%			
- ≥ 85/100			
- ≥ 95%			
Trimestriel			
Incidents	- Nombre de violations de données		
- Délai moyen de détection			
- Pourcentage de violations notifiées dans les délais			
-			

Baisse de 20% annuelle			
- ≤ 24h			
- 100%			
Mensuel			
Sous-traitants	- Pourcentage de sous-traitants évalués		
- Taux de conformité contractuelle			
- Score moyen d'évaluation des sous-traitants			
- 100% (critiques)			
- 100%			
- ≥ 80/100			
Trimestriel			

Plan d'amélioration continue

Neo Financia a défini un plan d'amélioration continue de son dispositif de protection des données pour 2025-2026

Axe	Actions prévues	Échéance
Automatisation	- Mise en place d'un outil de Data Discovery pour cartographie automatique	
- Automatisation de la purge des données en fin de conservation		
- Solution de traitement automatisé des demandes d'exercice des droits		
T4 2025		

Intégration dans le DevOps	- Intégration des tests de privacy dans la CI/CD	
- Création de bibliothèques privacy-by-design réutilisables		
- Automatisation des contrôles de conformité des applications		
T2 2025		
Formation avancée	- Programme de certification interne par niveau d'expertise	
- Parcours spécialisés par métier (data scientists, développeurs, etc.)		
- Exercices pratiques de simulation d'incidents		
T3 2025		
Gouvernance renforcée	- Mise en place d'un Privacy Council avec représentants métiers	
- Intégration des KPIs privacy dans les objectifs des managers		
- Création d'une cartographie dynamique des risques privacy		
T1 2025		
Technologies avancées	- Déploiement étendu des techniques de differential privacy	
- Implémentation de solutions de détection des données sensibles non structurées		
- Exploration de l'anonymisation basée sur la blockchain		

T4 2025		

Certifications visées

En complément de son programme d'amélioration continue, Neo Financia vise l'obtention des certifications suivantes:

- ISO 27701 (extension Privacy de l'ISO 27001) d'ici fin 2025
- Label CNIL Gouvernance RGPD pour le siège français en 2025
- Certification EDPB dès finalisation du référentiel européen
- Conformité certifiée DORA pour le volet protection des données en 2026
