Analyse des risques

Sodecaf

Table des matières

1. Étape 1 : Identification des Actifs

Les actifs représentent ce qui doit être protégé chez SODECAF dans le contexte du nouveau service Nextcloud.

1.1 Actifs Physiques

Actif	Description
Serveur Physique	Disque SSD pour l'OS + Nextcloud – Alimentations internes PSU (Power Supply Unit) risque de défaillance, usure.

1.2 Actifs Logiciels

Actif	Description
Nextcloud Core	Application collaborative principale – contient le code et la logique métier
Système d'exploitation, (machine virtuel)	Debian 12 (serveur) – noyau, drivers, services système
Système d'exploitation (Machine physique)	Windows Server 2025 - noyau, drivers, services système
Services web	Apache, PHP 8.1+, MariaDB – middleware applicatif
Clients de synchronisation	Clients Nextcloud desktop (Windows, macOS, Linux)

1.3 Actifs Informationnels (Données)

Actif	Description
Base de données NextCloud	Mots de passe, tokens, certificats, Logs d'accès, historiques de versioning
Données Utilisateurs	Paies, budgets, contrats fournisseurs, Répertoires, adresses email, téléphones, Noms, adresses, coordonnées de contact

1.4 Actifs Humains

Actif	Description
Administrateurs IT	Gestion technique, sécurité, maintenance du système
Collaborateurs SODECAF	Utilisateurs internes de l'outil Nextcloud
Clients externes	Accès aux espaces de dépôt et documents partagés

Direction / MOA	Pilotage, gouvernance, exigences métiers

1.5 Actifs Organisationnels

Actif	Description
Procédures de sécurité	Règles internes, gestion des accès, sécurité opérationnelle
Documentation technique	Architecture, configurations, guides d'exploitation
Sauvegardes	Backups système, données, bases de données
Plan de reprise	Procédures de continuité / PRA
Conformité légale	Respect RGPD, obligations comptables / fiscales

2. Étape 2 : Identification des Menaces

Pour chaque catégorie d'actifs, les menaces potentielles sont énumérées. Une menace représente un événement potentiellement dommageable.

2.1 Menaces Liées aux Données

N°	Menace	Description	Impact Potentiel
M1	Ransomware	Chiffrement des données clients/financières par malware	Indisponibilité, perte de données, rançon

M2	Fuite de données	Exfiltration de données comptables ou personnelles sensibles	Confidentialité compromise, violation RGPD
M3	Corruption de base de données	Altération de données comptables critiques	Intégrité compromise, incidents comptables
M4	Suppression accidentelle	Effacement involontaire de documents importants	Indisponibilité, perte irréversible
M5	Modification non autorisée	Altération frauduleuse de documents financiers	Intégrité compromise, fraude possible

2.2 Menaces Liées aux Accès

N°	Menace	Description	Impact Potentiel
M6	Attaque Man in the Middle (MITM)	Tentative d'espionnage sur les communications	Compromissions du secret professionnel
M7	Attaque par force brute	Tentative de deviner les mots de passe	Compromission de comptes utilisateurs
M8	Usurpation d'identité	Utilisation d'identifiants volés	Accès non autorisé, traçabilité compromise
M9	Élévation de privilèges	Passage d'un utilisateur standard à administrateur	Contrôle complet du système
M10	Accès clients externes non autorisés	Contournement des restrictions d'accès	Fuite de données, altération de documents

2.3 Menaces Liées à la Disponibilité

N°	Menace	Description	Impact Potentiel
M11	Panne ou défaillance matérielle	Défaillance disque SSD/HDD, Panne PSU du serveur	Indisponibilité service, perte de données, Arrêt serveur
M12	Débordement espace disque	Remplissage stockage, arrêt du service	Indisponibilité service, impossibilité d'upload
M13	Saturation base de données	Performance dégradée jusqu'à arrêt	Indisponibilité progressive

2.4 Menaces Liées à la Traçabilité

N°	Menace	Description	Impact Potentiel
M14	Suppression ou modification des logs	Effacement des journaux d'audit	Traçabilité perdue, preuves disparues
M15	Absence de monitoring	Pas de détection d'incident en temps réel	Incidents prolongés, impact maximisé

2.5 Menaces Opérationnelles

N°	Menace	Description	Impact Potentiel
M16	Erreur de configuration	Mauvais paramétrage sécurité, permissions, backups	Failles de sécurité, perte de données

3. Étape 3 : Identification des Vulnérabilités

Les vulnérabilités sont les faiblesses du système qui permettent aux menaces de se matérialiser.

3.1 Vulnérabilités Techniques – Logicielles

N°	Vulnérabilité	Menaces associées	Description
V1	Absence de mise à jour régulière Nextcloud	M1, M6, M7	Nextcloud non patché = CVE exploitables
V2	Absence de mise à jour OS / système	M1, M6, M7	Debian/Ubuntu non patchés = vulnérabilités kernel
V3	Mots de passe faibles	M7, M8	Absence de politique minimum (12+ caractères, complexité)
V4	Pas de 2FA/MFA	M7, M8, M9	Authentification simple = prise de contrôle facilitée
V5	Services inutiles activés	M1, M6	SSH, VNC, ports de debug actifs sans raison
V6	Pas de chiffrement des données au repos	M2, M4	Données lisibles en cas de vol disque
V7	Pas de chiffrement TLS 1.3	M2, M6	Communication HTTP non chiffrée
V8	Pas de limites de ressources (quotas)	M13	Pas de quota disque = débordement
V9	Pas de monitoring performances	M13	Pas d'alertes disque

V10	Pas de vérification d'intégrité	M3, M5	Pas de hash/checksum des données critiques

3.2 Vulnérabilités Techniques – Matérielles

N°	Vulnérabilité	Menaces associées	Description
V11	Alimentation serveur simple (pas redondante)	M11	Panne PSU = arrêt total du serveur
V12	Pas de monitoring matériel	M11, M12, M13, M14	Pas de prédiction panne (SMART, températures…)

3.3 Vulnérabilités Organisationnelles

N°	Vulnérabilité	Menaces associées	Description
V16	Absence de politique de gestion des accès	M10, M9	Pas de matrice des droits, permissions trop larges
V17	Pas de procédure de sauvegarde testée	M4, M11, M12	Sauvegardes non régulières ou restauration jamais testée
V18	Absence de plan de reprise d'activité	M11, M12	Aucune procédure sinistre = improvisation
V19	Manque de sensibilisation des utilisateurs	M1, M2, M4	Phishing, stockage de mots de passe, erreurs
V20	Absence de documentation technique	V1–V11	Mauvaise configuration = failles sécurité

V21	Absence de contrat de support technique	M1-M17	Incident = aucune assistance = résolution lente

3.4 Vulnérabilités Humaines

N°	Vulnérabilité	Menaces associées	Description
V22	Erreur humaine d'administration	M4, M17	Suppressions involontaires, mauvaise sauvegarde
V23	Négligence utilisateurs	M4, M2	Partages publics accidentels, mauvaise manipulation

4. Étape 4 : Les risques

4.2 Analyse Détaillée des Risques

ID	Actif	Menace	Prob.	Impact	Risque
R1	Données clients	Ransomware	3	4	12
R2	Données clients	Fuite données	3	5	15
R3	Données clients	Modification non autorisée	3	4	12
R4	Données financières	Suppression accidentelle	3	4	12
R5	Données financières	Corruption base de données	3	4	12
R6	Intégrité	Attaque MITM	3	4	12
R7	Accès utilisateurs	Attaque force brute	4	2	8
R8	Accès utilisateurs	Usurpation d'identité	4	2	8

R9	Accès administrateur	Élévation de privilèges	3	5	15
R10	Accès clients externes	Accès données sensibles	3	3	9
R11	Disponibilité	Panne disque SSD/HDD	3	4	12
R12	Disponibilité	Dégradation RAID	3	4	12
R13	Disponibilité	Panne CPU/RAM	2	3	6
R14	Disponibilité	Panne alimentation PSU	2	3	6
R15	Disponibilité	Débordement espace disque	4	2	8
R16	Disponibilité	Saturation base de données	2	2	4
R17	Traçabilité	Suppression logs d'audit	2	3	6
R18	Traçabilité	Absence monitoring	3	2	6
R19	Infrastructure	Erreur configuration	3	2	6

4.4 Matrice de Risque

Impact / Probabilité	Mineur	Significatif	Critique	Très critique	Catastrophique
Très probable	—	—	—	—	—
Probable	—	R7, R8, R15		—	—
Moyen	—	R18, R19	R10	R1, R3, R4, R5, R11, R12, R6	R2, R9
Rare	—	R16	R13, R14, R17	—	—
Très rare	—	—	—	—	—

5. Étape 5 : Traitement des Risques

5.1 CRITIQUES (R2, R6)

R2 - Fuite données clients

Mesures :

1. 2FA TOTP obligatoire (mot de passe + code téléphone)
2. Chiffrer données sensibles (illisibles sans clé)
3. Limiter accès par client (Client A voit uniquement ses données)
4. Enregistrer tout accès aux données + alertes quotidiennes
5. Procédure notification légale si fuite (48h max)
6. Certificat SSL (HTTPS)

R9 - Admin non autorisé

Mesures :

1. SSH keys + 2FA TOTP pour tout accès admin
2. Enregistrer TOUTE action admin
3. Limiter droits admin (accès justifié uniquement)

5.2 TRÈS URGENTS (R1, R3, R4, R5, R11, R12)

R1 - Ransomware

Mesures :

1. Sauvegardes 3-2-1 (3 copies / 2 supports différents / 1 hors-site)
2. Test restauration mensuel (vérifier que ça marche)
3. Verifier et Mises à jour quotidiennes Nextcloud + OS
4. Détection malware (EDR Incident Detection and Response) everywhere
5. 2FA + limites tentatives (5 = verrouillage 30 min)

R3, R4, R5 - Modification/Suppression/Corruption données

Mesures :

1. Versioning : garder 5+ versions anciennes (récupération facile)
2. Enregistrer qui modifie/supprime quoi (logs complets)
3. Sauvegardes régulières testées (restore possible)

R11, R12 - Pannes disques

Mesures :

1. RAID 10 ou RAID 5 (redondance : si 1 panne → données sauves)
2. Monitoring SMART quotidien (prévoir les pannes avant qu'elles arrivent)
3. Alertes disque dégradé (intervention immédiate)
4. Sauvegardes testées régulièrement

5.3 URGENTS (R7, R8, R10, R15)

R7, R8 - Attaques mots de passe + Vol identité

Mesures :

1. 2FA obligatoire
2. Limiter tentatives : 5 mots de passe faux = verrouillage 30 min (Fail2ban)
3. Politique mots de passe fort (12+ caractères)
4. Enregistrer connexions + alertes si anomalies (autre pays, heure étrange)

R10 - Accès client externe non autorisé

Mesures :

1. Limiter accès par client (Client A = ses données uniquement)
2. Accès lecture seule pour clients (voir/télécharger, pas modifier)
3. Enregistrer tous les accès clients
4. Chiffrement des données au repos (chiffrement symétrique)

R15 - Débordement espace disque

Mesures :

1. Quotas par utilisateur (50 Go interne / 10 Go client)
2. Alertes si 80% plein
3. Cleanup automatique fichiers temporaires

5.4 MOYEN (R13, R14, R17, R18, R16)

Mesures communes :

1. Monitoring SMART/température disques
2. Alertes seuils (CPU, RAM, disque)
3. Logs avec révision régulière
4. Documentation + checklists config

5.5 FAIBLE (R6, R16)

Mesures :

1. Surveillance régulière
2. Alertes basiques