

**Préparation aux cyberattaques et continuité  
des services – De la stratégie de résilience du  
système d'information à la sauvegarde des  
actifs informationnels en bibliothèques  
académiques**

Travail de Bachelor réalisé par :  
**Stephen VALOT**

Sous la direction de :  
**Arnaud GAUDINAT, professeur HES**

**Genève, le 21 juillet 2025**

**Information Science  
Haute École de Gestion de Genève (HEG-GE)**

## Déclaration

Ce Travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor of Science HES-SO en Information Science.

L'étudiant atteste avoir soumis son travail à un logiciel de détection de plagiat. Il accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le Travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au Travail de Bachelor, du juré et de la HEG.

Ce mémoire a bénéficié d'une assistance partielle via ChatGPT 4-o pour la structure, la syntaxe et l'orthographe. Certains traitements ont été réalisés localement avec le modèle Mistral 7B (Ollama), afin de respecter la souveraineté des données.

« J'atteste que le présent travail a été réalisé en utilisant uniquement les sources citées dans la bibliographie, qu'il est le fruit de ma réflexion personnelle et a été rédigé de manière autonome. »

Fait à Genève, le 21 juillet 2025

Stephen VALOT

## **Remerciements**

Je tiens à exprimer ma gratitude à tous les professionnels qui ont accepté de partager leurs expériences. Leur disponibilité, la richesse et la clarté de leurs expertises ont largement contribué à approfondir mes réflexions. Leur apport a été déterminant dans l'élaboration de ce mémoire, que j'espère utile et porteur de perspectives concrètes pour l'enrichissement des pratiques professionnelles au sein des institutions engagées, ou appelées à s'engager, dans ces démarches. J'adresse également mes sincères remerciements à mon mandant, pour sa confiance, sa disponibilité et la qualité de son accompagnement tout au long de ce projet.

Je remercie tout particulièrement celles et ceux qui m'ont transmis leurs avis et leurs retours pour ce travail mais également durant la formation. Par la justesse de leurs remarques, la rigueur de leurs relectures et la pertinence de leurs observations, ils ont largement contribué à renforcer la cohérence et la portée de ce travail.

Leur implication a apporté à mon parcours une profondeur humaine et intellectuelle dont je mesure pleinement la valeur.

## Résumé

Les bibliothèques des hautes écoles font face à des risques graduels liés à l'informatisation des services, à l'interconnexion et une dépendance accrue envers les prestataires externes. Les ressources électroniques représentent une part majoritaire des budgets d'acquisition, mais les moyens alloués à leur sécurisation demeurent insuffisants. Ce contexte laisse craindre des interruptions de services, exacerbées par l'augmentation des cas de cyberattaques. Ce travail de Bachelor développe une démarche de sécurité centrée sur la Bibliothèque de l'Université de Genève, dans une approche théorique et pratique. Bien que l'infrastructure soit intégrée au périmètre de cybersécurité de l'université, et que des dispositifs de reprise d'activité existent à l'échelle institutionnelle, un cloisonnement persiste. Les collections électroniques acquises auprès des éditeurs sous forme de licence d'accès et les outils indispensables à leur gestion, restent souvent mal identifiés, avec une visibilité limitée sur leur criticité et leur dépendance opérationnelle. Ces éléments justifient la mise en place d'un plan de continuité d'activité.

Les causes sont multiples, d'une organisation segmentée entre services, à l'absence de politiques en matière d'archivage de ces ressources. On relèvera la complexité des systèmes, souvent marqués par des dépendances opaques dont les risques sont sous-évalués. Sans une stratégie adaptée de prévention et de réponse, appuyée par des outils et des mesures de protection appropriés, le patrimoine scientifique est exposé à un risque réel de pertes irréversibles, ainsi qu'à des coûts de reconstruction bien supérieure à ceux d'une préparation anticipée. Basée sur une revue de la littérature, des études de cas et des entretiens internes et externes ce travail permet d'établir un état des lieux et d'identifier les écarts à l'aide d'une matrice de maturité. Elle constituera le socle d'une analyse des risques pesant sur les processus et composantes du système d'information en conformité avec les normes et les référentiels sectoriels. L'analyse vise à identifier les actifs et les dépendances critiques, les niveaux de sensibilité et d'impacts, ainsi que les mesures de sauvegarde envisageables, tant pour les données brutes, les métadonnées du catalogue, que pour le système intégré de gestion de bibliothèque. Il sera question d'apporter une réflexion sur la curation des ressources à préserver et à archiver de manière pérenne et d'élaborer un plan de continuité d'activité adapté aux besoins et aux spécificités des bibliothèques académiques. Les résultats confirment l'intensification des cybermenaces sur un patrimoine numérique sous-sécurisé, une maturité contrastée, ainsi qu'une forte dépendance aux prestataires externes due en partie à des clauses contractuelles lacunaires. Ils conduisent à des recommandations de stratégies croisées entre archivage et cybersécurité, la formalisation des plans de continuité, et de solutions opérationnelles d'accès alternatif au sein d'une culture de sécurité partagée.

Ces éléments serviront à définir des accès alternatifs en cas de crise, dans l'hypothèse où les scénarios de crise envisagés viendraient à se concrétiser. Cela suppose de repenser la gestion des ressources numériques en contexte d'urgence. Cette démarche coordonne les dispositifs existants afin d'aboutir un plan d'urgence des collections numériques. Centré sur les ressources scientifiques, ce travail se veut aussi plus large et adaptable à l'ensemble des institutions du savoir. Il entend offrir un cadre théorique utile à la préparation de réponses face à des événements de nature variée, susceptibles d'affecter les systèmes d'information, mais plus fondamentalement, la préservation et l'accès à la connaissance.

**Mots-clés :** Bibliothèques académiques - Ingénierie des systèmes d'information - Cybersécurité - Plan de continuité d'activité - Gestion des risques - Actifs informationnels - Archivage numérique - Bibliothèques numériques - Ressources électroniques - Conservation du patrimoine numérique - Plan de sauvegarde des collections numériques - Gouvernance et gestion du cycle de vie des données.

## Liste des abréviations

- ANSSI :** Agence Nationale de la Sécurité des Systèmes d'Information
- BIA :** Business Impact Analysis ou analyse d'impact sur les activités.
- CERT :** Computer Emergency Response Team. Équipe de réponse aux incidents de sécurité informatique, parfois CSIRT.
- CLOCKSS :** Controlled LOCKSS. Variante de LOCKSS avec gouvernance partagée.
- CVE :** Common Vulnerability Enumeration. Référentiel standardisé des vulnérabilités.
- CVSS :** Common Vulnerability Scoring System. Système de notation pour évaluer la gravité technique des vulnérabilités.
- DDoS :** Distributed Denial of Service. Attaque par déni de service distribué, submersion de serveurs par un grand nombre de requêtes.
- DiSTIC :** Division du Système et des Technologies de l'Information et de la Communication.
- DLP :** Data Loss Prevention. Prévention. Technologies et stratégies visant à éviter la fuite, la suppression ou le transfert non autorisé de données.
- E BIOS :** Expression des Besoins et Identification des Objectifs de Sécurité
- EDR :** Endpoint Detection and Response.
- IAM :** Identity and Access Management. Gestion des identités et des accès.
- IDS/IPS :** Intrusion Detection/Prevention System : Systèmes de détection et de prévention des intrusions dans les réseaux informatiques.
- LOCKSS :** Lots of Copies Keep Stuff Safe. Logiciel open source pour la préservation numérique distribuée.
- NIST :** National Institute of Standards and Technology). Institut national des standards et de la technologie (USA).
- OAI-PMH :** Open Archives Initiative - Protocol for Metadata Harvesting. Protocole standardisé pour l'échange de métadonnées entre entrepôts numériques.
- OAIS:** Open Archival Information System. Modèle de référence pour l'archivage pérenne de l'information numérique.
- OFCS :** Office fédéral de la cybersécurité. Autorité fédérale suisse chargée de la coordination et de la protection contre les cybermenaces.
- PAM :** Privileged Access Management. Gestion des accès privilégiés aux systèmes sensibles.
- PCA/BCP :** Plan de Continuité d'Activité ou Business Continuity Plan. Planification des mesures à prendre pour maintenir les activités critiques en cas de crise.

- PRA/DRP :** Plan de Reprise d'Activité ou Disaster Recovery Plan. Ensemble des procédures de rétablissement des systèmes après un incident majeur.
- RPO :** Recovery Point Objective. Perte de données maximale tolérable exprimée en durée, entre deux sauvegardes.
- RSSI :** Responsable de la sécurité des systèmes d'information.
- RTO :** Recovery Time Objective. Temps maximal acceptable pour rétablir un service ou un système après un incident.
- SafePLN :** Private LOCKSS Network. Réseau privé de préservation numérique basé sur le logiciel open source LOCKSS.
- SIEM :** Security Information and Event Management. Gestion des informations et des événements de sécurité.
- SIGB :** Système Intégré de Gestion de Bibliothèque. Logiciel centralisant la gestion des services de bibliothèque.
- SLA :** Service Level Agreement ou Accord de niveau de service. Contrat définissant les engagements entre fournisseur et client.
- SMSI :** Système de Management de la Sécurité de l'Information. Cadre de gestion visant à protéger les actifs informationnels d'une organisation.
- SOC :** Security Operations Center. Centre opérationnel de sécurité chargé de surveiller, détecter, analyser et répondre aux incidents de sécurité informatique.
- TTP :** Tactics, Techniques, and Procedures. Tactiques, techniques et procédures utilisées par les attaquants.

# Table des matières

Déclaration .....	i
Remerciements .....	ii
Résumé .....	iii
Liste des abréviations .....	v
Liste des tableaux.....	x
Liste des figures .....	xi
1. Introduction .....	1
1.1 Contexte et justification de la recherche .....	2
1.2 Problématique et questions de recherche.....	3
1.3 Hypothèses de recherche .....	4
1.4 Objectifs .....	5
2. Méthodologie .....	6
2.1 Définition des concepts.....	6
2.2 Recherche documentaire .....	9
2.3 Collecte des données qualitatives .....	10
2.4 Utilisation de données quantitatives.....	11
2.5 Analyses et interprétation des résultats.....	11
2.5.1 Synthèse des entretiens sur les pratiques .....	11
2.5.2 Résultats intermédiaires .....	12
3. Exposition, menaces et vulnérabilités en bibliothèque.....	13
3.1 État des lieux d'un contexte spécifique .....	13
3.2 Études de cas concrets d'attaques .....	15
3.3 Une typologie des menaces .....	16
3.3.1 Menaces externes, <i>ransomware</i> et attaques logiques.....	16
3.3.2 Menaces internes, erreurs humaines et négligences .....	19
3.3.3 Vulnérabilités liées aux dépendances à des services tiers .....	20
3.3.4 Vulnérabilités liées aux dépendances aux éditeurs scientifiques .....	24
3.3.5 Instabilités liées aux évolutions technologiques et géopolitiques .....	26
3.3.6 Dynamiques émergentes et déplacement de la menace .....	28
3.4 Stratégies de cybersécurité à l'échelle institutionnelle .....	31
3.5 Évaluation de la résilience informationnelle .....	33
4. Analyse du système d'information de la bibliothèque .....	36
4.1 Définition et périmètre des actifs en bibliothèque .....	36
4.2 Architecture générale du SI .....	37
4.3 Cartographie des flux de données .....	39
4.4 L'environnement applicatif de gestion.....	40
4.5 Intégration des ressources électroniques dans les actifs .....	42

<b>4.6 Actifs informationnels .....</b>	<b>43</b>
4.6.1 Identification des actifs.....	43
4.6.2 Catégorisation des actifs.....	45
4.6.3 Priorisation des actifs .....	46
4.6.4 Protection des actifs.....	49
<b>5. Gestion des risques et gouvernance de l'information .....</b>	<b>53</b>
<b>5.1 Appréciation des risques .....</b>	<b>53</b>
5.1.1 Identification des risques .....	54
5.1.2 Analyse des risques .....	56
5.1.3 Évaluation des risques .....	57
5.1.4 Traitement des risques .....	58
<b>5.2 Cartographies.....</b>	<b>59</b>
5.2.1 Une approche par l'analyse des processus .....	59
5.2.2 Une approche par la conformité.....	60
5.2.3 Lecture croisée par typologie et criticité.....	62
5.2.4 Les risques prioritaires .....	62
<b>5.3 Modèles et leviers de gouvernance.....</b>	<b>64</b>
5.3.1 Appuis institutionnels .....	64
5.3.2 Le cadre légal .....	65
5.3.3 La question du coût et la notion de confiance.....	66
5.3.4 Gestion data-centrée des collections électroniques .....	67
5.3.5 Une mutualisation des efforts pour des objectifs communs.....	69
<b>6. Plan de sauvegarde des collections électroniques .....</b>	<b>70</b>
<b>6.1 Extraction des données .....</b>	<b>70</b>
<b>6.2 Une protection contractuelle des ressources électroniques.....</b>	<b>72</b>
<b>6.3 Stratégie de sauvegarde et de préservation des actifs .....</b>	<b>74</b>
6.3.1 Niveau 1 – Stockage opérationnel .....	75
6.3.2 Niveau 2 - Sauvegarde consolidée .....	75
6.3.3 Niveau 3 - Archivage pérenne .....	76
<b>6.4 Stratégie d'accès dégradé aux données préservées.....</b>	<b>77</b>
6.4.1 Niveau A - Accès permanent, local .....	77
6.4.2 Niveau B - Accès permanent, réseau interne .....	78
6.4.3 Niveau C - Accès permanent, redondance sur site de secours.....	79
<b>6.5 La continuité d'activité .....</b>	<b>80</b>
6.5.1 Alignement du plan de continuité et de reprise d'activité .....	81
6.5.2 Mise en œuvre du plan de continuité d'activité, la gestion de crise .....	82
6.5.3 Remédiation et analyse post incident .....	85
<b>7. Évaluation, formation et amélioration continue .....</b>	<b>86</b>
<b>7.1 Stratégie de cyber défense pour les bibliothèques .....</b>	<b>86</b>
<b>7.2 Scénarios d'attaques .....</b>	<b>87</b>
<b>7.3 Système de management de la sécurité de l'information .....</b>	<b>88</b>

<b>7.4 Sensibilisation et formation du personnel</b> .....	<b>89</b>
<b>8. Discussion, évaluation, recommandations .....</b>	<b>90</b>
<b>8.1 Recommandations stratégiques et résilience opérationnelle .....</b>	<b>90</b>
<b>8.2 Analyse critique des résultats .....</b>	<b>91</b>
<b>8.3 Perspectives et discussion .....</b>	<b>92</b>
<b>9. Conclusion.....</b>	<b>96</b>
<b>Bibliographie .....</b>	<b>97</b>
<b>Annexe 1 : Registre des normes applicables.....</b>	<b>112</b>
<b>Annexe 2 : Questionnaire d'entretien semi-dirigée .....</b>	<b>114</b>
<b>Annexe 3 : Liste des personnes interrogées .....</b>	<b>115</b>
<b>Annexe 4 : Grille de traitement des résultats.....</b>	<b>116</b>
<b>Annexe 5 : Grille de synthèse de lecture .....</b>	<b>117</b>
<b>Annexe 6 : Synthèse des entretiens sur les pratiques externes.....</b>	<b>118</b>
<b>Annexe 7 : Synthèse des entretiens sur les pratiques internes.....</b>	<b>120</b>
<b>Annexe 8 : Étude de cas concrets d'attaques.....</b>	<b>124</b>
<b>Annexe 9 : Matrice de maturité RAMSID.....</b>	<b>134</b>
<b>Annexe 10 : Registre des groupes d'actifs .....</b>	<b>137</b>
<b>Annexe 11 : Cartographie des processus .....</b>	<b>138</b>
<b>Annexe 12 : Cartographie du SI de l'UNIGE .....</b>	<b>140</b>
<b>Annexe 13 : La définition d'une collection essentielle.....</b>	<b>141</b>
<b>Annexe 14 : Critères de priorisation des ressources électroniques ...</b>	<b>144</b>
<b>Annexe 15 : Analyse d'impacts métiers .....</b>	<b>145</b>
<b>Annexe 16 : Cartographie des risques .....</b>	<b>147</b>
<b>Annexe 17 : Synthèse des risques prioritaires .....</b>	<b>158</b>
<b>Annexe 18 : Schéma de données du réplica .....</b>	<b>159</b>
<b>Annexe 19 : Modélisation complète .....</b>	<b>161</b>
<b>Annexe 20 : Gestion de crise cyber .....</b>	<b>164</b>
<b>Annexe 21 : Fiche d'urgence, attaque par Ransomware .....</b>	<b>167</b>
<b>Annexe 22 : Scénarios de crise .....</b>	<b>171</b>
<b>Annexe 23 : Scénarios combinés et seuils d'alerte.....</b>	<b>173</b>
<b>Annexe 24 : Synthèse des livrables .....</b>	<b>174</b>

## Liste des tableaux

Tableau 1 - Sauvegarde et Archivage .....	9
Tableau 2 - Typologie des menaces et vulnérabilités des systèmes de préservation.....	26
Tableau 3 - Registre des groupes d'actifs informationnels.....	43
Tableau 4 - Critères de classification de l'information et des données.....	46
Tableau 5 - Méthode de priorisation des ressources électroniques .....	48
Tableau 6 - Niveaux d'impact sur l'organisation .....	56
Tableau 7 - Exemple de processus critique identifié .....	60
Tableau 8 - Échelle de criticité des risques .....	62
Tableau 9 - Matrices de criticité des risques bruts et nets .....	63
Tableau 10 - Niveau de mobilisation et évaluation d'impacts en cas de crise .....	84
Tableau 11 - Proposition d'un SOC open source .....	87
Tableau 12 - <i>Cyber kill chain</i> de l'attaque sur la British Library .....	125

# Liste des figures

Figure 1 - Organigramme UNIGE et entretiens réalisés en interne.....	10
Figure 2 - Dynamique entre menaces, vulnérabilités et risques.....	13
Figure 3 - Cycle de vie d'un <i>ransomware</i> .....	18
Figure 4 - Responsabilité selon la configuration du service en nuage .....	23
Figure 5 - Projection des tendances d'attaques informatiques.....	28
Figure 6 - Évènements sur le réseau de l'UNIGE sur une période d'un mois .....	31
Figure 7 - Score de posture de sécurité de l'UNIGE et d'institutions similaires.....	32
Figure 8 - Résultats graphique de la matrice de maturité.....	34
Figure 9 - Cartographie du SI de la bibliothèque de l'UNIGE .....	38
Figure 10 - Flux de données de la Bibliothèque de l'UNIGE (2025).....	39
Figure 11 - Exemple de cas d'usage des résultats du processus de catégorisation.....	45
Figure 12 - Les composantes de l'accès pérenne des ressources électroniques .....	50
Figure 13 - Concepts et propriétés de solutions d'archives.....	51
Figure 14 - Processus de gestion des risques ISO 27005 .....	53
Figure 15 - Pourquoi préserver les ressources électroniques .....	69
Figure 16 - Cycle d'extraction du catalogue .....	71
Figure 17 - Modélisation de la stratégie de sauvegarde – Sauvegarde pérenne .....	74
Figure 18 - Mise à disposition des données sauvegardées – Accès perpétuel.....	77
Figure 19 - Chronologie, dispositifs de continuité et jalons d'un incident critique .....	81
Figure 20 - Gestion de crise et chaîne de décisions.....	83
Figure 21 - Répartition du stockage du système Safe-PLN .....	143

Dans *La Bibliothèque de Babel*, Borges imagine une bibliothèque infinie contenant tous les livres possibles, où l'exaltation du savoir cède à une détresse abyssale face à l'impossibilité de s'y orienter. Cette vision trouve un écho troublant dans la cyberattaque ayant paralysé la British Library, transformant un espace de savoir universel en un labyrinthe muet, la matérialisation d'un paradoxe borgésien. L'intégralité de la connaissance est disponible, mais plus rien n'est accessible (Knight 2023).

# 1. Introduction

La rédaction de ce mémoire s'inscrit dans une nouvelle dimension de notre ère, que l'on désigne comme l'âge de l'information et dont les frontières sont sans cesse remises en question. L'informatisation massive de la société a transformé en profondeur nos modes de vie, nos institutions et nos accès à la connaissance. Le cyberspace est devenu un environnement technologique omniprésent, où se mêlent promesses de progrès et risques systémiques. Tandis que les institutions du savoir dont les bibliothèques opèrent désormais dans ce monde hyperconnecté, elles se trouvent exposées à des menaces multiples : cybercriminalité, dépendances techniques, et perte de contrôle sur leurs infrastructures. L'intrication croissante entre numérique et physique transforme les perturbations en répercussions concrètes sur les services, les usages et les missions institutionnelles. Ces évolutions continues appellent à une vigilance accrue face aux dynamiques entropiques des systèmes d'informations, et une réflexion urgente sur la souveraineté et la résilience informationnelle.

Dans le climat d'incertitude économique, politique et écologique, les bibliothèques académiques perpétuent leur mission essentielle de diffusion du savoir et de préservation, et apparaît la nécessité de devenir des bastions de résilience face aux menaces qui se multiplient. Ces institutions doivent désormais tirer parti des technologies mêmes qui les exposent, intelligence artificielle, cryptographie et cybersécurité, pour s'approprier les outils et les systèmes de protection pour la continuité d'accès à leurs collections dématérialisées. Cette dualité de la technologie, à la fois vecteur de vulnérabilité et solution défensive, redéfinit leurs stratégies de sauvegarde et de conservation du patrimoine. Leur engagement envers l'accès fiable à une information scientifique neutre et probante devient ainsi un impératif académique mais également sociétal, pour garantir la pérennité de la mémoire collective. La préservation des collections numériques prend toute son importance lorsque leur disparition, souvent irréversible, devient une réalité. La prétendue immuabilité d'Internet s'effrite devant les dépendances technologiques, pannes et autres coupures de service. Depuis 2022, une recrudescence d'événements critiques affecte le patrimoine scientifique et les infrastructures académiques. Dans ce contexte, la question n'est plus de savoir si une cyberattaque surviendra, mais quand elle frappera et si nos institutions seront aptes et préparées à protéger, résister et préserver le capital informationnel qu'elles abritent. Seront-elles toujours en capacité d'assurer la transmission de ces données à travers le temps et l'espace et peuvent-elles mobiliser leur héritage de protection des biens culturels matériels pour en étendre les principes aux nouveaux médias de l'information.

Si la cybersécurité semble parfois exploiter les craintes collectives, ce mémoire s'ancre résolument dans une perspective de solutions concrètes et d'optimisme raisonné. Les vulnérabilités spécifiques aux bibliothèques seront examinées, en requalifiant les ressources numériques comme actifs informationnels. À l'aide d'une adaptation des normes de sécurité contemporaines, un diagnostic des infrastructures existantes pourra être établi pour concevoir des systèmes résilients face aux menaces identifiées et aux risques quantifiables. Si la numérisation renforce la conservation et l'accès au patrimoine scientifique, elle introduit également de nouvelles vulnérabilités. La recherche examine dans quelle mesure les bibliothèques, en tant que fondation centrale de la diffusion du savoir, doivent être considérées comme des infrastructures critiques.

## 1.1 Contexte et justification de la recherche

Les bibliothèques académiques dépendent aujourd’hui massivement des infrastructures numériques et des services cloud pour la gestion, la diffusion et l'accès à leurs collections. La transition d'un modèle d'achat à un modèle de licence d'accès imposé par les éditeurs a également renforcer cette dépendance (Metrat, Oury 2017). Si cette transition a facilité l'élargissement rapide des collections, tout en conservant un niveau d'accessibilité et de gestion documentaire acceptable, elle a également exposé les institutions à de nouvelles vulnérabilités, aux cyberattaques, aux pannes techniques et aux interruptions de service (Ngwum et al. 2020). Les missions de recherche, d'enseignement et de service à la cité se trouve menacées. L'externalisation des infrastructures et la dépendance accrue à des prestataires tiers exposent les bibliothèques aux incidents affectant leurs systèmes d'information (Bellini, Tammaro 2024). L'accès continu aux contenus essentiels aux missions de recherche, d'enseignement et d'apprentissage repose désormais sur des mesures de sécurité contractuelles et techniques, proactives et réactives (Ghernaouti 2022).

Les attaques récentes contre des institutions de renom, telles que la British Library, la Toronto Public Library et l'Internet Archive, ont révélé les limites des dispositifs existants de protection et de continuité numérique (Breeding 2024). Ces incidents ont paralysé l'accès aux collections, interrompu les services et mis en péril la disponibilité, l'intégrité et la confidentialité des données. Au-delà de ces atteintes ils entraînent des coûts de remédiation particulièrement élevés, tant en termes de mobilisation des ressources humaines que d'investissements financiers pour le rétablissement des services (Lindström, Spirkina 2024). Ces exemples démontrent qu'avoir des sauvegardes régulières est essentiel mais ne suffit pas : c'est l'ensemble du système d'information qui doit être sécurisé et conçu pour une reprise rapide après un événement critique (Kahn 2004). Il est nécessaire d'approfondir notre compréhension des mécanismes de protection des bibliothèques et des archives numériques et leurs rôles essentiels dans la préservation d'une culture en perpétuelle disparition (Messarra, Freeland, Ziskina 2024). C'est dans ce contexte que le projet tend à développer un cadre opérationnel de résilience pour la Bibliothèque de l'Université de Genève, aussi bien pour permettre d'évaluer sa posture de sécurité, de déterminer et qualifier les ressources prioritaires, d'assurer un accès pérenne à ces données et d'assumer une continuité de service au travers d'outils de gestion résilients et de solutions alternatives.

Ce travail est réalisé pour la Coordination de la Division de l'Information Scientifique (CoDIS) de l'Université de Genève (UNIGE), qui harmonise les pratiques entre les différents sites de la Bibliothèque et assure la gouvernance des ressources scientifiques et pédagogiques. L'UNIGE, comme de nombreuses institutions académiques, possède un patrimoine documentaire largement dématérialisé, avec une part croissante de son budget dédiée aux collections électroniques (Alexandre 2014). Aujourd'hui, plus de 85 % des acquisitions (UNIGE 2025a) concernent des ressources électroniques, ce qui atteste de l'importance stratégique de ces ressources, que l'on peut considérer comme les actifs informationnels de l'organisation. Cependant, l'absence de plan d'urgence pour ces ressources et de plan de continuité d'activité les exposent à des risques d'indisponibilité en cas de cyberattaque, de panne critique ou de défaillance d'un prestataire externe. Aucun dispositif de reprise d'activité ne garantit, l'accès aux catalogues, au SIGB ou aux bases de données institutionnelles en cas d'incident majeur (Kederlhüé, Iriarte, 2023). Contrairement aux collections physiques, couvertes par des plans

de sauvetage (DIS 2025), la protection et la récupération des collections numériques restent largement sous-évaluées.

Il est urgent de développer une stratégie de résilience numérique, fondée sur la continuité des services et la protection des actifs numériques. Cette démarche doit s'inscrire dans le respect des standards minimaux de l'Office Fédérale de la Cybersécurité (OFCS) (DDPS 2023), et des exigences de la Directive générale de gestion de la continuité des services numériques de l'UNIGE (UNIGE 2021a; 2021b). Elle constitue également une étape préparatoire à la mise en œuvre de la politique générale de gestion du cycle de vie des données portée par le *Data Office*. Enfin, l'analyse des retours d'expérience d'institutions ayant subi des incidents majeurs permet d'identifier des bonnes pratiques et d'anticiper les vulnérabilités, contribuant ainsi à renforcer la résilience globale du système d'information académique. Le mémoire vise donc à répondre à ce besoin identifié par le service comme critique. Il s'inscrit dans une logique d'adaptabilité, afin que les solutions proposées puissent être mises en œuvre sur les différents sites de la Bibliothèque de l'Université de Genève, mais également dans d'autres institutions confrontées à des défis similaires.

L'étude s'inscrit dans la stratégie 2024-2027 de la Bibliothèques de l'UNIGE en s'appuyant sur l'axe 4, pour un soutien renforcé à la science ouverte et vise les mesures de développement prévus dans l'axe 6 pour un pilotage avisé (UNIGE 2024). En juin dernier, l'Université a dévoilé la stratégie numérique 2025 - 2028, dont l'une des priorités est de renforcer sa résilience face aux risques informatiques. Elle s'engage à anticiper et atténuer les menaces pour protéger les données sensibles et garantir la continuité des activités, en adoptant une approche « *secure by design* » en se dotant de plans de réponse en cas de cyberattaque (UNIGE 2025b). À l'heure de la transformation numérique, les bibliothèques jouent un rôle fondamental dans la conservation, la transmission et la mise à disposition des connaissances. Intégrées dans des systèmes complexes mêlant dimensions humaines, technologiques et organisationnelles, elles sont devenues des infrastructures critiques à protéger au même titre que les secteurs de l'énergie, de la santé ou des transports (Conseil Fédéral 2024). Face à une multiplication des menaces, la cybersécurité devient un enjeu stratégique, tant pour la continuité de leurs services que pour la confiance des usagers et des partenaires (Bellini, Tammaro 2024).

## 1.2 Problématique et questions de recherche

Le secteur de l'éducation et de la recherche est particulièrement exposé aux risques cyber, en raison de son ouverture aux collaborations externes et de la diversité de ses usagers (ESRI 2024). Les bibliothèques académiques situées à l'intersection des secteurs de la recherche, de l'enseignement et pour certaines de la santé, elles cumulent les vulnérabilités de ces domaines (Kederlué, Iriarte 2023). Une interruption d'accès à leurs ressources numériques illustrerait les enjeux de continuité et de résilience. La problématique centrale donne lieu à plusieurs axes d'analyse, ainsi que des questions de recherche spécifiques.

Comment les bibliothèques académiques peuvent-elles garantir la résilience de leurs systèmes d'information et la continuité d'accès à leurs ressources numériques de manière pérenne face aux cyberattaques et aux interruptions de service ?

Identification des vulnérabilités :

- Quelles sont les principales menaces pesant sur les systèmes d'informations des bibliothèques et sur les ressources électroniques ?

- Ces ressources électroniques peuvent-elles être considérées comme des actifs informationnels ?
- Comment adapter les plans d'urgence traditionnellement conçus pour les collections et fonds physiques et les plans de continuité et de reprise d'activité informatiques pour les ressources numériques ? Sont-ils adaptables au contexte des bibliothèques ?

Continuité des services et accès en mode dégradé :

- Quelles solutions permettraient de maintenir un accès aux catalogues, aux ressources électroniques et aux fonctions principales du SIGB en cas de panne ou d'attaque ? Comment garantir un accès autonome et sécurisé, même en environnement isolé ?
- Quelles stratégies de protection, de sauvegarde et d'archivage peuvent garantir l'accès aux ressources numériques en cas d'incident ? L'archivage pérenne constitue-t-il un moyen de mitigation des risques cyber ?
- Comment équilibrer la sécurité et l'ouverture de l'accessibilité des ressources dans un contexte de crise ?

Gouvernance et gestion des risques :

- Quels cadres de gouvernance et de gestion des risques peuvent renforcer la résilience ?
- Quels modèles de gouvernance et protocoles de réponse peuvent être adaptés aux bibliothèques académiques ?
- Quels sont les actifs informationnels critiques en bibliothèque académique et comment les prioriser, les sauvegarder et en garantir un accès pérenne ?

Stratégie durable et adaptation :

- Comment inscrire la résilience numérique dans une stratégie évolutive et durable ?
- Quels sont les défis techniques, organisationnels et juridiques liés à la mise en place d'une cybersécurité efficace en bibliothèque académique ?
- Quels indicateurs permettent d'évaluer l'efficacité des dispositifs mis en place ?

### 1.3 Hypothèses de recherche

Plusieurs hypothèses émergent de ce questionnement :

- Les bibliothèques académiques sous-estiment la criticité de leurs ressources électroniques, et leurs dépendances externes ce qui les rend vulnérables aux cyberattaques et aux pannes.
- Une gestion centralisée des risques et un cadre normatif structuré pourraient améliorer la résilience des systèmes documentaires.
- La redondance des infrastructures et la mise en place de solutions d'accès en mode dégradé sont essentielles pour garantir la continuité des services.
- L'archivage pérenne permet de sécuriser durablement les données et les contenus des ressources électroniques.
- La sauvegarde, l'archivage pérenne et la gestion du cycle de vie des données est un moyen de mitigation des risques cyber et numériques.
- Une adaptation continue et une sensibilisation accrue du personnel et des usagers contribueraient à réduire significativement les incidents de cybersécurité.

## 1.4 Objectifs

La réflexion est proposée comme une méthode de réponse aux cybermenaces en bibliothèque, aux risques liés à la sécurité de l'information numérique, en mobilisant des moyens et pratiques issus des sciences de l'information. Il s'agit d'appliquer les principes de cybersécurité et de la gestion des risques au contexte, tout en tirant parti des ressources internes, des processus, et des dispositifs existants. Dans une phase proactive d'identifier, évaluer et traiter ces risques, puis dans une phase active d'agir sur les méthodes de sauvegardes vers des systèmes alternatifs d'accès. Enfin d'imaginer l'amélioration continue des mesures pour tendre vers une approche holistique de la résilience conforme à un système de management de la sécurité de l'information (SMSI) selon la norme ISO 27001(ISO 2022a). La démarche de sécurité proposée s'articule autour de quatre étapes interdépendantes :

- Une analyse initiale approfondie, impliquant une revue de la littérature, une étude des cas concrets, des normes applicables et des entretiens ciblés avec des experts du secteur et les homologues internes à l'organisation. Il en résulte une comparaison critique des pratiques actuelles à travers une matrice de maturité.
- Un travail de cartographie approfondi des processus métiers et des actifs stratégiques, en vue d'élaborer un registre des risques permettant d'évaluer leur criticité ainsi que leurs impacts potentiels sur la disponibilité, l'intégrité et la confidentialité. Ce cadre amènera la réflexion sur la hiérarchisation des ressources électroniques considérées comme les actifs informationnels critiques au niveau métier.
- À partir des résultats obtenus, un cadre opérationnel sera modélisé afin de proposer une stratégie cohérente de sauvegarde, d'archivage et d'accès aux actifs, en réponse à des scénarios de crises. Ce cadre permettra de documenter les applications et données essentielles aux processus métiers, via une analyse d'impact sur les activités. Les éléments critiques ainsi définis seront intégrés dans un Plan de Continuité d'Activité (PCA), en cohérence avec le Plan de Reprise d'Activité (PRA) existant.
- Enfin une phase d'amélioration continue est prévue mais ne sera que partiellement adressée, afin de proposer, d'optimiser et d'adapter de manière itérative les procédures établies tout en envisageant leur ajustement à différents contextes institutionnels.

Les résultats de chaque étape méthodologique viendront enrichir concrètement la démarche de sécurité, pour une stratégie globale effective et évolutive. Néanmoins l'étude ne peut offrir qu'une vue figée de la situation à un instant donné du contexte. Les recherches empiriques sur la cybercriminalité, ne présentent qu'un état des lieux partiel, d'un phénomène constamment en mouvement (Ghernaouti 2022). Il s'agit de concevoir des mesures dont la courbe d'obsolescence soit inférieure à celle des menaces qu'elles visent à contenir. L'intégration d'un système de gestion de la sécurité de l'information permettra de créer un point de départ, une sensibilisation, une correspondance de vocabulaire et d'assurer une mise à jour continue des stratégies de résilience.

## 2. Méthodologie

La méthodologie repose sur une analyse de données qualitatives, une revue de littérature, et des études de cas analysant les cadres conceptuels établis dans les domaines de la sécurité de l'information et de la cybersécurité, de la gouvernance des technologies de l'information et de la préservation numérique. Elle est enrichie par l'étude de la littérature grise, incluant des rapports internes, des documents techniques non publiés et des analyses propres à l'institution cible. L'intégration de ces documents était nécessaire pour s'aligner de manière complète et cohérente dans le cadre existant de l'institution, proposer une démarche réaliste (Barnum 2022), et comprendre les enjeux qu'implique la résilience des systèmes d'information en bibliothèque académique pour proposer des solutions adaptées.

La recherche documentaire a constitué une base pour l'analyse, en mobilisant des sources scientifiques, professionnelles, institutionnelles et médiatiques. Elle a permis d'initier les études de cas sur les acteurs, menaces et vulnérabilités (Annexe 8), tout en élargissant le périmètre du sujet vers une approche intégrée de la gestion des risques. Cette démarche a été complétée par une exploration de sites de fuite de données sur le *darknet*, afin d'identifier des modes opératoires et les réseaux utilisés par les cybercriminels. L'approche qualitative de la recherche s'est articulée autour de plusieurs entretiens semi-dirigés conduits avec un panel diversifié d'experts (Annexe 6, 7). Ces entretiens, menés tant auprès d'acteurs internes qu'externes à l'institution, permettent de confronter perspectives théoriques et réalités opérationnelles. Ce mode de collecte a été déterminant pour orienter le travail, confronter les approches et enrichir la démarche d'évaluation de sécurité. Ils ont été riches d'enseignement pour la conduite de nouvelles recherches, l'identification d'acteurs et la proposition de solutions envisageables.

### 2.1 Définition des concepts

L'étymologie du préfixe *cyber* trouve ses racines dans le mot grec *kybernetes*, κυβερνήτης, signifiant « gouverner » (Déon 2023), et a été formalisé par le mathématicien Norbert Wiener dans son ouvrage de 1948, *Cybernetics : Or Control and Communication in the Animal and the Machine* (Wiener 2019), définissant la science constituée par l'ensemble des théories relatives au contrôle, à la régulation et à la communication entre l'être vivant et la machine (Ghernaouti 2022). Ce terme a ensuite été popularisé par William Gibson dans son roman *Neuromancer* (1984), où il forge le mot « *cyberspace* » pour désigner un espace virtuel interconnecté, anticipant l'essor d'Internet et des environnements numériques partagés. Dans son acception contemporaine, il désigne tout ce qui se rapporte aux environnements numériques, aux technologies de l'information et de la communication (IT) et aux interactions qu'elles permettent. Ce préfixe s'est étendu à un vocabulaire spécialisé dans des domaines de la sécurité (*cybersécurité*, *cyberdéfense*), la technologie, ou les sciences sociales (*cyberculture*) (Lévy 1997). Cette dynamique s'observe également dans les sciences de l'information, avec des concepts comme *cyberdocumentation* ou *cyberpatrimoine* (Cavalier, Poulain 2015). Ce développement lexical témoigne de la structuration d'un espace numérique parallèle au monde physique, doté de logiques, de risques et de besoins spécifiques. Il impose une approche interdisciplinaire pour appréhender la complexité des mutations induites.

Le terme *cyberpatrimoine* désigne l'ensemble des ressources informationnelles nativement numériques ou numérisées qui constituent aujourd'hui une part croissante du patrimoine documentaire universitaire et scientifique. La croissance exponentielle de ce *cyberpatrimoine*

pose des enjeux critiques liés à la conservation pérenne, à l'obsolescence rapide des formats numériques et à l'organisation des infrastructures informatiques nécessaires pour prévenir toute perte ou altération (Ferracci 2016).

La cybersécurité est l'état cible d'un système d'information capable de faire face à des atteintes susceptibles d'altérer la disponibilité, l'intégrité ou la confidentialité des données, ainsi que des services qu'il héberge ou rend accessibles (ANSSI 2024a). Ces attributs permettent de s'assurer qu'un système fonctionne comme prévu, que les données ne sont ni altérées ni exposées, que l'origine et les actions des utilisateurs sont vérifiables, et que les événements peuvent être retracés. Le terme désigne l'ensemble des stratégies, des mesures techniques, organisationnelles et juridiques visant à protéger les systèmes d'information, les réseaux, les données et les services contre les menaces issues du cyberspace (NRC 1991). La cybersécurité cherche à prévenir, détecter, répondre et se rétablir face aux incidents, qu'il s'agisse de malveillance, de vulnérabilités techniques ou d'erreurs humaines (Ghernaouti 2022).

La valeur informationnelle s'articule aussi autour de la triade disponibilité, intégrité, confidentialité, constituant les axes permettant d'apprécier la criticité des actifs informationnels au regard des objectifs stratégiques et organisationnels. La disponibilité caractérise l'exigence d'accessibilité temporelle et fonctionnelle de l'information pour les utilisateurs légitimes, garantissant la continuité des processus métiers. L'intégrité traduit l'impératif de préservation de l'authenticité et de la complétude des données contre toute altération non autorisée ou accidentelle, préservant ainsi la fiabilité informationnelle. La confidentialité, quant à elle, matérialise le principe de restriction d'accès aux seules entités habilitées, protégeant la sensibilité des informations contre les divulgations inappropriées (Baillargeon et al. 2019). Cette approche est fréquemment enrichie par l'intégration de critères tels que la traçabilité, la capacité à retracer l'historique des accès et modifications ; l'audibilité, la vérification et le contrôle des opérations effectuées, ainsi que la non-répudiation, l'impossibilité de nier l'origine ou la réception d'une information. Chaque critère peut présenter des niveaux d'exigence différenciés selon la nature et l'usage des données concernées (Gouvernement du Québec 2016).

Le concept de *cyber résilience* prend ici tout son sens en désignant la capacité d'un système à anticiper, absorber, s'adapter et se rétablir après un incident d'origine cybernétique, qu'il s'agisse d'une attaque, d'une panne ou d'un effondrement partiel du système, issue d'actions accidentelles ou malveillantes (ENISA, 2021 ; NIST, 2021). Face à l'ampleur des enjeux économiques, scientifiques, culturels cette capacité devient une condition essentielle de la continuité de la mission et de la confiance (Ghernaouti, Aghroum 2012).

La résilience est un modèle conceptuel issu des secteurs de la physique, du nucléaire, de l'aviation et de la santé, visant à assurer la continuité des services et à apprendre des perturbations. C'est la « capacité intrinsèque d'un système à entretenir ou rétablir un état dynamiquement stable qui lui permette de poursuivre ses opérations après un incident majeur ou en présence d'un stress continu. » (Leplat 2007). Un système est résilient s'il peut s'ajuster avant, pendant et après une perturbation, et maintenir ses fonctions critiques malgré l'imprévu. Elle se construit à l'échelle organisationnelle via des systèmes adaptatifs, des capacités collectives, et une culture de l'apprentissage (Capdarest-Arest, Tompson, Zipperer 2022).

La continuité des services désigne la capacité d'une organisation à maintenir ses fonctions essentielles, à continuer ses opérations à un niveau acceptable et prédéfini, malgré des perturbations d'origine diverses, qu'elles soient ponctuelles, prolongées ou permanentes (ISO 2019). Dans le contexte spécifique d'une bibliothèque, ce concept implique la garantie d'un accès ininterrompu aux ressources documentaires et informationnelles, indispensable pour la réalisation de sa mission, pour l'enseignement et la recherche, indépendamment des incidents susceptibles d'affecter l'infrastructure technique, organisationnelle ou les relations avec les fournisseurs externes.

Différents types de plans coexistent selon leur périmètre et leurs finalités. Dans le champ bibliothéconomique, le plan de reprise d'activité (PRA ou *disaster response plan, DRP*), vise principalement à restaurer les services et à organiser le sauvetage des collections imprimés, tout en assurant la continuité des activités internes et publiques. À l'échelle des systèmes d'information, ce PRA se focalise sur la reprise des services numériques critiques. Le plan de continuité d'activité (PCA ou *Business Continuity Plan, BCP*), quant à lui, adopte une approche globale incluant les processus et services métiers essentiels, ressources humaines, finances, etc. Enfin, le plan d'urgence (emergency management plan) est plus large encore et relève souvent des pouvoirs publics, notamment en cas de catastrophe naturelle (Kahn 2012). Dans une perspective organisationnelle et informatique, le PCA désigne l'ensemble des mesures assurant la continuité des activités critiques. Il s'appuie sur le plan de secours informatique (PSI, ou PRA dans le cas de l'UNIGE) pour garantir la résilience du système d'information. Le management de la continuité d'activité (MCA/Business continuity management ou BCM) encadre la mise en œuvre de ces dispositifs (Boulet 2008). Ce terme sera remplacé par le SMSI (système de management de sécurité de l'information)(ISO 2022a). Dans ce travail, nous utilisons les référentiels institutionnels en considérant le PRA comme un plan de contingence à portée informatique, et le PCA comme un plan de continuité d'activité orientée métier, qui englobe le PRA et intègre les spécificités d'un plan de sauvetage des collections appliquée aux ressources électroniques.

Une ressource électronique en bibliothèque désigne un contenu documentaire ou informationnel disponible sous format numérique, accessible via des réseaux informatiques, généralement Internet, et souvent hébergé sur des plateformes externes appartenant à des éditeurs ou fournisseurs (Beagrie 2013). Il peut s'agir de revues scientifiques, bases de données, livres numériques, actes de conférences, ou encore de contenus multimédias. La dématérialisation rend nécessaire de nouvelles stratégies et complique l'accès aux documents, hétérogènes dans leur format, ergonomie, droits d'usage et modalités de consultation. Ces ressources se distinguent par leur nature labile, évolutive et médiate (Alexandre 2015), ce qui complexifie leur gestion et leur préservation à long terme. Contrairement aux documents physiques, les bibliothèques ne possèdent généralement pas les fichiers eux-mêmes, mais acquièrent un droit d'accès temporaire, dans le cadre de modèles économiques basés sur l'abonnement ou l'accès à distance sécurisé (Corrado, Moulaison 2014). Ce glissement de la propriété vers l'usage s'accompagne d'une dilution des responsabilités en matière de conservation, et rend les bibliothèques dépendantes des prestataires pour garantir l'accès pérenne aux contenus. La croissance exponentielle des données, la diversité des modèles commerciaux et l'évolution rapide des technologies rendent essentielle l'intégration de garanties de conservation, de traçabilité et d'accès pérenne pour l'enseignement, la recherche et le patrimoine scientifique (Alexandre 2014).

Enfin la sauvegarde représente le processus méthodique de duplication et de préservation temporaire des données actives garantissant leur restauration à la suite d'un incident, tandis que l'archivage, inscrit dans une temporalité plus longue, assure la conservation pérenne des informations à valeur probatoire ou patrimoniale selon des normes assurant leur authenticité, leur intégrité et leur accessibilité durable (ISO 2025a).

Tableau 1 - Sauvegarde et Archivage

Critères	Sauvegarde	Archive
Objectif	Restauration rapide en cas d'incident	Conservation long terme pour raisons légales ou analytiques
Durée de rétention typique	Courte (quelques jours à 1 mois maximum)	Longue (7, 15, voire 40 ans)
Type d'accès	Fréquent en cas de problème	Rare, planifié, voire exceptionnel
Format typique	Systèmes de fichiers, instantanés, snapshots	Stockage objet, bandes magnétiques, cloud froid
Exemples d'usage	Récupération d'un fichier supprimé, reprise après crash	Réponse à une enquête réglementaire, analyse historique

(Wright 2024)

## 2.2 Recherche documentaire

Le sujet a été décomposé afin d'isoler et de déterminer ses concepts fondamentaux ainsi que leurs périmètres. Cette analyse a identifié les éléments spécifiques, discriminants et ceux transversaux ou combinables dans un plan de recherche thématique. Les axes ont été déclinés en sous-thèmes et ont ensuite été décomposés en concepts liés. Plusieurs concepts ont fait l'objet d'une normalisation par l'utilisation de thésaurus spécialisés, de glossaires (ANSSI 2024a) et de la norme ISO 27000 (ISO 2020) pour garantir la précision des graphies, de la sémantique et optimiser l'efficacité des recherches. Cette normalisation a abouti à des mots-clés, auxquels ont été associés des synonymes, antonymes ou notions complémentaires, variations linguistiques, ainsi que leurs traductions en anglais, langue principale pour la littérature scientifique sur ce sujet. Ces mots-clés ont ensuite servi à construire des équations de recherche adaptées aux différents outils et plateformes, incluant des moteurs de recherche, des catalogues et dépôts institutionnels, ainsi que des bases de données bibliographiques et plein-texte. Les critères de sélection des sources ont privilégié la pertinence, la récence des données, et la rigueur méthodologique des articles. Des critères d'exclusion ont aussi été définis pour éliminer les documents hors périmètre, ou présentant des informations peu enrichissantes.

La consultation d'ouvrages, supports de cours et conférences spécialisées a permis d'approfondir le sujet, tandis que les bibliographies associées ont élargi le corpus initial. Une documentation technique spécialisée a aussi été nécessaire sur les aspects plus précis, ainsi qu'une veille proactive sur des plateformes spécialisées, blogs d'intérêt en cybersécurité ainsi que des projets liés à l'analyse et aux traçages de *malware* sur le darknet.

La phase de recherche, de collecte et de traitement de la littérature scientifique et a été interrompue aux deux tiers de l'avancement du travail, plus tard que ce que le principe d'exploration-exploitation optimal pré suppose (Christian, Griffiths, Griffiths 2023). Cette décision s'est imposée face à l'intensité quotidienne des publications et actualités relatives à la cybersécurité, phénomène qui ne présente aucun signe de ralentissement. Certains articles issus de la recherche ont pu enrichir le programme de veille de la Bibliothèque.

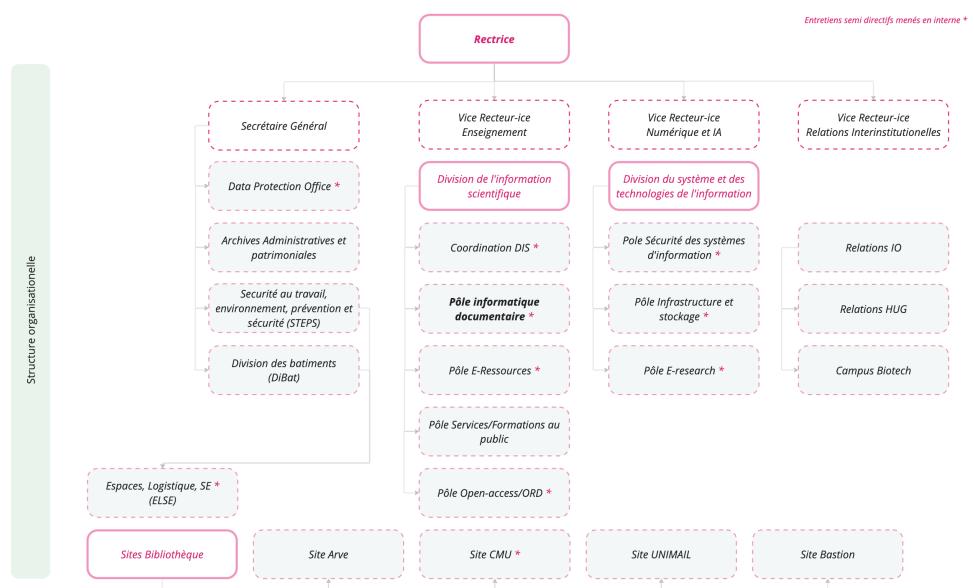
## 2.3 Collecte des données qualitatives

Le choix de récolter ce type de données par l'intermédiaire d'entretiens semi-directif (Annexe 2) a été motivé pour mettre à profit des expériences et des compétences variées sur le thème de la cybersécurité. Avoir une assise professionnelle solide et pouvoir la transposer sur une analyse métier en bibliothèque académique. Une grille d'entretien semi-directif a été élaborée pour structurer les réponses de manière cohérente mais en laissant libres les participants de développer tel ou tel thème.

Chaque terme-clé, issu du sujet, a été décomposé en concepts, puis rattaché à des groupes de notions similaires afin de constituer des thématiques pouvant répondre aux hypothèses. Ces thématiques ont servi à la classification et à la sélection des documents retenus, puis ont été utilisées dans la construction des questionnaires. Les 6 axes identifiés sont :

- Identification et compréhension des menaces et des vulnérabilités pesant sur les SI des bibliothèques académiques, et les ressources électroniques
- La protection des actifs informationnels, la priorisation et la classification des ressources numériques critiques
- La mise en place, l'usage de plans d'urgence et de dispositifs de gouvernance et de répartition des responsabilités
- La continuité opérationnelle et les solutions alternatives d'accès pérennes aux services
- Les stratégies de sauvegarde, d'archivage numérique et de gestion de l'obsolescence technologique
- Enfin, les recommandations et perspectives identifiées et les cas rencontrés et les retours d'expérience

Figure 1 - Organigramme UNIGE et entretiens réalisés en interne



CC BY NC Stephen Valot 2025

Les entretiens internes présentés en Figure 1 ont concerné les services et parties prenantes de l'UNIGE impliqués dans les problématiques de cybersécurité, de gouvernance, de gestion

documentaire et des données. Au cours de ces entretiens il s'est révélé incontournable de se greffer aux mesures et aux politiques existantes au sein de l'institution pour la validité de la proposition mais également pour ajouter une utilité concrète pour la suite de ce projet à l'interne.

Les entretiens externes (Annexe 3) ont impliqué des profils variés tel des spécialistes en cybersécurité des directeurs du système d'information, des responsables de l'infrastructure, responsables de la sécurité du système d'information, des responsables de solutions de préservation numériques. Mais aussi des chercheurs, spécialistes en conservation du patrimoine physiques et numériques, gestionnaires des collections électroniques, archivistes et bibliothécaires.

Ces données qualitatives détaillées permettent d'appréhender avec précision les nuances et la complexité des phénomènes étudiés, tout en validant ou réorientant les axes pris lors des premières phases de recherche et d'études de cas. Chaque entretien a fait l'objet d'un compte-rendu (Annexe 4). Les synthèses ont été traités sous forme d'une grille thématique et ont permis de collecter et d'interpréter les résultats, mais aussi d'identifier les écarts entre les pratiques observées et les attentes formulées. Ces résultats ont été croisés avec les données des études de cas et de la revue de littérature afin d'établir un état des lieux complet, essentiel à la définition opérationnelle des besoins à court, moyen et long terme.

## 2.4 Utilisation de données quantitatives

Afin d'établir une hiérarchisation raisonnée des ressources électroniques à préserver, des données quantitatives ont été mobilisées. La distinction a d'abord été faite entre les ressources électroniques acquises et celles produites par l'institution. Des extractions de statistiques ont été effectuées à partir de la plateforme ALMA Analytics, pour analyser les usages, en s'appuyant sur des rapports conformes à la norme COUNTER fournis par les éditeurs. Ces données internes ont été transmises par le pôle e-ressources pour une quantification des différents types de ressources. En complément, une extraction des termes contractuels liés aux licences consortiales a été réalisée afin d'identifier les clauses d'accès pérenne dans les accords.

## 2.5 Analyses et interprétation des résultats

Les entretiens ont permis d'identifier les menaces pertinentes, de valider les normes à suivre, et de mieux cerner les vulnérabilités existantes. Le choix d'un panel composé à la fois d'acteurs internes et externes a offert une vision complète de la situation actuelle, facilitant l'établissement d'un état des lieux. Cette approche a contribué à définir les cadres de référence et de sécurité à mobiliser, ainsi que les mesures prioritaires à mettre en œuvre. L'objectif a été d'inscrire cette démarche dans la continuité des pratiques existantes, en veillant à un alignement stratégique et opérationnel.

### 2.5.1 Synthèse des entretiens sur les pratiques

Les entretiens externes ont été menés dans une démarche d'analyse comparative (Annexe 6) sur un panel d'institutions issues de l'enseignement supérieur, de la recherche et du domaine patrimonial. L'objectif était de mettre en perspective les enjeux de préservation numérique à travers différents contextes organisationnels, technologiques et géographiques.

La synthèse des entretiens internes (Annexe 7) s'appuie sur une réflexion, menée à plusieurs niveaux. L'analyse a été structurée en tenant compte des différentes couches du système d'information : de l'infrastructure technique aux applications, en passant par les données, jusqu'aux enjeux de gouvernance. Cette approche permet de comprendre les points de friction et de coordination nécessaires pour une gestion cohérente des ressources électroniques.

### 2.5.2 Résultats intermédiaires

Les recommandations formulées par les institutions externes interrogées convergent sur :

- Finaliser et renforcer les stratégies de sauvegarde avec des solutions robustes hors-site et off-line selon le modèle 3-2-1
- Automatiser les procédures critiques, améliorer la documentation et instaurer une communication alternative en cas de crise
- Évaluer régulièrement les risques et les infrastructures selon des normes reconnues (ISO 27001, EBIOS RM, NIST)
- Formaliser une gouvernance claire et partagée, avec une priorisation des ressources critiques basée sur des guides de bonnes pratiques
- Développer une culture institutionnelle de la gestion des risques, incluant des formations régulières et des indicateurs métiers
- Encourager les collaborations interinstitutionnelles pour renforcer la résilience documentaire, travailler à la mutualisation des ressources et à la coopération.

Ces recommandations insistent sur la nécessité d'adapter les stratégies selon les contextes spécifiques de chaque institution. La majeure partie des personnes interviewé insiste aussi sur l'aspect du financement qui doit lui aussi être pérenne et dimensionnés autant dans les projets de sécurité informatique, préservation numérique que d'archivage à long terme.

Les recommandations internes se focalisent quant à elle sur :

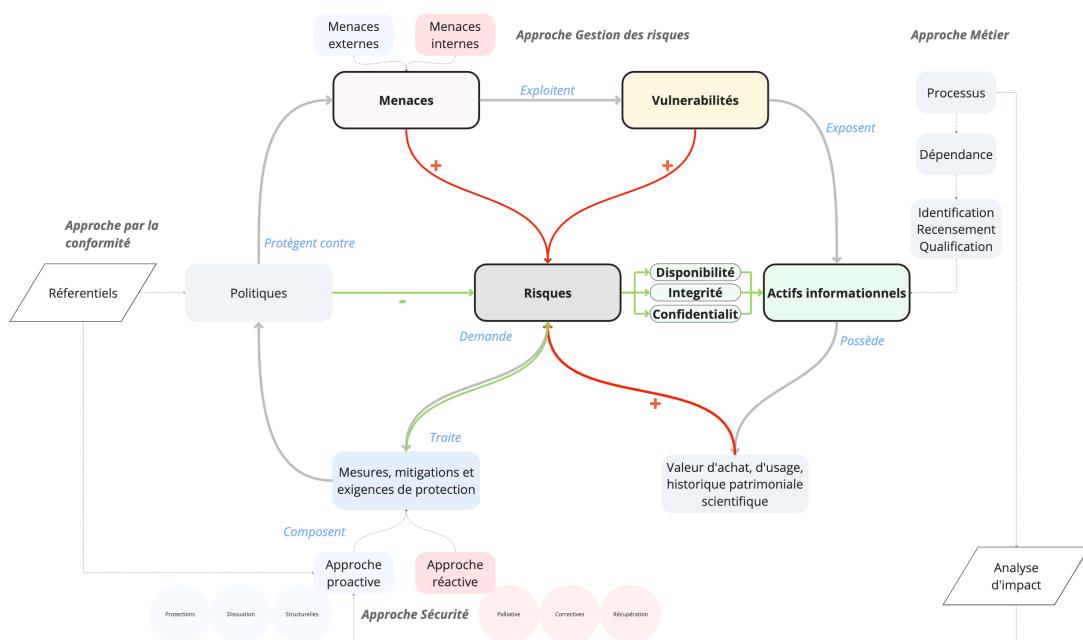
- La nécessité d'une revue annuelle systématique des plans de continuité
- La création et la tenue d'un registre exhaustif des actifs informationnels prioritaires, internes et externalisés au niveau métier
- La sensibilisation à la gestion documentaire et numérique est considérée comme prioritaire
- L'adaptation au contexte numérique de la rigueur déjà appliquée aux archives physiques
- L'intégration de la préservation numérique dans les contrats d'acquisition avec les éditeurs et de l'archivage électronique à la stratégie globale de l'université
- À court et moyen terme, une sauvegarde minimale des catalogues est proposée.

À long terme, il est recommandé d'intégrer davantage les ressources critiques dans les plans de continuité institutionnels. La mise à profit des refontes des systèmes d'information des services métiers comme levier de sensibilisation et de formation est fortement préconisée, en vue d'instaurer une véritable culture institutionnelle autour de la sécurité et de la préservation numérique.

### **3. Exposition, menaces et vulnérabilités en bibliothèque**

Dans le champ de la cybersécurité, trois concepts structurent l'analyse des incidents potentiels et l'élaboration des stratégies de protection : les vulnérabilités, les menaces et les risques. Une vulnérabilité désigne toute faiblesse inhérente à un système d'information qu'elle soit d'ordre technique, humaine ou organisationnelle susceptible d'être exploitée pour compromettre la sécurité des actifs. Les menaces, quant à elles, renvoient à des événements ou à des acteurs malveillants qui pourraient tirer parti de ces vulnérabilités (ANSSI 2024a).

Figure 2 - Dynamique entre menaces, vulnérabilités et risques



Adapté de (la gestion des risques de la norme Afnor Z 74-260-1, Ghernaouti 2022)

Ce triptyque, figure 2, constitue le socle des méthodologies d'analyse et de gestion des risques en cybersécurité, et en sécurité de l'information telles que décrites dans la norme ISO 27005 (ISO 2018). Il permet une évaluation des facteurs de fragilité et une priorisation des mesures de mitigation, dans notre contexte, la protection et la couverture des ressources électroniques dans l'infrastructure de la bibliothèque reposant sur l'infrastructure de l'université.

### **3.1 État des lieux d'un contexte spécifique**

À l'intersection de la recherche, de l'enseignement et de la préservation du patrimoine, les bibliothèques académiques et scientifiques s'inscrivent dans le paysage de l'enseignement supérieur. Contrairement aux bibliothèques publiques, généralement rattachées aux municipalités, ou aux bibliothèques patrimoniales relevant des cantons ou de la confédération. Leur sort est étroitement lié à celui des hautes écoles, tant en termes d'opportunités que de vulnérabilités. Cette liaison permet aux bibliothèques de bénéficier des infrastructures, des dispositifs de sécurité, et des compétences des services informatiques institutionnels. Mais cela renforce aussi leur exposition aux risques. En raison de leur environnement ouvert, elles constituent des cibles potentielles lors d'attaques visant l'établissement ou des points d'entrée privilégiés pour des intrusions. Leur vulnérabilité est renforcée par l'écosystème auquel elles appartiennent, partageant métadonnées, systèmes d'authentification et ressources avec les

universités, les centres de recherche et d'autres infrastructures critiques (Bellini, Tammaro 2024). Elles sont liées à de nombreuses parties prenantes notamment les facultés dont les priorités peuvent diverger de celles de l'administration ou des services techniques. Car les hautes écoles font face à une diversité de menaces (Welch 2019). L'absence de mises à jour ou de correctifs de sécurité constitue une vulnérabilité particulièrement critique. Encore faut-il pouvoir mobiliser les ressources pour les réaliser et s'assurer de la validité des protections contre les atteintes visant à compromettre les trois fondamentaux de la sécurité de l'information, confidentialité, intégrité et disponibilité des systèmes d'information.

La multimodalité des ressources en bibliothèque impose une approche transversale, encore cloisonnée, entre d'une part la préservation des documents physiques profitant d'une expérience séculaire et, d'autre part, une préservation numérique, dont la gestion est récente. Cette dernière est perçue à tort comme dématérialisée donc du ressort exclusif des équipes informatiques. En réalité, les infrastructures numériques, serveurs, terminaux, supports de stockage, reposent aussi sur une matérialité tangible. Cette dualité appelle à une convergence des stratégies de conservation. Il convient de repenser de manière concertée les espaces et dispositifs de conservation, en partant du principe que les zones sécurisées destinées à l'archivage numérique peuvent, et doivent partager les mêmes exigences que celles dédiées aux archives physiques. Ils doivent garantir la sécurité des accès, le contrôle de l'environnement, la surveillance et la résilience. La contrainte de l'espace physique qui touche les collections imprimées trouve un équivalent dans la charge croissante liée à l'hébergement, la consommation énergétique et la maintenance des serveurs. L'ère de l'information connaît une augmentation exponentielle de la production et de la consommation de données. Progressant plus rapidement que les lois de Moore sur la densité de transistor et de Kryder sur la densité des supports de stockage, les stratégies de stockage de données actuelles ne pourront répondre à la demande, devant atteindre cette année, plus de 170 ZB selon les estimations (Wang et al. 2024 ; Extance 2016).

Dans cette perspective une harmonisation interne et externe des pratiques, une politique d'archivage pérenne, commune à l'ensemble des supports (papier et numérique), doit être étudiée. Elle implique une coordination entre les différents services de l'université, le rectorat et les instances déjà actives en matière de mutualisation des ressources, avec une mobilisation de partenaires externes comme la *Protection des biens culturels de la Ville de Genève*. Une telle démarche permettrait un gain significatif d'efficience, tant en matière de gouvernance que d'exploitation des ressources disponibles. Actuellement, les pratiques restent hétérogènes et s'appuient peu sur les cadres déjà existants. Le plan de sauvetage des collections peut être une base de cette réflexion. Plusieurs experts internes précisent la nécessité de disposer localement de certaines informations critiques, mais ces données sont aujourd'hui stockées sans véritable stratégie de gestion unifiée.

Il est essentiel d'articuler la sauvegarde et l'archivage à long terme dans le cadre d'une politique cohérente. Là où les procédures de sauvegarde visent une restauration rapide après un incident, l'archivage s'inscrit dans une logique de préservation durable, de traçabilité, et de pérennité de l'accès à l'information. Les conséquences de son absence peuvent être patrimoniales (perte irréversible d'un document unique), fonctionnelles (interruption de service), éthiques (manipulation des contenus par IA), financières (coûts juridiques, sanctions, perte de financement), ou réputationnelles. Une attaque peut durablement entamer la confiance des usagers et des communautés scientifiques (Bellini, Tammaro 2024).

### **3.2 Études de cas concrets d'attaques**

Sans prétendre à l'exhaustivité, les études de cas présentées visent à éclairer certains des mécanismes, moyens d'actions, des vulnérabilités exploitées par différentes typologies de menaces, lors d'incidents de cybersécurité majeurs ayant touché des institutions comparables à celles de notre périmètre. La cybersécurité dépasse les seuls dispositifs techniques. Elle nécessite une compréhension des profils d'acteurs malveillants, de leurs motivations, ainsi que des vecteurs d'attaque qu'ils mobilisent (Ghernaouti, 2022). La cybercriminalité s'appuie sur une combinaison de tactiques visant les vulnérabilités humaines, techniques et organisationnelles, telles que l'ingénierie sociale, l'usurpation d'identité ou encore l'exploitation de failles logicielles et matérielles (Ghernaouti, 2022). L'acquisition de cette connaissance constitue un prérequis pour concevoir des stratégies de détection, renforcer la posture de sécurité et favoriser une culture organisationnelle de vigilance. L'étude, fondée sur cette documentation, encourage aussi le partage des retours d'expérience afin d'établir les fondements d'une vigilance collective entre les institutions poursuivant des missions similaires.

Plusieurs études de cas d'institutions similaires à notre objet d'étude ont été analysées (voir Annexe 8 pour le détail). La British Library, victime d'une attaque par rançongiciel en 2023, a vu ses activités fortement perturbées, avec des pertes significatives en disponibilité, intégrité et confidentialité de ses données, révélant des lacunes en authentification multifactorielle et segmentation réseau. Cet incident insiste sur l'importance critique d'une architecture de sauvegarde redondante et hors ligne pour assurer la pérennité des collections numériques mais aussi des catalogues. L'Université de Neuchâtel (2022), a mis en évidence la nécessité de stratégies proactives incluant chiffrement, segmentation des réseaux et sensibilisation des utilisateurs. À Zurich (2023), une attaque DDoS déclenchée par la fuite d'identifiants rappelle la pertinence d'une surveillance proactive des forums criminels et d'une gestion rigoureuse des mots de passe. La Haute École Spécialisée de Lucerne (2025), victime d'un *ransomware* dans un laboratoire isolé, alerte sur les risques liés au *shadow IT* et l'importance d'une collaboration rapide avec des partenaires externes spécialisés. L'Université de Leipzig (2023) a subi une fuite massive de données personnelles, démontrant les vulnérabilités dans la gestion du cycle de vie des données utilisateurs et soulignant l'importance d'une réponse rapide, même après une attaque opportuniste. En France (2022-2023), des établissements d'enseignement supérieur ont subi une vague d'attaques qui illustrent la nécessité d'une réponse institutionnelle centralisée et de politiques de cybersécurité. L'attaque contre l'Université Paris-Saclay (2024) montre les influences que peuvent avoir des périodes sensibles comme les grands événements internationaux, et le contexte géopolitique. Le cas du centre médical universitaire du Vermont (2020) révèle comment une cyberattaque visant un hôpital peut affecter indirectement les bibliothèques universitaires de santé, justifiant la nécessité de plans spécifiques de continuité. Enfin, les attaques sur des centres de calcul du CERN et de l'EPFZ (2020-2024) montrent l'importance d'une architecture réseau Zero-Trust et des stratégies de sauvegarde en dévoilant l'impact financier à posteriori de ce type d'incident. Les attaques contre l'Internet Archive (2024), garant de la mémoire numérique mondiale, accentuent le besoin critique de renforcer la résilience des infrastructures documentaires, tant techniquement que financièrement. Ces cas démontrent unanimement l'urgence d'une approche intégrée et proactive de la cybersécurité dans le secteur documentaire et académique.

Bien que la nature dynamique et le caractère évolutif de la cybercriminalité, dont les acteurs s'organisent en fonction d'opportunités changeantes, rend impossible une représentation figée. Il est alors question d'identifier des tendances (Ghernaouti 2022). Ces évolutions constantes constituent une menace mais aussi un moyen de mitigation et constitue l'enjeu prioritaire pour les institutions académiques (ESRI 2024). Celles-ci se révèlent protéiformes et souvent opportunistes, avec une prédominance marquée des attaques par *ransomware*. Le site Konbriefing (Kondruss 2025) recense les incidents de cybersécurité déclarés dans le secteur de l'enseignement et de la recherche. En 2023, 137 attaques visant ces institutions ont été recensés officiellement signalées et documentées, témoignant de la pression croissante sur ce secteur (Liu, Zou 2023).

### 3.3 Une typologie des menaces

L'escalade exponentielle de la cybermenace résulte de trois mutations convergentes. La professionnalisation criminelle illustrée par l'émergence du *Ransomware as a Service* (RaaS) démocratisant les attaques, la « structuration économique du *darknet* générant 2,1 milliards de dollars en 2021, et l'explosion des vulnérabilités avec un doublement des failles "Zero Day" exploitées entre 2019 et 2021 » (CIGREF 2023). Cette dynamique entre commercialisation, infrastructure criminelle et multiplication des points d'entrée, favorise les attaques par rebond créant ainsi un écosystème lui-même résilient et adaptatif.

Les menaces les plus fréquemment relevées dans la littérature, les études de cas et les entretiens se répartissent en trois catégories principales. Les menaces externes, telles que les rançongiciels (*ransomware*), l'hameçonnage, les attaques par déni de service ou encore l'exfiltration de données. Les menaces internes incluent la dépendance aux fournisseurs et systèmes tiers, les erreurs humaines, ainsi que celles liées aux modèles économiques ou politiques. Enfin, les menaces émergentes, comme la désinformation, l'exploitation malveillante de l'intelligence artificielle, l'accroissement des attaques automatisées par bots ciblant les contenus, les risques environnementaux pesant sur les infrastructures numériques, ainsi que les conflits armés menacent directement le patrimoine documentaire et numérique.

#### 3.3.1 Menaces externes, *ransomware* et attaques logiques

Les rançongiciels, ou *ransomwares* apparaissent comme la menace externe la plus courante. « La grande majorité des attaques par rançongiciels sont opportunistes et profitent du faible niveau de maturité en sécurité numérique de leurs victimes. » (ANSSI 2020). Il consiste à chiffrer les données critiques d'une organisation, souvent après les avoir exfiltrées, et exiger une rançon pour leur restitution et leur non-diffusion. Cette typologie d'attaque se distingue par son degré élevé de sophistication, comparable dans certains cas à celui des opérations d'espionnage étatiques. Afin d'accroître leur portée et leurs effets, les cyberattaquants combinent fréquemment les *ransomware* à d'autres logiciels malveillants, ce qui permet à la fois l'exfiltration de données sensibles et l'exploitation illicite des ressources matérielles des systèmes compromis. Ce type d'incident est devenu classique et cible particulièrement les institutions du secteur public et éducatif (Khadgi 2023). Une évolution notable de cette menace réside dans l'usage croissant de la double extorsion. Les attaquants menacent de chiffrer les données, mais également de les publier afin d'accentuer la pression sur la victime.

L'enseignement supérieur et les bibliothèques, sont confrontés à ce vecteur d'attaque privilégié par les cybercriminels. L'étude « *The State of Ransomware in Education* », menée par Sophos (2023), analyse les évolutions de ce phénomène, basée sur une enquête

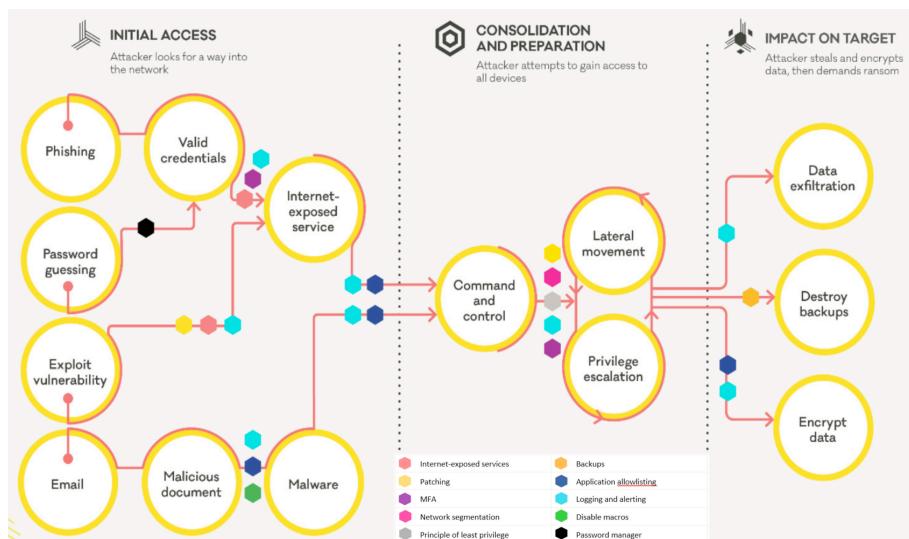
d'envergure réalisée auprès de 200 établissements éducatifs dans 14 pays. Si 2024 révèle une légère baisse des attaques dans l'enseignement supérieur, 66 %, contre 79 % en 2023, ce secteur reste parmi les plus ciblés, avec des conséquences importantes sur le plan financier et opérationnel. Principalement causées par l'exploitation de vulnérabilités, des identifiants compromis ou des courriels malveillants, elles conduisent dans 73 % des cas au chiffrement des données, et dans 35 % à leur vol. Bien que toutes des institutions interrogées aient finalement récupéré leurs données, 56 % d'entre elles ont verser une rançon, tandis que 63 % ont utilisé des sauvegardes. Les hautes écoles, bien qu'ayant renforcées leurs capacités de sauvegarde des données, demeurent particulièrement vulnérables à des tentatives de compromission de ces sauvegardes, réussies dans 71 % des cas. Cette vulnérabilité est d'autant plus préoccupante que les coûts associés à la récupération après une attaque ont quadruplé en un an, atteignant en moyenne 4,02 millions de dollars pour le secteur (SOPHOS 2023). La fréquence élevée des paiements de rançon 67 % ainsi que le montant médian de ces paiements témoignent d'une tendance inquiétante pouvant encourager une escalade future des attaques. Les établissements ayant versé une rançon ont connu des délais de rétablissement plus longs : 38 % ont mis plus d'un mois à récupérer leurs données, contre 21 % pour ceux ayant restauré à partir de sauvegardes (SOPHOS 2023; Schwartz 2023).

Le groupe Rhysida auteur de l'attaque contre la *British Library* (Annexe 8) incarne cette menace externe qui fonctionne selon un modèle de *ransomware-as-a-service* (RaaS). Ils louent leurs outils et son infrastructure à des affiliés en échange d'une part des rançons (Houghton, Winterburn, Oakley 2025). Ils ciblent délibérément les mécanismes de récupération, qu'il supprime via des outils natifs pour empêcher toute restauration (Khadgi 2023). Ce type de mode opératoire justifie la nécessité de réPLICATIONS hors ligne via des politiques de sauvegarde et d'archivage. Cela implique de renforcer la sécurité technique des sauvegardes, mais également les stratégies de réponse aux incidents pour limiter l'impact de ce type d'attaque. La coopération avec les autorités publiques et les organismes spécialisés en cybersécurité devient également une nécessité (Welch 2019). Par ailleurs, les effets des *ransomware* dépassent souvent la sphère immédiate de la victime, et compromettent ainsi l'intégrité de chaînes d'approvisionnement entières. Au-delà des pertes financières, les victimes subissent des interruptions d'activité, des dommages réputationnels, des contentieux juridiques et une perte durable de confiance (DDPS 2024a).

Bien que certaines organisations optent pour le paiement des rançons dans l'espoir de restaurer rapidement l'accès à leurs données, les statistiques révèlent une efficacité incertaine (Poupard 2018). Seulement 58 % des entités ayant payé ont pu récupérer leurs données, et à peine 21 % ont obtenu une restauration complète. De surcroît, 80 % de ces organisations ont subi une nouvelle attaque, parfois perpétrée par le même groupe (SOPHOS 2023). Cette menace alimente un modèle économique cybercriminel lucratif, et contribue à sa prolifération (ANSSI 2020). En Suisse, le paiement d'une rançon n'est pas explicitement illégal mais soulève néanmoins des enjeux juridiques. « Les entreprises qui versent des fonds en cryptomonnaie à des cybercriminels pourraient être accusées de complicité de blanchiment d'argent (art. 305bis CP), de soutien à une organisation criminelle (art. 260ter CP) ou de financement du terrorisme (art. 260quinquies CP) » (DDPS 2024b).

En complément de ces observations, des outils comme RansomLook.io<sup>1</sup> (Dulaunoy, Fafner 2022) permettent de construire une veille des attaques par *ransomware*. Ce projet *open source*, centralise des données issues de blogs spécialisés, de forums, de chaînes Telegram publiques, de comptes cryptographiques révélés (Dulaunoy, Fafner 2022). Il permet d'identifier les victimes, de suivre les dernières attaques déclarées et de repérer les fuites de données sur les sites marchand du darknet. L'initiative NoMoreRansom (2021) est également intéressante en mettant à disposition les clés de déchiffrement connues des groupes exploitant des *ransomwares*.

Figure 3 - Cycle de vie d'un *ransomware*



(CERT NZ, CISA 2023)

Les organisations ne peuvent efficacement contrer ces attaques en se focalisant uniquement sur le rançongiciel lui-même. En effet, les cybercriminels s'introduisent généralement dans les systèmes d'information plusieurs semaines avant de déclencher l'attaque. Cette phase préalable (Figure 3) implique l'utilisation de divers programmes malveillants (*malwares*), des chevaux de Troie, des outils spécialisés dans le vol ou l'effacement d'informations (*stealer*, *wiper*), ainsi que des outils légitimes de test d'intrusion détournés de leur usage initial. Ces attaques logiques désignent l'ensemble des menaces ciblant les systèmes d'information via des moyens technologiques. Si les organisations disposent généralement de mesures courantes pour y faire face dans leur plan de sécurité informatique, la sophistication croissante des attaques, désormais orchestrées par des organisations criminelles structurées, appelle à un surcroit de vigilance (Boulet 2008). Plus une institution est dépendante de ses systèmes numériques, plus elle doit intégrer ces menaces dans la gestion des risques et son plan de continuité d'activité. Ces scénarios doivent être anticipés comme des situations de crise majeures dans les dispositifs de continuité.

L'identification précoce des outils de rançongiciel renforce la détection des menaces, mais doit s'inscrire dans une stratégie de sécurité alliant correction des vulnérabilités et sensibilisation des usagers.

<sup>1</sup> Sous licence GNU GPL 3.0, RansomLook.io s'appuie sur des sources reconnues telles que Malpedia, Ransomwhe.re ou ThreatLabz, cet outil constitue une ressource exploitable pour documenter les modes opératoires, les typologies de cibles et l'évolution des menaces.

### **3.3.2 Menaces internes, erreurs humaines et négligences**

Au-delà des attaques externes très médiatisées, les menaces internes représentent également des inquiétudes pour les établissements d'enseignement supérieur. Leurs infrastructures numériques ouvertes augmentent leur surface d'attaque et sont souvent accessibles à une communauté aux profils et niveaux d'habilitation hétérogènes : étudiants, doctorants, assistants techniques, parfois détenteurs de droits étendus (ESRI 2024). Par effet de bord les services numériques des bibliothèques, se retrouvent par ce biais ainsi exposé.

Trois vecteurs de menaces internes émergent. La fraude académique, motivée par des enjeux de performance ou de bénéfices personnels, et se manifeste par la modification de notes, la fuite de sujets d'examen ou la manipulation d'outils anti-plagiat. Le sabotage ou la revanche personnelle, souvent en lien avec des conflits internes ou des exclusions, peut entraîner le blocage de portails pédagogiques (via DDoS internes ou tentatives d'injection de malwares sur des plateformes éducatives), affectant directement la disponibilité des cours et la réputation de l'institution. Enfin la monétisation de données universitaires, notamment par la revente de comptes institutionnels, de bases d'emails ou de comptes donnant accès à des résultats de recherche sur des forums clandestins (Lallie et al. 2023). Les ressources électroniques volées et diffusées illégalement peuvent exposer la bibliothèque à des poursuites légales pour violation de droits d'auteur ou licences. Les éditeurs surveillant le réseau de leur côté, envoient des « *infringement notice* » pour les usages non autorisés aux services de sécurité de l'UNIGE et aux services de la Bibliothèque (Entretien P.L'Hostis, 2025).

Plusieurs facteurs accentuent les vulnérabilités des systèmes d'information des hautes écoles. La culture d'ouverture des établissements rend la segmentation du réseau difficile (Hughes 2024). L'hétérogénéité des compétences numériques parmi les usagers, le maintien des accès après le départ d'un utilisateur pour faciliter les collaborations universitaires et l'externalisation croissante des services numériques exposent l'université aux failles de ses prestataires et étend la surface d'attaque. Le scénario de risque interne typique combine un accès légitime à un système, une élévation des priviléges, puis l'exploitation d'une faible traçabilité. En l'absence de politiques de moindre privilège (PAM), de journalisation et de campagnes de sensibilisation, les universités s'exposent à des conséquences graves. Selon Lallie et al. (2023), cinquante-huit cyberattaques ont été recensées dans le secteur de l'éducation britannique, le rançongiciel étant le type d'attaque externe, là encore le plus fréquent. Du côté interne, le piratage motivé par un gain personnel domine. Les étudiants apparaissent comme une menace à prendre en compte, non homogène dans ses motivations, et requérant des mesures de prévention et de réponse adaptées.

On distinguera également la notion de « *Shadow IT* » qui désigne l'ensemble des matériels, logiciels, services ou applications cloud utilisés par les collaborateurs d'une organisation sans validation, ni contrôle de la direction des systèmes d'information (DSI). Cette pratique, souvent motivée par des besoins d'efficacité ou de contournement de procédures perçues comme trop rigides, est particulièrement répandue dans les environnements académiques où l'autonomie des chercheurs et des départements est valorisée. Cette menace est aussi souvent liée au manque de ressources ou de solutions officielles adaptées. Il complique la gestion des incidents, en empêchant la DSI d'avoir une vision exhaustive du périmètre à protéger et d'appliquer des mesures préventives globales. Il est difficile de protéger ce dont on n'a pas connaissance. Dans les bibliothèques universitaires, cela peut concerner l'usage de services de synchronisation non autorisés, l'hébergement personnel de bases de données, ou encore

des développements locaux de scripts ou interfaces web. La remédiation de ce type de vulnérabilités passe par un management des actifs, basé sur la devise « *Know your infrastructure* ». Il s'agit de recenser, et suivre l'ensemble des équipements et services utilisés, y compris ceux liés à des processus métiers parfois négligés. Une telle cartographie permet d'identifier les éléments non autorisés, mais aussi de comprendre les interdépendances critiques. D'autre part une sensibilisation des utilisateurs peut réduire les risques liés à ces pratiques pour l'organisation. La prise en compte des besoins réels des utilisateurs lors de la mise à disposition et le développement de solutions peut permettre de ne pas déclencher ce besoin d'alternatives (Entretien -, 2025).

À l'UNIGE, c'est le manque d'alignement entre les objectifs de recherche et les contraintes administratives qui entraîne ces risques. Plusieurs facultés ont la volonté de mettre en place des infrastructures informatiques pour soutenir leurs activités de recherche ou leurs projets d'archivage numérique, nécessitant l'approbation technique et financière de la Division du Système et des Technologies de l'Information et de la Communication (DiSTIC). Cependant, l'absence de budgets transférables entre les facultés et la division conduit cette dernière à refuser son support, même pour des projets jugés pertinents. En conséquence, certaines équipes se tournent vers des solutions alternatives hors supervision centrale. Configurés sans respecter les standards institutionnels en matière de sécurité informatique, ces dispositifs échappent à toute gestion centralisée des accès, des mises à jour et des sauvegardes. Cette situation devient particulièrement critique lorsque ces ressources cessent d'être maintenues, notamment à la fin d'un projet de recherche. En restant opérationnels sans surveillance, ces équipements obsolètes représentent alors un point d'entrée vulnérable sur le réseau institutionnel, ouvrant potentiellement la voie à l'exploitation de failles non corrigées, à l'exfiltration de données ou à l'introduction de logiciels malveillants. Ce sont les risques concrets d'une gouvernance insuffisamment alignée aux besoins opérationnels des unités de recherche, l'essor des problèmes de financement peut alors constituer une fragilité structurelle pour la cybersécurité de l'institution.

Il existe aussi des menaces non intentionnelles qui relèvent de facteurs humains, car la sécurité n'est pas une activité technologique (Ghernaoui 2022), elle est avant tout un enjeu managérial, dépendant de décisions, de comportements et de compétences individuelles. Les personnes peuvent être malveillantes ou les cibles de chantage et de toute sorte de pressions et être à l'origine d'un problème de sécurité. (Ghernaoui 2022). Même des personnes expérimentées peuvent commettre des erreurs techniques, compromettant la disponibilité ou l'intégrité des données. Cela signifie que les données peuvent devenir indisponibles, disparaître ou être diffusées de manière non autorisée. Ces risques internes appellent à une vigilance constante, fondée sur la sensibilisation et l'adoption de bonnes pratiques adaptées au niveau de sensibilité des données.

### **3.3.3 Vulnérabilités liées aux dépendances à des services tiers**

Avec l'adoption croissante des services cloud dans les bibliothèques académiques notamment des systèmes intégrés de gestion de bibliothèques (SIGB) en *Software-as-a-Service* (SaaS) de nouvelles menaces apparaissent. Ces solutions offrent des avantages opérationnels concrets mais introduisent aussi une série de dépendances techniques, contractuelles, économiques, environnementales et même politiques qu'il est important d'évaluer.

D'abord l'architecture cloud induit une dépendance accrue aux infrastructures réseau qui constitue en soi une vulnérabilité critique (Poupard 2018). On peut se questionner sur le devenir de l'accès dans le cas d'une attaque qui constraint l'isolation du réseau du système d'information de la bibliothèque. De plus, ce type de service renforce la centralisation des fonctions critiques auprès d'acteurs tiers, entraînant une dilution du contrôle institutionnel. Cette configuration expose les institutions à une série de risques, parmi lesquels figure la perte de gouvernance sur les données, de la capacité à contrôler leur cycle de vie, leur localisation, leur sécurité ou leur effacement effectif. La gestion s'en retrouve limitée, voire inexisteante, dans certains contextes (CERT-FR 2025).

À travers les dépendances logicielles, une faille ou une compromission chez un tiers peut avoir des répercussions sur l'ensemble d'une organisation. Les attaques de type *supply chain* visent à introduire du code malveillant directement dans des mises à jour logicielles légitimes entraînant une contamination massive de l'ensemble des systèmes clients, à l'échelle internationale (Poupard 2018) comme le cas « *NotPetya* ». Plus récemment l'exemple de *CrowdStrike*, où une erreur dans une mise à jour a généré une instabilité sur les postes Windows à l'échelle mondiale (Browne 2024). Même des solutions réputées sécurisées peuvent devenir des vecteurs involontaires d'attaque. Dans le contexte académique, où les infrastructures dépendent fortement de prestataires, ces risques doivent être intégrés dans les stratégies de sécurité et de continuité d'activité. Le monopole technologique de certains fournisseurs engendre une situation de verrouillage contractuel « *vendor lock-in* ». La migration vers d'autres prestataires ou la réversibilité vers des infrastructures internes deviennent délibérément trop complexes et coûteux (Hastings 2017). Parmi les risques associés à cette dépendance figurent notamment :

- La perte de maîtrise sur les flux d'information et les conditions de traitement
- La difficulté à démontrer la conformité aux exigences réglementaires
- La localisation incertaine des données et la multiplicité des forfaits légaux applicables
- Le risque d'indisponibilité lié à des défaillances réseau ou du fournisseur
- Les priviléges étendus des administrateurs du cloud, susceptibles d'être détournés
- L'impossibilité de mener des audits de sécurité indépendants sur ces environnements
- Les compromissions de l'hébergement mutualisé, si le cloisonnement est insuffisant
- La garantie de l'effacement définitif, traçable des données à la fin de leur cycle de vie (Ghernaouti 2022)

L'Agence nationale française de la sécurité des systèmes d'information (ANSSI) rapporte un niveau élevé de menace cyber sur le cloud (CERT-FR 2025). Les atteintes augmentent en complexité et en intensité, avec des attaquants qui se spécialisent dans le ciblage de ces environnements (Boero 2025a). Une absence de prise en compte de ces enjeux liés à la gouvernance peut conduire à un désengagement progressif des bibliothèques en matière de compétences techniques internes. Ce phénomène peut se traduire par un sous-investissement dans les effectifs spécialisés, une perte de savoir-faire, et une dépendance à l'égard de prestataires externes pour l'exploitation et la maintenance des infrastructures. Cette dynamique, visible dans de nombreuses bibliothèques universitaires britanniques (Bowie 2024), se manifeste par la réduction des équipes techniques et la priorisation de solutions technologiques génériques ou tendances au détriment des systèmes fondamentaux. Sans

clauses contractuelles précises, les modalités d'accès aux données deviennent incertaines et même des contrats solides ne garantissent pas toujours le respect effectif des engagements.

Cette dépendance compromet la souveraineté numérique, d'où la nécessité d'une volonté politique forte, particulièrement dans le secteur public (Ghernaouti 2022). Ce constat concerne aussi les services numériques institutionnels, notamment ceux de Microsoft, utilisés pour le stockage, la bureautique et la communication. Conscients de ces enjeux plusieurs États européens amorcent un virage vers des solutions *open source* et des logiciels libres, pour renforcer leur autonomie stratégique (Serries 2025). Le Conseil d'État Genevois, confronté à un compromis entre pragmatisme et souveraineté, s'est finalement résolu à adopter les applications Microsoft, hébergées sur les serveurs de la firme américaine, assumant cette forme de dépendance technologique (Barbey 2025). L'UNIGE devient elle aussi de plus en plus dépendante<sup>2</sup> de services de la firme comme *SharePoint*.

Face à certaines attaques logiques le choix d'une architecture *cloud-native* apporte aussi des avantages. Les environnements cloud reposent majoritairement sur des accès via API, ce qui limite l'efficacité des techniques de chiffrement utilisées par les *ransomwares* (Chen 2022). Dans ces environnements, les applications sont souvent immuables et éphémères ce qui limite la capacité des *malwares* à s'installer durablement, car toute compromission est effacée dès qu'une instance est recréée à partir d'une image saine. L'intégration de contrôles d'accès (IAM), la gestion des clés de chiffrement et la mise en œuvre de sauvegardes géo redondantes et versionnées renforcent encore cette protection. Si les acteurs malveillants développent progressivement des tactiques adaptées, la combinaison de ces mesures préventives et défensives offre aujourd'hui un haut niveau de résilience face aux scénarios d'attaque (Chen 2022). La responsabilité du client passe alors d'une logique de couverture technique à contractuelle. Le *cloud* facilite la duplication des actifs numériques sur des infrastructures distribuées, mais cela nécessite une approche réfléchie pour garantir leur disponibilité en cas de crise (Hastings 2017). Le tableau de veille publié par le CERT-FR montre la diversité et l'ampleur des menaces de ces environnements : compromissions de services SaaS, latéralisations entre environnements *on-premise* et cloud, attaques contre les chaînes d'identité et d'accès, exploitation d'API légitimes à des fins malveillantes, ou utilisation même des infrastructures cloud pour héberger ou pour exfiltrer des données sensibles (CERT-FR 2025; Boero 2025a).

Parmi les mesures prioritaires à mettre en œuvre pour renforcer la résilience des systèmes en nuages face aux cybermenaces figurent la planification d'un Plan de Continuité d'Activité (PCA) et d'un Plan de Reprise d'Activité (PRA), l'adoption des bonnes pratiques de prévention contre les attaques par déni de service, ainsi que l'utilisation systématique des options de sauvegarde sécurisée proposées par les prestataires, lorsque disponibles (CERT-FR 2025). On notera également :

- La gestion des identités et des accès avec l'activation de l'authentification multi facteur (MFA) pour l'ensemble des comptes administratifs et une révision régulière des droits d'accès selon le principe du moindre privilège.

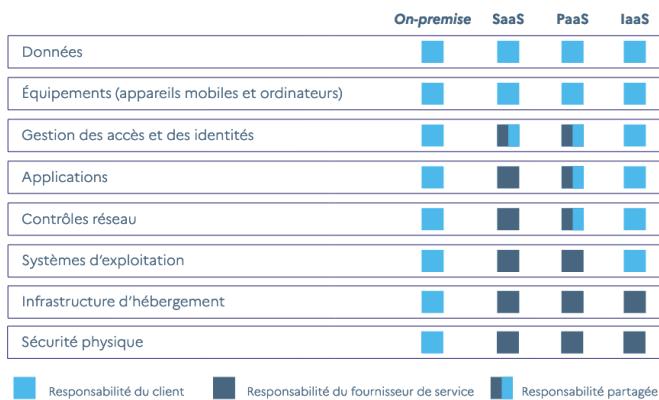
---

<sup>2</sup> Un indice de résilience numérique (IRN), en cours de développement par plusieurs entreprises françaises, combine l'évaluation des prestataires cloud avec l'analyse de la culture organisationnelle (Lemonnier 2025).

- La détection proactive des comportements anormaux. L'analyse des journaux d'accès (logs) fournis par le prestataire SaaS, intégrés dans un système de supervision (SIEM).
- La robustesse de la politique de sauvegarde qui doit être réalisées de façon sécurisée sur des environnements isolés, et la capacité de restauration des données critiques validée régulièrement au travers de tests.
- Enfin, le contrôle de la configuration du SIGB et de son exposition réseau. Seules les interfaces et API strictement nécessaires doivent être exposées, avec un chiffrement systématique des flux.

Ces dispositifs doivent être complétés par une sensibilisation des équipes, en particulier face aux risques de phishing, de manipulation de données et une procédure de remontée des incidents doit être diffusée pour une réponse rapide en cas d'attaque (CERT-FR 2025).

Figure 4 - Responsabilité selon la configuration du service en nuage



(CERT-FR 2025)

Pour un SIGB en mode SaaS, il est essentiel d'identifier les données critiques et de s'assurer que le fournisseur applique des stratégies de sauvegarde multisites, avec des garanties contractuelles sur la redondance et la portabilité des données (Hastings 2017). La migration vers le cloud est souvent perçue à tort comme un transfert complet de responsabilité (Figure 4), mais les organisations restent, en réalité, garantes des données externalisées (Ghernaouti 2022). Cette délégation s'accompagne souvent d'une dilution des compétences internes, un coût élevé pour un service généralement bien sécurisé. L'externalisation dans le cloud représente une réponse pragmatique aux contraintes budgétaires et organisationnelles, mais n'exonère en rien les institutions de leurs responsabilités.

La Bibliothèque doit compléter ces dispositifs par des sauvegardes indépendantes, isolées du cloud principal et tester régulièrement la capacité de restauration. La supervision des services cloud doit inclure des mécanismes d'alerte en cas d'anomalie ou d'indisponibilité (monitoring des API, suivi des temps de réponse, analyse des logs). Par ailleurs, ces dépendances techniques et contractuelles doivent être inventoriées, afin de disposer d'un plan de repli en cas de défaillances, intégré dans un PCA et aligné avec la politique de gestion de la continuité d'activité de l'UNIGE (UNIGE 2021b).

La dépendance place les institutions dans une relation contractuelle asymétrique, souvent encadrée par des conditions imposées. Dans le cas du SIGB Alma, distribué par Ex Libris cette dépendance prend une dimension commerciale forte, limitant l'accès direct aux métadonnées de gestion et réduisant la marge de manœuvre des équipes, aussi en raison

d'une gouvernance éclatée entre bibliothèques coordonnées par Swiss Library Service Plateforme (SLSP). L'accès aux journaux d'activité est aussi limité, empêchant les institutions de réaliser des audits de sécurité et compromettant leur autonomie. Si les accords de niveau de service (SLA) définissent des seuils d'indisponibilité, il est impératif de prévoir la continuité en cas de dépassement.

### 3.3.4 Vulnérabilités liées aux dépendances aux éditeurs scientifiques

La disparition progressive de notre patrimoine culturel numérique est accélérée par la domination des plateformes et des modèles de diffusion temporaires régis par les intérêts commerciaux. En cas de rachat, de faillite ou même de simple repositionnement commercial, un fournisseur peut retirer des milliers de titres inopinément et effacer une part de la mémoire scientifique mondiale faute de véritables copies pérennes (Pasteur 2024). La préservation numérique est garante de la persistance des liens et des citations, notamment par le biais du système des identifiants numériques pérennes comme le Digital Object Identifier (DOI) (Polchow 2021). Pourtant, une analyse sur plus de 7,4 millions de publications montre que 27,64 % de ces objets numériques ne semblent faire l'objet d'aucune mesure de préservation dans les archives étudiées. Plus inquiétant encore, près d'un tiers des membres de Crossref (32,9 %) n'assurent aucune préservation numérique identifiable, en contradiction avec les recommandations de la *Digital Preservation Coalition* (DPC) (Eve 2024).

Au-delà des menaces globales, certaines indisponibilités ponctuelles mais significatives peuvent affecter les services numériques essentiels des bibliothèques universitaires, contraignant l'accès et le bon déroulement des activités courantes. Ainsi, une interruption d'accès peut découler d'un changement administratif ou technique comme ce fut le cas avec les modifications d'adresses IPs aux Hôpitaux Universitaires de Genève (HUG). Ces adresses, préalablement enregistrées auprès des éditeurs conformément aux accords contractuels<sup>3</sup>, conditionnent l'accès aux ressources électroniques de l'UNIGE. Leurs modifications non communiquées avaient coupé les HUG de tout accès aux ressources scientifiques.

La cessation brutale des activités de l'éditeur Editores Medicorum Helveticorum (EMH) en 2024 est révélatrice de cette dépendance aux éditeurs. Fondée en 1997 sous l'impulsion conjointe de la Fédération des médecins suisses et de Schwabe, EMH<sup>4</sup> s'était imposée comme un acteur de la communication scientifique dans le domaine médical. La décision unilatérale de la FMH, actionnaire majoritaire, de retirer son soutien a précipité la faillite d'EMH, qui a officiellement déposé le bilan (Joelving 2024). Cette décision a provoqué une discontinuité brutale d'accès au savoir médical suisse, interrompant les parutions mais aussi l'accès aux archives numériques et la fermeture immédiate du site swisshealthweb.ch. Au-delà de l'incident économique, cette faillite questionne sur la vulnérabilité des écosystèmes éditoriaux spécialisés, lorsque ceux-ci dépendent d'un modèle de gouvernance déséquilibré et d'une vision strictement comptable de l'édition scientifique numérique.

Face à cet événement, seule la résilience documentaire mutualisée fondé sur l'archivage pérenne distribué a permis de préserver une partie de ce patrimoine scientifique. Contacté à

---

<sup>3</sup> L'UNIGE et les HUG sont liés par un contrat de service pour la fourniture de l'accès aux ressources électroniques au personnel soignant.

<sup>4</sup> Elle assurait la diffusion de titres comme le *Swiss Medical Forum*, *Primary and Hospital Care* ou *Swiss Archives of Neurology, Psychiatry and Psychotherapy*. Cette dernière revue, une publication citée pour avoir accueilli les écrits de figures comme Jung ou Foucault.

la suite de la découverte de l'indisponibilité, les administrateurs de l'archive CLOCKSS, ont activé les mécanismes de sauvegarde d'urgence, et ont permis de rendre librement accessibles les archives de trois des six revues affectées (pour la période 2016–2024) (CLOCKSS 2025). L'organisation a débuté un processus de reconstruction par la sollicitation des collections physiques détenues par des bibliothèques partenaires. La soudaineté et la portée de ce type d'événements justifient la problématique liée à la fragilité du patrimoine scientifique ainsi que la thèse de l'importance stratégique des infrastructures d'archivage pérenne et des alliances institutionnelles pour éviter ce que certains appellent un « épistémicide » (WAME, 2025). Ce n'est pas sans rappeler la fermeture de la plateforme de livres électroniques Dawsonera<sup>5</sup> en juillet 2020 révélant les vulnérabilités du modèle d'accès dans l'édition académique (Entretien Y.Grandcolas, 2025). Comme beaucoup de choses importantes que nous tenons pour acquises, nous ne connaissons pas leur vraie valeur jusqu'à ce qu'elles nous soient enlevées (Lindström, Spirkina 2024).

*ProQuest Ebook Central* est actuellement au cœur d'une controverse en raison de changements significatifs dans son modèle économique et ses modalités d'acquisition. En 2025, *ProQuest*, propriété de *Clarivate*, a annoncé la fin de certains modèles d'acquisition de livres électroniques, notamment l'achat perpétuel, l'acquisition basée sur la demande (DDA) et l'acquisition basée sur les preuves (EBA). Ces décisions suscitent des préoccupations des professionnels qui craignent à nouveau une dépendance aux abonnements et une perte de contrôle sur la constitution de leurs collections comme ce fut le cas lors du passage aux modèles de bouquet de journaux par les éditeurs *for-profit* (Caraco 2019).

Cet exemple nous recentre sur l'enjeu central des archives distribuées et de l'archivage pérenne des revues scientifiques numériques (Beagrie 2013). « Assurer la conservation des revues scientifiques numériques et leur accessibilité à long terme relève d'une action concertée, coordonnée et durable de la part de multiples intervenants. » (Alexandre 2015). La complémentarité entre bibliothèques et éditeurs devient essentielle. Les premières visent à garantir l'accès dans le temps, tandis que les seconds souhaitent préserver leurs modèles économiques. L'intervention d'un tiers garant de l'intégrité archivistique permet de concilier ces objectifs parfois divergents, tout en limitant les risques de défaillance individuelle. La pérennité des ressources électroniques repose alors moins sur des solutions techniques que sur une sécurisation contractuelle. Il est impératif d'inscrire dans les contrats des garanties tangibles. Des scénarios de sortie explicites, une adhésion à des réseaux d'archivage distribués tels que Portico, CLOCKSS, une clause de succession technologique garantissant la remise des fichiers et métadonnées à un tiers de confiance en cas de défaillance ainsi que l'intégration de l'éditeur à une « *dark archive* », deviennent des conditions minimales. À défaut, chaque faillite ou fusion d'éditeur risque d'entraîner la perte irréversible de pans entiers de la mémoire scientifique. Une telle base contractuelle permet d'anticiper les ruptures, de guider les arbitrages documentaires et de soutenir une stratégie de continuité. En l'absence de clauses de succession technologique, d'exports réguliers ou de miroirs locaux, les bibliothèques se retrouvent captives d'accords commerciaux dont elles ne maîtrisent ni la durée ni les conditions de retrait. À terme, cette dépendance fait peser un double risque. Patrimonial d'une part du à la disparition irréversible d'articles, jeux de données ou

---

<sup>5</sup> Dawsonera, exploitée par Dawson Books, était une plateforme majeure, offrant un accès à des milliers d'e-books pour les bibliothèques universitaires et a cessé ses activités rendant l'ensemble des contenus inaccessibles du jour au lendemain.

monographies qui documentent l'évolution des connaissances. Opérationnel et réputationnel d'autre part qui porte atteinte à la confiance et la perte de crédibilité des établissements incapables d'assurer un accès ininterrompu.

### 3.3.5 Instabilités liées aux évolutions technologiques et géopolitiques

Les objets numériques sont intrinsèquement fragiles et soumis à de multiples formes de dégradation qui s'accentuent avec le temps. L'un des risques les plus pernicieux est l'altération silencieuse des données, ou *bit-rot*, la corruption d'un seul bit peut rendre un fichier totalement illisible. À cela s'ajoutent l'obsolescence des formats, des logiciels et des supports de stockage, qui peut empêcher l'accès aux fichiers (Rosenthal et al. 2005). Ces menaces s'inscrivent dans un environnement technique où les changements fréquents de systèmes, multiplient les risques de perte ou de corruption (Tableau 2). La préservation numérique repose sur une infrastructure vulnérable à des défaillances matérielles, des erreurs logicielles, des interruptions réseau ou des failles dans les processus (Barateiro et al. 2010).

Tableau 2 - Typologie des menaces et vulnérabilités des systèmes de préservation

Vulnerabilities	Process	Software faults Software obsolescence
	Data	Media faults Media obsolescence
	Infrastructure	Hardware faults Hardware obsolescence Communication faults Network service failures
	Disasters	Natural disasters Human operational errors
	Attacks	Internal attacks External attacks
	Management	Economic failures Organizational failures
	Legislation	Legislative changes Legal requirements

(Barateiro et al. 2010)

Les stratégies de réponses combinent la migration régulière des formats, l'émulation des environnements d'origine, la redondance géographiquement distribuée des copies, et la diversification des technologies. Le maintien de métadonnées techniques, l'audit régulier de l'intégrité des fichiers et la mise à jour proactive des infrastructures sont également nécessaires pour anticiper les défaillances et garantir l'accès pérenne aux contenus (Barateiro et al. 2010). À mesure que les technologies évoluent, les méthodes de stockage changent, laissant parfois de côté des informations jugées secondaires à l'époque mais dont la valeur n'est pleinement comprise que lorsqu'elles deviennent inaccessibles. Enfin, les risques de nature organisationnelle ou réglementaire, tels qu'une gouvernance déficiente ou un changement législatif, rappellent que la résilience ne peut se limiter à des solutions techniques, et nécessite d'intégrer les dimensions humaines, juridiques et stratégiques.

Dans une étude sur la disparition des revues scientifiques en *Open Access*, des chercheurs ont révélé que 174 revues, couvrant l'ensemble des grandes disciplines de recherche et des régions du monde, ont disparu d'internet entre 2000 et 2019 (Laakso, Matthias, Jahn 2021). Cette disparition s'explique par l'absence d'archives ouvertes, complètes et accessibles. Une autre analyse de 2015 portant sur 326 bases de données en biologie a montré que plus de 60 % d'entre elles avaient disparu, étaient devenues non fonctionnelles ou ne disposaient plus que de fonctionnalités limitées (Attwood, Agit, Ellis 2015).

Il devient tout aussi important d'élargir l'analyse à des risques de nature politique et idéologique. Les bibliothèques sont aussi des symboles de liberté intellectuelle, parfois

attaqués pour des raisons politiques (Martel 2025; Lankes 2025). Les exemples récents de censure, de réécriture de l'histoire, et de pression idéologique sur les institutions culturelles montrent que les contenus numériques peuvent être délibérément modifiés, supprimés ou rendus inaccessibles non pas pour des raisons techniques, mais pour des motifs de contrôle symbolique. La suppression de contenus relatifs au changement climatique, à la santé publique ou aux inégalités sociales constitue une entrave à la transparence démocratique, à la liberté académique et à l'élaboration de politiques publiques éclairées. Cette disparition de données officielles, qualifiée d'« autodafé numérique » (Genevois 2025), remet en question l'accès au savoir et menace également les fondements de la recherche scientifique et du débat démocratique. Ces événements suscitent de plus en plus d'inquiétudes quant à la pérennité des ressources électroniques, des données scientifiques (Strecker et al. 2023) et des sites web institutionnels (Rivero 2024)(Genevois 2025). Cela génère une perte de confiance et un climat de méfiance envers les autorités, accentuant les fractures sociales et idéologiques.

Selon Dorothea Strecker, chercheuse en gestion des données de recherche à l'Université Humboldt de Berlin « La fermeture des dépôts constitue une réelle menace pour la disponibilité perpétuelle des données de recherche » (Strecker et al. 2023). La communauté scientifique alerte sur les failles persistantes dans les dispositifs actuels de préservation. Les équipes en charge des dépôts numériques sont encouragées à mettre en place des plans de contingence, incluant des réseaux de secours entre dépôts et des services d'archivage pérenne, afin de garantir l'accès à long terme aux contenus. Une étude de 2023 révèle que, sur plus de 3 000 dépôts de données, 191 avaient fermé, dont près de la moitié sans transfert de responsabilité, suggérant une perte définitive des données (Hedley 2025). Même les grands dépôts restent vulnérables, comme l'a illustré la panne de PubMed en mars 2025 (Mallapaty 2025a; 2025b). Jonas Recker, archiviste à l'Institut Leibniz, alerte sur le manque d'anticipation des fermetures causées par des pertes de financement ou des changements de mission (Hedley 2025).

Au-delà du périmètre des bibliothèques qui sont des points d'accès à un écosystème d'information plus large, d'autres infrastructures également à risque, jouent un rôle essentiel dans l'accès à l'information scientifique. L'incertitude entourant les données de recherche hébergées ou produites aux États-Unis suscite des inquiétudes au sein de la communauté scientifique suisse, notamment quant à la nécessité d'anticiper des solutions de sauvegarde pour en assurer la continuité et la préservation (Minet 2025). Certaines ne sont pas gérées directement par les bibliothèques cependant, elles forment avec elles, un écosystème critique pour la science avec des conséquences concrètes allant bien au-delà du monde de la recherche<sup>6</sup>. Bien qu'elles ne se limitent pas à l'accès à la littérature, elles en dépendent, et révèlent la synergie entre données et publications (Entretien P.Ruch, 2025).

Ces faits appellent à une approche collaborative de la préservation, où les dépôts s'aligneraient avec des structures similaires. En Allemagne, une « checklist de cessation » est en cours de développement pour formaliser le transfert de données vers d'autres dépôts, via des protocoles d'accord (Hedley 2025). Les coupures de financements menacent aussi les sphères des communs numériques scientifiques de la cybersécurité comme l'arrêt des

---

<sup>6</sup> Une étude du Secrétariat d'État à la Formation et à l'Innovation SEFRI est en cours sur les risques relatifs à la protection contre les pertes de données de recherche et des services fournis par des pays extra-européens (Minet 2025).

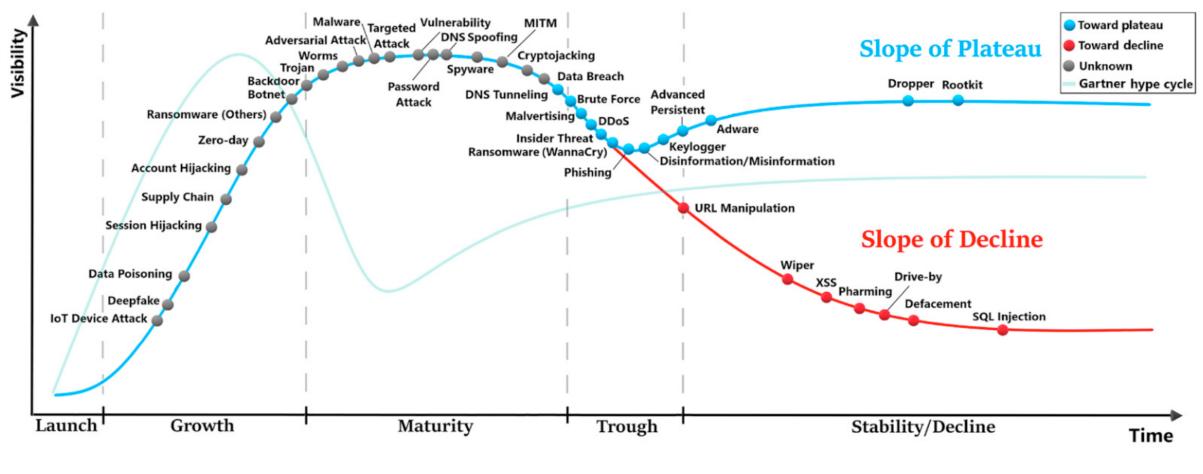
financements de la base CVE MITRE, et contrainte de se muer en fondation pour la poursuite de ses activités pourtant essentielles (Solomon 2025).

Ces situations marquent le maillage que forment les bibliothèques, les centres de recherche, les communautés *Open Data* et les communs numériques dans un écosystème informationnel mondial dont la fonction centrale est d'assurer la pérennité, l'intégrité et l'accessibilité des données scientifiques. La collaboration doit être une composante constructive des moyens de remédiations. Le recours à des systèmes distribués, des copies multiples, des formats ouverts, et à des dépôts sécurisés hors de l'infrastructure principale, apparaît comme un levier de résilience, de résistance intellectuelle face à des logiques de contrôle ou d'effacement.

### 3.3.6 Dynamiques émergentes et déplacement de la menace

« La présence d'une vulnérabilité n'entraîne pas de dommage en elle-même, puisque la présence d'une menace est nécessaire pour l'exploiter. Une vulnérabilité à laquelle ne correspond aucune menace peut ne pas exiger la mise en œuvre d'une mesure de sécurité, mais il convient qu'elle soit identifiée et surveillée en cas de changements. » (ISO 2018).

Figure 5 - Projection des tendances d'attaques informatiques



(Almahmoud et al. 2023a)

La figure 5 présente un modèle prédictif inspiré du *Gartner Hype Cycle*, appliqué aux cyberattaques basées sur l'analyse de données massives via l'apprentissage automatique. Du lancement au déclin il anticipe l'évolution de 42 types d'attaques (Almahmoud et al. 2023a).

La désinformation constitue désormais une menace reconnue dans le champ de la cybersécurité, en tant que problème sociétal et politique, mais également comme une forme d'attaque exploitant les vulnérabilités cognitives humaines. Les exemples récents montrent l'ampleur des campagnes de désinformation avec des impacts concrets sur la société, la santé et la sécurité publique (Caramancion et al. 2022). Récemment l'Agence de l'Union Européenne pour la Cybersécurité (ENISA) l'a formellement intégrée parmi les huit principales catégories de menaces cyber (ENISA 2024) elle affecte la confidentialité, l'intégrité et la disponibilité de l'information par le biais d'un « hacking cognitif » (Caramancion et al., 2022). La désinformation vise à manipuler l'opinion publique par la diffusion de contenus faux ou biaisés et exploite des vulnérabilités psychologiques de la même manière que les attaques informatiques exploitent des failles techniques. Elle agit de manière discrète et persistante, échappant aux défenses classiques, et génère un impact supérieur sur l'opinion publique, la

stabilité des institutions ou la confiance dans ses services (ENISA 2024). Intégrer la désinformation dans les référentiels de gestion des risques cyber en bibliothèque est plus que légitime. Reconnues comme des institutions de confiance, garantes de l'information vérifiée, elles peuvent involontairement devenir des vecteurs d'amplification si leur réputation est instrumentalisée pour légitimer des contenus trompeurs. Il s'agit de défendre l'intégrité informationnelle des citoyens et des organisations dans un espace numérique saturé de récits falsifiés (ENISA 2024).

Les avancées de l'intelligence artificielle (IA) ont ouvert une nouvelle ère technologique et soulèvent des défis en matière de cybersécurité. Les capacités de l'IA générative comportent des risques en facilitant la création de codes malveillants et en amplifiant le potentiel des cyberattaques (ESRI 2024). D'un côté, elle est utilisée par les acteurs malveillants pour automatiser des actions offensives telles que le scan de réseaux, l'exploration d'architectures systèmes, ou encore des attaques de type phishing, d'ingénierie sociale ou d'hypertrucage. On relève notamment le «*IA poisoning* », une technique d'attaque exploitant la dépendance des développeurs envers les assistants de code (Korben 2025). En contaminant les jeux de données d'entraînement utilisés, des acteurs malveillants peuvent introduire des portes dérobées invisibles dans le code généré. L'apprentissage automatique de certains modèles peuvent aussi apprendre à contourner les règles explicites pour maximiser une métrique, au détriment de la sécurité. Cela ouvre la voie à des comportements non anticipés, notamment dans les systèmes auto-adaptatifs (Kucharavy et al. 2024). Ces usages renforcent l'efficacité des attaques et deviennent une considération croissante pour les systèmes de défense. La stratégie nationale suisse de cybersécurité, analyse en profondeur ces menaces, propose des mesures de mitigation mais intègre aussi les LLM dans les stratégies de défense numérique via une adoption responsable (Kucharavy et al. 2024).

De l'autre côté, l'IA constitue un outil stratégique pour la détection et la défense. Dans le contexte où les systèmes génèrent des volumes massifs de données, elle offre une capacité d'analyse augmentée en permettant, l'identification d'anomalies sur les réseaux ou le pré-tri d'alertes de sécurité (Entretien -, 2025). L'objectif est d'anticiper les attaques des années à l'avance, d'adopter des mesures et d'allouer efficacement leurs ressources (Almahmoud et al. 2023b). Cette automatisation partielle permet de soulager les analystes humains et de réagir plus rapidement à des menaces complexes (Entretien F.Petit, 2025). En mobilisant l'apprentissage automatique (Perrod 2023) les organisations peuvent détecter les tendances et les compromissions futures. Cette technologie instille une pression liée à l'activité de bots automatisés chargés de collecter massivement du contenu pour l'entraînement de modèles. Les sites web, les bases de données, les archives ouvertes subissent un trafic anormalement élevé pouvant perturber voire paralyser la disponibilité de ces ressources. Les «*bots IA* » ciblent des contenus riches et actualisés, pour alimenter les systèmes génératifs (Kwon 2025). Cette situation touche particulièrement les dépôts en libre accès, où la philosophie d'ouverture se heurte à des pratiques d'extraction (*scraping*) intensif et menace leur stabilité technique. Selon une enquête de la *Confédération of Open Access Repository*, plus de 90 % des membres interrogés ont subis des tentatives de *scraping* par IA, dont les deux tiers ont connu des interruptions de service (COAR 2025). Face à cela, les éditeurs et hébergeurs tentent de mettre en place des solutions techniques (Burnel 2025). L'enjeu réside dans l'équilibre délicat entre le filtrage des bots et l'accès légitime via des réseaux universitaires.

Cette situation interroge l'aspect juridique et réglementaire de cette exploitation. En juin 2025, « la justice américaine a donné raison à Meta dans une affaire de droit d'auteur liée à l'entraînement de son IA, jugeant l'usage des œuvres raisonnable » (swissinfo.ch 2025). Plusieurs acteurs, comme l'éditeur Wiley, appellent à la nécessité d'une autorisation explicite pour ce type d'usage. En l'absence de telles mesures, les ressources scientifiques risquent de devenir à la fois surexploitées et fragilisées, compromettant leur pérennité (Kwon 2025). La récente initiative de *Cloudflare* pour bloquer par défaut les robots d'exploration IA et à proposer un modèle économique « *Pay Per Crawl* » peut être une réponse aux problématiques de captation non régulée (Burnel 2025). Elle ouvre la voie à une monétisation des contenus et pourrait contribuer à soutenir financièrement la préservation numérique, en redirigeant une partie des revenus générés vers les institutions productrices de contenus patrimoniaux ou scientifiques. En mai 2025, ce même fournisseur a neutralisé l'attaque DDoS la plus intense jamais enregistrée (7,3 Tbits par seconde). Un exemple de l'augmentation massive du trafic automatisé sur Internet qui accroît la surface d'exposition des services numériques face aux attaques volumétriques et aux surcharges réseau (Boero 2025b). En 2024, le trafic Internet généré par des bots a dépassé celui d'origine humaine (51 % du total). L'IA aide aussi des acteurs malveillants à déployer des bots à grande échelle. Les attaques DDoS et l'exploitation des API sont particulièrement touchées, 44 % du trafic des bots cible désormais ces interfaces. Les secteurs comme l'enseignement supérieur ou la santé sont particulièrement exposés et la qualité de service est dégradée par surcharge et interruption (Imperva 2025).

Une menace souvent sous-estimée sur le registre scientifique est son exposition aux risques environnementaux liés au changement climatique. K. Pendergrass, archiviste à Harvard, désigne dans ses travaux les coûts écologiques de la préservation numérique et alerte sur le fait que le dérèglement climatique compromet à la fois la conservation des supports numériques et analogiques. Malgré son ampleur, cette problématique demeure insuffisamment prise en compte, contrairement à d'autres préoccupations environnementales mieux intégrées. Il faut faire un choix de valeur concernant ce qui doit être sauvagardé et conservé, soutenant que tout ne peut ni ne doit être archivé indéfiniment. La mémoire scientifique repose sur une sélection raisonnée des contenus (Hedley 2025).

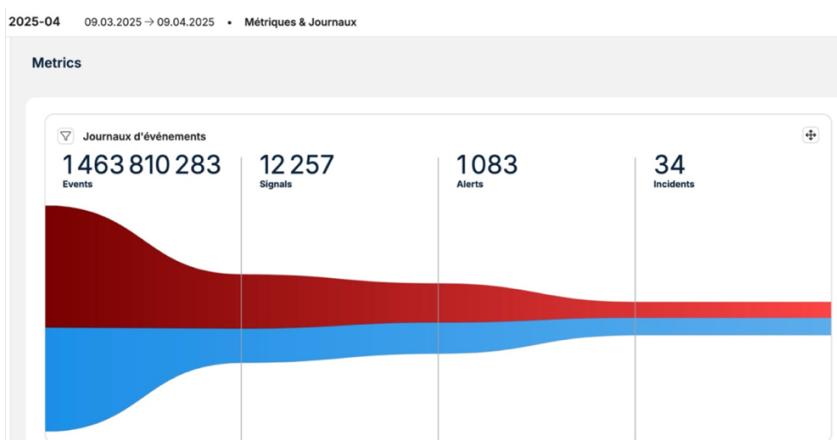
Les conflits armés modernes constituent également une atteinte directe pour le patrimoine et les infrastructures culturelles. Les bibliothèques et les archives, sont souvent les premières victimes collatérales des guerres. La destruction physique est couplée à la perte d'infrastructures numériques (Smithers 2025a). Depuis le début de la guerre en Ukraine, l'UNESCO recense une destruction de onze bibliothèques endommagées sur un total de 236 sites culturels touchés (2023). Ces atteintes concernent à la fois des bibliothèques centrales, scientifiques et régionales (Читомо 2022; Martinez 2023). La législation Ukrainienne impose aux éditeurs scientifiques de déposer les publications dans le dépôt légal de la Bibliothèque nationale Vernadsky. Cette infrastructure centralisée héberge actuellement plus de 1,43 million d'articles uniques. Cependant, sans redondance suffisante, en cas de sinistre ou d'attaque ciblée sur ses serveurs, l'intégralité de ces contenus pourrait être irrémédiablement perdus. D'après les données du *Directory of Open Access Journal* (DOAJ), seulement 14,8 % des revues indexées en Ukraine sont archivées via des réseaux pérennes identifiés par le *Keepers Registry* (Zimba et al. 2025). Dans ce contexte, l'accès aux collections électroniques ne constituent pas une priorité, mais cette situation traduit une vulnérabilité critique de préservation à long terme (Zimba et al. 2025). Sur le plan patrimonial, la mutualisation et la duplication distribuée des ressources numériques apparaissent comme l'unique rempart

contre la perte irrémédiable de savoirs en cas de destruction physique des infrastructures (Smithers 2025a). Dans le reste de l'Europe on assiste à une recrudescence des tentatives d'intrusions. L'augmentation des attaques opportunistes et ciblées, amplifiées par le contexte géopolitique impose également le respect d'obligations fédérales et cantonales, notamment sur le filtrage des flux réseau provenant de régions à risque (Entretien P.L'Hostis, 2025).

### 3.4 Stratégies de cybersécurité à l'échelle institutionnelle

Dans le cadre de sa stratégie de cybersécurité, l'UNIGE s'appuie sur un centre de cyberdéfense opéré en partenariat avec ses services internes et ses prestataires. Le dispositif, intègre un Security Operations Center (SOC) et assure une supervision centralisée et en temps réel des événements de sécurité sur le système d'information universitaire.

Figure 6 - Événements sur le réseau de l'UNIGE sur une période d'un mois



(SSI UNIGE, 2025)

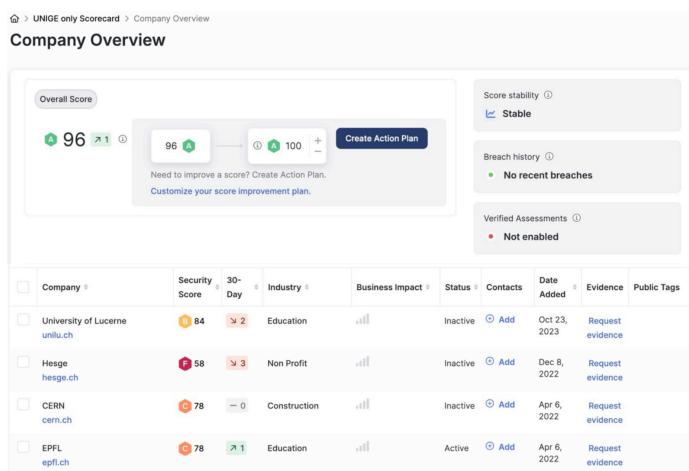
Grâce à des outils de collecte, corrélation et analyse automatisée des logs et des incidents, le SOC permet la détection précoce des menaces et d'accélérer la capacité de réponse face aux cyberattaques. La Figure 6 montre le traitement des événements remontés dans le SOC sur une période d'un mois. Elle témoigne de la persistance et de la fréquence élevée des éléments à traiter. En complément, l'UNIGE déploie une stratégie de surveillance des vulnérabilités, couvrant les applications web et les systèmes d'exploitation exposés sur Internet. Cette supervision s'appuie sur des outils automatisés et des scans réguliers ciblés sur les périmètres sensibles (UNIGE 2018). Elle permet d'identifier et de prioriser les actions de remédiation. L'équipe de sécurité réalise également, des tests d'intrusion (*pentests*) sur des systèmes critiques ou à fort enjeu. Ces audits techniques complètent la surveillance continue et permettent de vérifier la résilience des dispositifs face à des scénarios d'attaques réalistes (Entretien P.L'Hostis, 2025). La sécurisation des communications web repose sur une politique de gestion des certificats électroniques TLS<sup>7</sup>. Les sites publics ou liés à l'image de l'UNIGE sont protégés par des certificats *Extended Validation* (SWITCHpki/QuoVadis), qui garantissent un haut niveau de confiance. Les services internes à usage restreint privilégient l'usage de certificats *Let's Encrypt*, permettant un déploiement rapide et automatisé (UNIGE 2018).

---

<sup>7</sup> Le protocole TLS (anciennement SSL) sécurise les échanges sur Internet en assurant l'authentification du serveur, la confidentialité et l'intégrité des données. Utilisé dans le protocole HTTPS, en client-serveur sans modifications des protocoles applicatifs.

L'UNIGE met en œuvre une gestion renforcée des accès privilégiés via un bastion informatique. Ce dispositif centralise et sécurise les connexions distantes nécessaires à l'administration des systèmes critiques par les prestataires et les administrateurs. Il impose une authentification forte, trace l'intégralité des sessions, et limite strictement les accès accordés. Le bastion constitue ainsi une protection contre les risques liés aux comptes à priviléges, fréquemment ciblés dans les cyberattaques avancées. La stratégie s'inscrit dans une logique de défense en profondeur, des mécanismes de prévention, de protection des accès critiques, de détection proactive, de tests de robustesse et de traçabilité renforcée. Cette approche vise à réduire les risques résiduels en s'assurant qu'aucune barrière isolée ne constitue un point unique de défaillance.

Figure 7 - Score de posture de sécurité de l'UNIGE et d'institutions similaires



(SSI UNIGE, 2025)

Actuellement, le score de la protection de la surface d'attaque externe de l'UNIGE obtient 96 sur 100 (Figure 7) via une évaluation externe indiquant une posture de cybersécurité maîtrisée en comparaison à la moyenne du secteur académique. En effet l'UNIGE déploie des défenses fortes, recommandées à de multiples reprises dans la littérature. La participation régulière à la veille nationale permettent aussi une adaptation continue des dispositifs. Des initiatives spécifiques sont en place, comme la présence d'un expert dédié aux questions de sécurité des données sensibles de recherche et précise l'effort mené pour sécuriser les échanges d'informations sensibles, même si les bibliothèques restent globalement moins exposées à ces enjeux spécifiques (Entretien P.L'Hostis, 2025). La protection des actifs informationnels repose sur une gestion des accès et des flux réseau. Alors que les réseaux universitaires adoptaient autrefois une politique permissive, ils s'orientent désormais vers une approche restrictive. Tout est bloqué par défaut, et seuls les accès strictement nécessaires sont autorisés. Toutefois, des flux légitimes peuvent être détournés à des fins malveillantes, notamment pour exploiter des failles applicatives ou systèmes. La stratégie de sécurité repose ainsi sur une classification des actifs selon leur criticité, un suivi permanent des vulnérabilités, l'identification des serveurs obsolètes et une vigilance forte face aux menaces de type « Zero-Day ». D'autres mesures préventives s'appuient sur des standards reconnus, tels que le « OWASP Top 10 »<sup>8</sup> (OWASP 2021) pour établir les directives de sécurité afin de promouvoir

<sup>8</sup> L'Open Worldwide Application Security Project est une organisation internationale de référence dans le domaine de la sécurité. Son Top 10, recense les principales vulnérabilités web, sur la base de données d'audits de sécurité et d'avis d'experts.

une approche « *secure by design* » dans le développement des applications (UNIGE 2017). Ces bonnes pratiques visent à limiter les vulnérabilités les plus fréquentes dès la phase de conception. L'enjeu de sécurité pour la Bibliothèque réside principalement dans la disponibilité et l'intégrité des données. Si une indisponibilité temporaire constitue un obstacle à la continuité de service et à la qualité d'accès pour les usagers, elle reste, dans un temps raisonnable, surmontable. En revanche, la perte définitive qu'elle soit causée par une cyberattaque, une défaillance technique ou une mauvaise stratégie de préservation représente une atteinte grave à la mémoire scientifique. Cela compromet l'accès pérenne aux savoirs, la mission documentaire des bibliothèques et leur responsabilité vis-à-vis de la communauté académique. Quels que soient la persistance et l'impact de l'atteinte, ces dysfonctionnements entame la confiance des tiers de confiance dans l'espace numérique (Poupard 2018).

Le traitement de ces menaces passe par l'application de standards minimaux de sécurité informatique mis en œuvre dans la directive de « Gestion de la continuité d'activité - Sécurité de l'information » (UNIGE 2021b), l'application de la classification sur la sensibilité des données (cf Tableau 4 p.47 ) et d'une approche spécifique lorsque les projets impliquent des données réglementées exigeant des mesures complémentaires. L'efficacité de ces directives reposent sur une collaboration entre les équipes techniques centrales et les équipes métier, permettant d'adapter les référentiels de sécurité aux spécificités des différents contextes. À notre niveau du SI, un registre des actifs informationnels devient nécessaire pour distinguer les services internes des services externalisés, mieux maîtriser la continuité opérationnelle et envisager une révision périodique des plans de continuité et des services numériques critiques à travers une analyse d'impact. Les entretiens internes (Annexe 7) révèlent que cette démarche demeure inachevée. Certains métiers n'ont pas été associés au processus, et le service de sécurité informatique n'a pas bénéficié des retours d'expérience qu'aurait pu offrir cette analyse. Or, les résultats obtenus pour d'autres services prouvent l'intérêt manifeste, pour l'ensemble des parties prenantes, de reconduire une telle approche.

### 3.5 Évaluation de la résilience informationnelle

Une évaluation croisée de la maturité en matière de préservation numérique et de sécurité de l'information a été menée après l'évaluation des besoins de la Division de l'Information Scientifique (DIS) de l'UNIGE. L'objectif est de diagnostiquer les pratiques actuelles, d'identifier les points de vulnérabilité et de proposer une trajectoire d'amélioration pour la Bibliothèque. Baptisé « RAMSID » pour Référentiel d'Analyse de la Maturité de la Sécurité du Systèmes d'Information Documentaire elle évalue la situation actuelle et détermine des axes de progression sur les écarts identifiés dans la revue de littérature et la conduite des entretiens pour la démarche de sécurité. La matrice est conçue à partir de deux référentiels combinés :

- le *Digital Preservation Coalition Rapid Assessment Model* (DPC 2024a), spécifiquement conçu pour les institutions, bibliothèques, archives, musées etc.
- le NIST Cybersecurity Framework (CSF) 2.0 Maturity Tool (NIST 2024), pour évaluer les pratiques de cybersécurité dans les organisations complexes.

L'adaptation conjointe de ces deux modèles a permis de proposer une grille d'évaluation couvrant à la fois les aspects organisationnels, techniques et métiers (Annexe 9). La matrice est structurée en dix domaines d'évaluation, répartis selon deux niveaux : **stratégique** sur lequel nous n'avons que peu de levier d'action et **opérationnel** lequel la marge de manœuvre est plus importante et permet par rebond de faire évoluer le premier. Chaque domaine est

évalué selon une échelle de 4 niveaux. *Awareness* (prise de conscience), *Basic* (mise en œuvre partielle ou ponctuelle), *Managed* (pratiques consolidées), *Optimized* (amélioration continue, alignement stratégique). Les dix domaines évalués (Figure 8) sont :

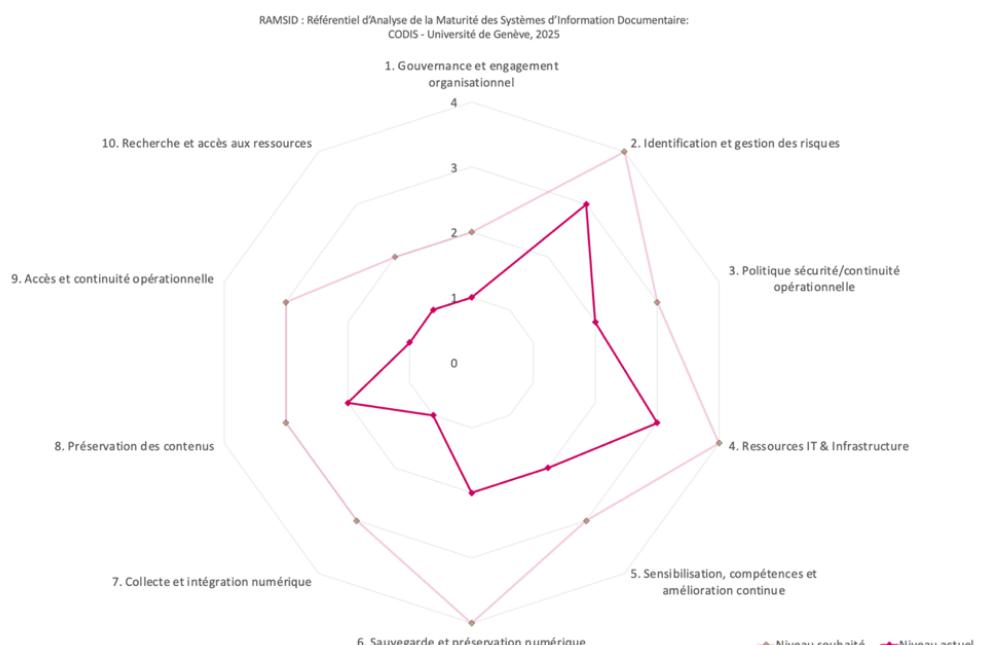
#### **Au niveau stratégique :**

- Gouvernance et engagement organisationnel
- Identification des risques et vulnérabilités
- Politique de sécurité et de continuité
- Infrastructures et ressources informatiques
- Sensibilisation et amélioration continue

#### **Au niveau opérationnel :**

- Sauvegarde et préservation numérique
- Collecte, transfert et intégration
- Préservation de l'intégrité des contenus
- Accès et continuité opérationnelle
- Recherche et accès aux ressources préservées

**Figure 8 - Résultats graphique de la matrice de maturité**



Adapté de (DPC RAM, 2024)

Le fait de combiner deux matrices existantes se révèle pertinent dans une perspective interdisciplinaire alliant archivistique et cybersécurité. Les deux modèles se renforcent mutuellement : la préservation sans cybersécurité est fragile, et la cybersécurité sans préservation peut conduire à une perte irrémédiable. En articulant ces deux cadres reconnus, la matrice proposée constitue un outil que les institutions peuvent adapter à leur propre niveau, et guider les actions à mener pour accroître leur résilience informationnelle globale.

L'analyse révèle une situation contrastée. Certains domaines témoignent d'une certaine maturité, notamment la gestion des risques informatiques et l'infrastructure technique au niveau cyber, qui sont déjà bien structurées. Toutefois, plusieurs aspects apparaissent comme des axes d'améliorations :

- L'absence d'une politique d'archivage et de gestion du cycle de vie des données
- L'absence de politique unifiée de préservation numérique
- Faible reconnaissance institutionnelle et une visibilité partielle des services impliqués
- La faible formalisation des procédures de versement et de sauvegarde
- Le manque de solutions alternatives d'accès aux ressources en cas d'indisponibilité (dark archive, interface miroir, consultation offline)
- Une gouvernance encore fragmentée, peinant à articuler les responsabilités entre fonctions support (DiSTIC, DIS, rectorat) et les métiers.
- Une dualité entre les services administratifs et les facultés.

La majorité des domaines évalués se situent aujourd'hui entre les niveaux *Basic* et *Managed*, tandis que les aspects liés à l'accès d'urgence et à la recherche de contenus préservés restent au niveau *Awareness*. À l'issue de cette évaluation, plusieurs recommandations ont été formulées :

- Adopter une stratégie globale de préservation numérique, intégrée à la gouvernance de la donnée et articulée avec les politiques de sécurité et de continuité institutionnelles.
- Formaliser les procédures de sauvegarde, de versement et d'archivage pour tous les types de ressources numériques, en les harmonisant avec les systèmes existants
- Mettre en place des solutions d'accès résilientes (copies locales, portails statiques, consultations offline), testées régulièrement.
- Renforcer la documentation et les tests de scénarios de crise, notamment pour les ressources électroniques critiques (thèses, SIGB, revues e-books, bases de données, SIGB).
- Instaurer une culture transversale de la préservation, en développant des formations métiers, des indicateurs de suivi, et une gouvernance partagée entre les acteurs fonctionnels et techniques.

Cette matrice de maturité servira de base pour suivre les progrès à un horizon de 12 à 18 mois, et adapter les plans d'action en fonction des évolutions réglementaires, technologiques et organisationnelles. Au regard des indicateurs de disponibilité, de la qualité de l'infrastructure, ainsi que des technologies et procédures en place ou imaginables, la posture de cybersécurité et les capacités techniques de l'Université en matière de préservation numérique apparaissent solides et performantes. Les outils sont là, les standards sont en voie d'être respectés. Toutefois, les fragilités persistent au niveau stratégique, en ce qui concerne les choix d'externalisation des services et l'implication des métiers. L'UNIGE dispose de la capacité et de l'infrastructure nécessaire mais il manque un pilotage transversal, une articulation cohérente entre les différents acteurs le Rectorat, la DIS, la DISTIC et les Archives pour transformer cet ensemble de briques robustes mais segmentés en une stratégie intégrée de gouvernance et de valorisation durable du patrimoine numérique.

## 4. Analyse du système d'information de la bibliothèque

Le système d'information (SI) désigne un ensemble structuré de ressources humaines, techniques et organisationnelles destiné à collecter, traiter, stocker et diffuser l'information au sein d'une organisation (ISO 2020). Il repose sur l'interaction entre des composantes sociotechniques : les personnes, les procédures, les logiciels, les données et les équipements informatiques. L'enjeu consiste à identifier, catégoriser et hiérarchiser ces actifs afin de déterminer ceux qui doivent être intégrés dans les dispositifs protection, pour distinguer les services internes des services externalisés, et mieux maîtriser la continuité opérationnelle.

### 4.1 Définition et périmètre des actifs en bibliothèque

Selon la norme ISO 27005 (2018), un actif informationnel est "tout élément ayant de la valeur pour l'organisation". Dans le cadre de l'étude, cette définition peut être interprétée en décrivant trois catégories. Les infrastructures technologiques qui permettent l'accès, la gestion et la préservation ; les applications qui sont les interfaces des processus métiers et structurent le cycle de vie ; enfin les données, les contenus informationnels et leurs métadonnées de gestion. Le périmètre analysé couvre le système d'information documentaire au sens large. Il s'étend des couches techniques, aux couches métiers, dont les collections électroniques. Il intègre de ce fait les dépendances techniques et applicatives nécessaires pour leurs gestions.

Les collections électroniques sont composées principalement des ressources électroniques acquises par la bibliothèque sous forme d'accès ou en achat ferme (Ebooks, journaux, articles et rapports) ainsi que les contenus produits par l'institution (publications, thèses, mais aussi jeux de données). Ce mémoire n'aborde pas la question de la préservation des publications en *Open Access* non affiliées à l'institution, bien que cet enjeu demeure capital et difficile à éluder dans une perspective globale de conservation scientifique (Laakso, Matthias, Jahn 2021; Claerr, Moufflet 2014).

La conversion des collections en actifs se justifie par l'hypothèse qu'elles sont les composantes les plus sensibles du système d'information des bibliothèques. Le SI est mis en œuvre pour en assurer la disponibilité, l'intégrité, et la confidentialité. Elles doivent être appréhendé non plus comme un support documentaire, mais comme une combinaison d'actifs informationnels, au sens du patrimoine immatériel de l'organisation et de la sécurité de l'information (Gouvernement du Québec 2016). Cette approche s'inscrit dans une perspective de la gouvernance, où les infrastructures, les applications, et les données de gestion, sont intégrés à la notion de capital stratégique (Laney 2018) et représentent bien des actifs informationnels (Hug Buffo 2020).

Les collections électroniques présentent plusieurs caractéristiques propres aux actifs critiques. D'abord elles requièrent des investissements financiers importants, près de 7 Millions en 2024 à l'UNIGE (UNIGE 2025a). Elles soutiennent les fonctions centrales et quotidiennes, la recherche scientifique et l'enseignement, nécessaires à la réalisation de la mission de l'institution et dont l'indisponibilité peut entraîner des perturbations majeures. Par ailleurs, ces ressources peuvent héberger des données rares au caractère exclusif, difficilement remplaçables, leur protection est alors incontournable pour l'intégrité scientifique et la continuité des missions académiques. Les collections physiques, sont d'ailleurs déjà considérées comme des actifs de la bibliothèque, elles bénéficient d'un plan de sauvetage, intégrant des protocoles de prévention, d'intervention et de restauration en cas de sinistre. Ce

dispositif, aligné sur les standards de gestion des biens culturels, constitue une couverture pour la continuité de l'accès à ses ressources. Les collections électroniques ne disposent pas de dispositifs équivalents bien que l'on puisse les considérer comme patrimoine culturel immatériel (Olgiati 2005).

« Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization » (InterPARES, 2017).

L'information constitue en ce sens « une ressource essentielle qui doit être protégée tout au long de son cycle de vie » mais les actifs « n'ont pas tous la même valeur et ne nécessitent pas tous le même niveau de protection ». Un organisme devra adapter ses mesures selon le degré de criticité pour respecter ses obligations légales, éviter les pertes, atteindre ses objectifs de service et renforcer la confiance des utilisateurs (Gouvernement du Québec 2016).

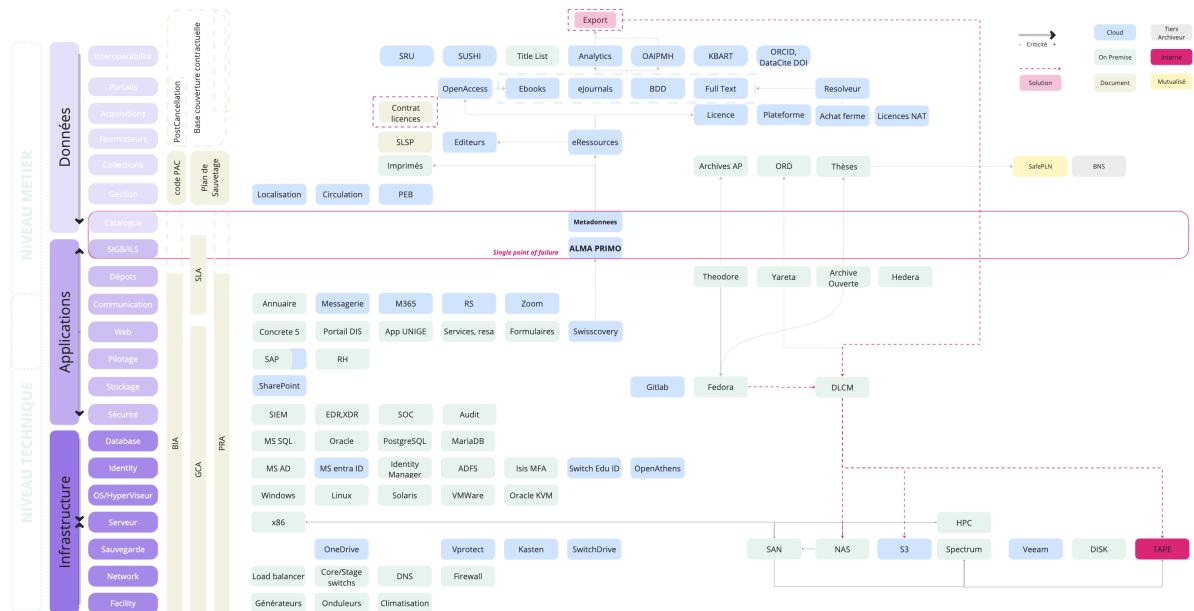
## 4.2 Architecture générale du SI

L'information repose sur des infrastructures physiques communes et ce indépendamment de leurs types. On distingue les données administratives et scientifiques. En bibliothèque, ces deux dimensions sont imbriquées, le SIGB gérant à la fois les données de gestion des collections et les contenus ou le signalement de celles-ci. Ce qui complexifie leur gouvernance et leur sécurisation car il est aussi difficile d'en représenter la responsabilité à cause de leurs propriétés, ces données décrivant des ressources matérielles et virtualisées, en local et externalisées dans le cloud.

La cartographie du système d'information fait partie de l'évaluation nécessaire pour l'analyse de risques et la constitution d'un plan de continuité. Elle formalise une vision structurée des actifs numériques, de leurs interdépendances logique et physique et de leur contribution au fonctionnement global de la bibliothèque. Elle constitue un appui essentiel pour identifier les vulnérabilités, hiérarchiser les mesures de sécurité et repérer les zones de couverture insuffisantes. En rendant l'existant lisible, elle oriente les priorités de protection et met également en lumière les dépendances entre les outils, les points de fragilité critiques (SPOF), et permet d'évaluer la résilience globale du système.

Au travers des entretiens avec les services IT nous avons pu compléter une cartographie de l'infrastructure de la bibliothèque reposant sur celle de l'infrastructure de l'UNIGE (Figure 9 et Annexe 12). Sur cette visualisation le SIGB constitue l'unique interface entre le système d'information de l'UNIGE et les ressources électroniques. Privée des métadonnées et de la base de connaissances d'Alma, la collection numérique devient inexploitable et invisible, noyée dans la masse du Web. Elle bénéficie pour l'heure d'une protection insuffisante via une couverture contractuelle mais non unifiée avec le plan de reprise. En représentant les dispositifs techniques et contractuels en place, cette visualisation permet d'identifier ces lacunes, mais aussi les bonnes pratiques déjà mises en œuvre. Elle ouvre par ailleurs la voie à une réflexion sur les synergies possibles entre les solutions existantes, en vue d'optimiser la sécurité. Enfin, elle contribue à clarifier les responsabilités où le cloud rend la gouvernance du SI plus complexe.

Figure 9 - Cartographie du SI de la bibliothèque de l'UNIGE



CC BY NC Stephen Valot 2025

Il en résulte que le SIGB ainsi que les données qu'il contient doit être catégorisé comme un service numérique essentiel au sens de l'UNIGE, et intégré en tant que tel dans le plan de reprise d'activité. La question qui se pose est donc de déterminer de quelle manière et sous quelle forme cet objectif peut être atteint.

Une autre approche pour mener ce travail consiste à s'appuyer sur une *Configuration Management Database* (CMDB), une base de données permettant d'inventorier l'ensemble des actifs ainsi que les relations existantes entre eux (Boulet 2008). Dans le cadre de la norme ISO 27001, qui exige l'identification, la classification et la protection des actifs (contrôle A.5.9 de l'Annexe A de la norme) (ISO 2022a), la CMDB constitue un outil du système de management de la sécurité de l'information (SMSI). Elle permet d'assurer la traçabilité des actifs critiques, de soutenir l'analyse des risques, de faciliter la gestion des mises à jour et d'alimenter les processus de réponse aux incidents. Une CMDB renforce ainsi la capacité à protéger ses actifs et agit comme un récolelement topographique électronique des applications dans le système d'information.

L'architecture de stockage et de sauvegarde repose sur plusieurs systèmes complémentaires répartis sur deux sites principaux. Le stockage primaire s'appuie sur une architecture Network Attached Storage (NAS), répartie en deux clusters sur chacun des sites et disposant d'une capacité de 6 pétaoctets. Sur le Site 1, le NAS repose sur deux nœuds connectés à plusieurs baies de stockage via un réseau Storage Area Network (SAN), tandis que le site 2 est équipé de trois nœuds reliés à plusieurs baies de stockage, également à travers le SAN. Il est nécessaire pour l'accès rapide et redondant aux volumes de données. Une réPLICATION quotidienne des partages est mise en œuvre entre le Site 1 et le Site 2, permettant en théorie une perte maximale de 24 heures de données en cas de sinistre. Toutefois, des interventions manuelles sont nécessaires pour réactiver les services sur le Site 2, puis pour reconfigurer la réPLICATION lors du retour sur le Site 1. Cela représente un point de fragilité dans la logique de continuité. Concernant les sauvegardes, plusieurs infrastructures coexistent, répondant à différents besoins opérationnels (Veeam, vProtect, Kasten, IBM Tivoli Storage Manager).

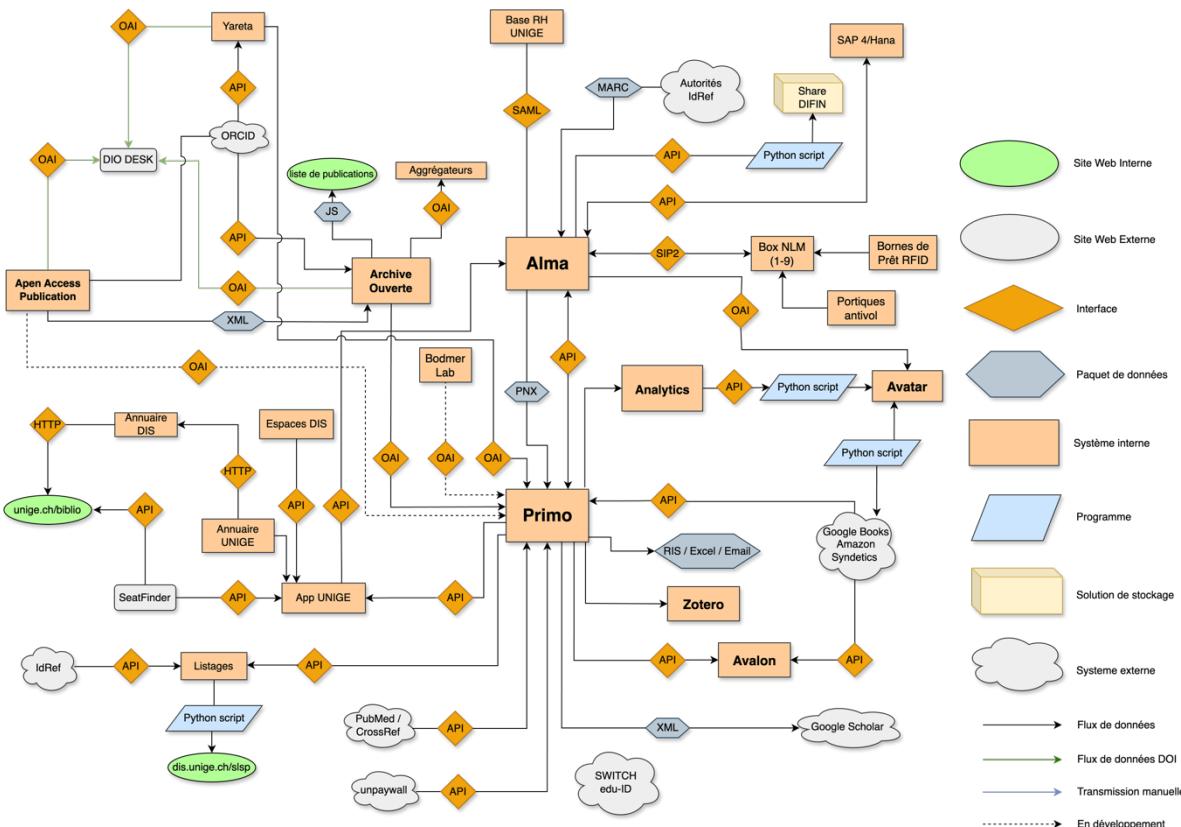
L'instance TSM est une librairie de cassettes à bande et permet la sauvegarde complète des données NAS en 48 heures, avec une rétention de deux ans (Entretien F.Ducret, 2025).

Cette architecture traduit un niveau de maturité élevé en matière de résilience et de protection des données, avec une attention portée à la diversification des technologies, à la réPLICATION, et à la segmentation fonctionnelle des sauvegardes. Toutefois, l'absence d'automatisation de la reprise d'activité entre les deux sites, ainsi que la complexité de gestion de l'architecture, fait valoir la nécessité d'un alignement plus fort avec les standards de continuité (indicateurs RTO/RPO) et d'un renforcement des procédures d'orchestration. La coexistence de plusieurs solutions doit être connue et organisée pour garantir la cohérence globale du dispositif, en particulier en cas d'attaque ciblée.

### 4.3 Cartographie des flux de données

Au niveau de la Bibliothèque la complexité intrinsèque du SI constitue un facteur de vulnérabilité. Cette fragilité est due aux appels nécessaires pour la centralisation des données, via le moissonnage (*harvesting*) des ressources ouvertes et d'autres plateformes internes et externe. Le dépôt de publications (Archive Ouverte), l'archive de données de recherche (Yareta) ainsi que les sources externes (par ex. PubMed) sont moissonnées pour être signalés dans « swisscovery UNIGE ». Si le SIGB Alma est dorénavant un service numérique essentiel, son outil de découverte, Primo VE (derrière le portail « swisscovery » connecté à Alma) l'est tout autant par sa qualité de point d'accès central aux métadonnées agrégées (Figure 10). Le mapping des ressources acquises et moissonnées qu'il rend disponible par le signalement, constitue le catalogue conceptuel des collections élargies de l'UNIGE.

Figure 10 - Flux de données de la Bibliothèque de l'UNIGE (2025)



Inspiré du (schéma de la bibliothèque de l'ETH, Pablo Iriarte, 2025)

Il agit comme point d'entrée centralisé vers l'ensemble des ressources documentaires, qu'elles soient sous licence, en libre accès ou issues des collections physiques. Sa défaillance, même temporaire, compliquerait rapidement l'accès aux contenus scientifiques pour les utilisateurs, affectant directement les missions d'enseignement et de recherche. De surcroît, toute la couche d'infrastructure repose sur des dépendances externes : services SaaS, systèmes d'authentification fédérés, résolveurs de liens, synchronisation avec les bases de connaissance centralisées, et l'interopérabilité avec d'autres services tiers (éditeur, agrégateur, plateformes de données).

Dans ces échanges externes on retrouve *SWITCH edu-ID*, une infrastructure fédérée externalisée d'authentification développée par la Fondation SWITCH pour le secteur académique. Elle permet aux utilisateurs d'accéder, avec un identifiant unique, au compte personnel sur *swisscovery*. Infrastructure de confiance intégrant des mécanismes de sécurité (protocole SAML 2.0), elle est destinée à protéger l'identité numérique des utilisateurs. Le principe de minimisation des données limite la transmission des attributs aux seules informations strictement nécessaires, réduisant l'exposition des données personnelles. Il constitue une dépendance technique supplémentaire (cf. partie 3.3) et ajoute une couche de complexité au niveau de l'utilisateur sur la gestion de leurs propres mots de passe.

La criticité est renforcée par le rôle fonctionnel du SIGB dans le cycle de vie de l'information : gestion des abonnements, suivi des licences, signalement dans le catalogue, accès distant sécurisé, et intégration avec les outils de recherche utilisés par la communauté académique. Il est le système documentaire sur lequel s'appuient les processus. En cas de problème de disponibilité, l'accès à toutes ces fonctionnalités se trouve compromis. Bien que ce ne soit pas l'unique point d'accès sur internet à ces ressources, il est l'unique à les centraliser et à permettre l'accès au contenu sur la bonne plateforme, acquis par la Bibliothèque et protégé par les droits contractuels eux-mêmes inclus dans le programme.

#### **4.4 L'environnement applicatif de gestion**

Le SIGB Alma, prend en charge la gestion des collections physiques et électroniques, les données des usagers, des prêts et des demandes, permet le signalement et l'accès aux ressources. Il est aussi garant des licences que l'on possède et fait le lien avec le système de facturation. Il permet la gestion administrative de tout le cycle de vie des ressources électroniques, depuis les tests jusqu'à la suppression. Il prend en charge l'ensemble du traitement documentaire, de l'inventaire des collections à leur indexation, en incluant les fonctions de contrôle des accès, et de signalement sur Primo VE.

Primo VE permet la recherche et la consultation unifiée des collections physiques et électroniques gérées dans Alma. Il intègre un résolveur de liens qui, à partir d'une requête OpenURL génère dynamiquement les liens profonds vers les ressources électroniques signalées en fonction de la disponibilité effective, des droits d'accès définis par les licences souscrites, et du profil de l'utilisateur identifié. Celle-ci affiche dynamiquement les options d'accès disponibles, comme le texte intégral, le prêt ou la demande. La création de ces liens à la volée, repose sur une base de connaissance propriété du fournisseur ExLibris. Elle n'est donc pas reproductible à partir des métadonnées disponibles sur Alma, ce qui limitera la précision d'un éventuel catalogue alternatif, où les liens proposés ne pourront pas pointer sur un article en particulier, sauf s'il dispose d'un DOI. Il est important de distinguer les données

destinées à la gestion administrative de celles produites ou acquises dans le cadre des missions documentaires.

Dans le contexte de mutualisation coordonné par SLSP, les standards techniques garantissent une cohérence à l'échelle nationale, mais freinent les ajustements locaux. Ces contraintes posent des questions de souveraineté numérique, de capacité d'adaptation et de pérennité des services dans le temps au niveau de chaque institution. Ce modèle centralisé, bien qu'efficace, sécurisée et fiable pour garantir la stabilité et la maintenance de nombreuses institutions en Suisse, peut s'avérer moins flexible pour répondre aux besoins spécifiques et évolutifs. Cela limite les capacités d'intervention directe de l'institution en cas d'incident et accentue la nécessité de plans de contingence, incluant la redondance des données et du service, des canaux de communication et d'accès alternatifs, et une documentation d'urgence pour la communauté. Par exemple, concernant l'obtention des logs d'Alma, qui serait nécessaire à améliorer la posture de sécurité, SLSP ne dispose pas d'un levier suffisant pour les obtenir. Les institutions conservent tout de même une marge d'autonomie sur les données de leur zone institutionnelle via divers outils d'exportation, ainsi qu'une option de sauvegarde locale premium proposée par Ex Libris (*Alma back up*). Toutefois, cette solution onéreuse nécessite une infrastructure spécifique pour recevoir les données.

Ex Libris conserve donc une maîtrise exclusive de la restauration complète en cas d'incident, et la granularité des récupérations reste incertaine. Face à ces limitations, certaines initiatives peuvent être imaginées, comme le développement d'une base de données indépendante à partir de l'exploitation des données de la zone institutionnelle (IZ) dans une volonté de reprendre le contrôle sur les données, et permettre un accès alternatif, des opérations de nettoyage, de correction de masse ou à des fins statistiques. Cette autonomie partielle ne constitue pas une solution complète de continuité d'activité en cas de compromission du système principal. En cas de cyberattaque ou d'interruption prolongée, comme le déménagement de son datacenter (Ex Libris 2024) aucun mécanisme de bascule n'est prévu.

Plusieurs applications internes, développées spécifiquement pour répondre aux besoins métiers, utilisent aussi les APIs d'Alma pour automatiser diverses tâches de supports liées à la gestion documentaire. Elles couvrent des fonctions d'impression automatique au guichet d'accueil, de listage de notices Alma et IdRef, des modifications en lot, de génération d'étiquettes de côtes, d'extraction et d'envoi des PDFs attachées aux factures vers SAP, ou encore des outils de valorisation des ressources électroniques comme Avalon et Avatar. Ces applications traitent des données parfois confidentielles et sont devenues indispensables au fonctionnement normal du SI. À ce titre, elles doivent faire l'objet de mesures de sécurité dès leur conception, conformément aux principes de « *secure by design* » et ce en conformité avec le guide de sécurisation des applications (UNIGE 2021c). Le recours à des développements rapides ou non documentés peut exposer l'institution à des vulnérabilités (Poupard 2018), notamment en cas de dépendance au savoir tacite des équipes systèmes ou les erreurs humaines sur les accès et les mises à jour.

Une stratégie de routine d'exports réguliers, couplée à un stockage distribué et une solution d'accès de secours s'avère être une solution pour possiblement garantir une continuité minimale des services en cas d'indisponibilité, et renforcerait le contrôle de l'institution sur ses propres données vis-à-vis du fournisseur.

## 4.5 Intégration des ressources électroniques dans les actifs

La vision héritée des collections imprimées influence la manière dont les collections électroniques sont appréhendées. Les éditeurs continuent de structurer leurs offres autour de revues et de périodiques, et commercialisent les contenus dans une logique proche de celle de l'abonnement physique. Ce qui ne correspond plus à la demande de la communauté à desservir qui adoptent une lecture ciblée sur des parties spécifiques des articles, principalement le résumé, les résultats et l'introduction (OES 2025). Ce travail s'essaie de considérer ces contenus comme des actifs informationnels à part entière dans un objectif de sécurité. La transition dans les bibliothèques universitaires d'une acquisition fondée sur l'achat d'imprimés à un modèle centré sur l'accès aux ressources électroniques a profondément transformé leurs pratiques contractuelles (Metrat, Oury 2017). Cela a remis en question leur capacité à garantir la pérennité de leurs collections. Contrairement aux ouvrages imprimés acquis de manière définitive, les ressources sous licence demeurent la propriété des éditeurs, rendant les bibliothèques tributaires de clauses contractuelles parfois floues, notamment en cas de résiliation (Polchow 2021).

Pour pallier ces évolutions, les nouveaux usages et répondre aux mutations de l'offre du marché de l'édition scientifique, la complexité des systèmes documentaires s'est progressivement accrue. Pensés pour répondre à l'accroissement et à la diversité des ressources électroniques, à leur gestion et leurs signalements, ces systèmes intègrent aujourd'hui une grande variété de données, métadonnées, informations de localisation, d'exemplaires, de licences, dont l'administration peut dépasser les capacités internes des bibliothèques. Cette tendance a conduit à un recentrage des compétences sur l'utilisation de ces solutions plutôt qu'à leurs conception, favorisant involontairement la perte de maîtrise. En exemple, bien que les bibliothécaires produisent une partie des métadonnées, l'accès aux index et leur exploitation reste limité. L'usage des résolveurs de liens contraint l'export de liens profonds ou la constitution de corpus documentaires spécifiques.

Le regroupement des ressources en bouquets, modèle économique favorisé par les grands éditeurs, complique l'identification détaillée des collections. On dénombre dans le SIGB 515'722 ebooks et 86'249 périodiques, ce qui illustre l'ampleur du corpus numérique et les défis que pose son administration sans suivi précis, et métadonnées fiables.

À ce jour, l'archivage des publications à l'UNIGE n'est pas réfléchi dans la gestion du cycle de vie des publications, aucune stratégie de type "*dark archive*" ou équivalent de LOCKSS n'est envisagée, les garanties du fournisseur et des autres acteurs étant jugées suffisantes. Ces éléments révèlent toutefois une autonomie limitée vis-à-vis des fournisseurs, tant en matière de souveraineté des données que de capacités de restauration indépendante. Mais peut s'expliquer, compte tenu du volume et de la complexité des données gérées dans le système. Cette observation s'inscrit dans un écosystème avec plusieurs parties prenantes : bibliothèques, consortiums, plateformes nationales, auteurs, mais aussi éditeurs, qu'ils soient commerciaux (*for-profit*) ou à but scientifique (*for science*). La responsabilité des éditeurs dans la préservation et l'accès pérenne aux publications qu'ils diffusent doit être aussi engagée. Leur rôle dépasse la simple mise à disposition des contenus : ils ont également un devoir de transparence sur l'usage, ainsi qu'une part de responsabilité dans les garanties de conservation à long terme.

## 4.6 Actifs informationnels

« Un actif désigne tout élément ayant de la valeur pour l'organisme et nécessitant, par conséquent, une protection. » ISO 27005(ISO 2018). Il est nécessaire de les identifier, de les catégoriser, de les prioriser pour pouvoir les protéger.

### 4.6.1 Identification des actifs

Le SI articule ses différentes couches fonctionnelles, autour des catégories d'actifs suivantes :

- **Les ressources électroniques**, comprenant les contenus sous licence, leurs métadonnées et identifiants, contrats de licence et éléments de gestion documentaire.
- **Les dépôts institutionnels**, tels que l'Archive Ouverte UNIGE, pour la conservation et la diffusion des publications de l'institution.
- **Les contenus internes**, les guides, formations, memento ou procédures qui soutiennent la médiation documentaire et favorisent une appropriation des ressources.
- **Le système d'information documentaire** englobe les infrastructures logicielles (Alma, Primo VE, résolveur de liens) connectées aux dispositifs d'authentification.
- **Les données institutionnelles**, issues du pilotage et du fonctionnement de la bibliothèque (statistiques, abonnements), permettent d'orienter les choix stratégiques et d'objectiver les décisions budgétaires.
- **Les données utilisateurs**, historiques de transactions, logs aux serveurs d'applications, soumises aux cadres légaux de protection des données (LPD, RGPD).
- **Les équipements numériques et solutions de stockage** regroupent les serveurs, les infrastructures de sauvegarde, garants de la disponibilité, de la sécurité et de la pérennité des données numériques.
- **Le capital humain et les compétences**, des savoir-faire en bibliothéconomie, gestion de métadonnées, administration de systèmes, pour assurer la maîtrise et l'évolution du système.

Ce travail aboutit à une liste structurée des actifs (Annexe 10) et des processus métiers associés, servant de base au processus de gestion des risques en sécurité de l'information.

Tableau 3 - Registre des groupes d'actifs informationnels

Catégorie d'actif	Description détaillée	Exemples concrets	Rôle dans la bibliothèque	Criticité	Priorité	Risques associés
Ressources électroniques	Revues électroniques, livres numériques, bases de données scientifiques, plateformes éditeur	PubMed, ScienceDirect, UpToDate, e-books en médecine	Accès aux contenus scientifiques, support aux activités pédagogiques et de recherche.	3	1	Perte d'accès, altération des données, problème de licences, cyberattaques.
Système d'information	Infrastructures logicielles de gestion des ressources et des utilisateurs.	SIGB, portail documentaire, outil de découverte, résolveur de	Organisation, accès et diffusion des ressources, gestion des prêts.	4	1	Défaillance du système, perte de données, indisponibilité, intrusion.
Données utilisateurs	Informations personnelles et comportementales des usagers.	Historique de prêt, données de connexion, profils personnalisés	Adaptation des services, analyse des usages, sécurité d'accès.	4	2	Fuite de données, non-conformité LPD et RGPD, usurpation d'identité.
Données institutionnelles	Données internes liées au fonctionnement, à la stratégie et aux finances.	Statistiques d'usage, rapports d'activités, abonnements	Pilotage stratégique, prise de décision, justification budgétaire.	2	2	Manipulation des données, mauvaise gouvernance, perte d'information stratégique.
Équipements numériques	Matériel informatique et dispositifs numériques utilisés pour l'accès ou la gestion de l'information.	Serveurs, postes de travail, lecteurs RFID, bornes de prêt	Support physique à l'accès et à la gestion des services documentaires.	2	3	Défaillance matérielle, obsolescence, vol, attaque physique.
Capital humain / compétences	Ensemble des connaissances et expertises du personnel.	Bibliothécaires spécialisés, administrateurs système, formateurs	Exploitation, gestion et sécurisation des autres actifs.	3	1	Départs non anticipés, mauvaise transmission des savoirs, erreurs humaines.
Contenus internes	Documents produits localement pour l'accompagnement à l'utilisation des ressources.	Guides d'utilisation, tutoriels, notices bibliographiques	Valorisation et facilitation de l'usage des ressources.	2	3	Non sauvegarde, perte de valeur informative, obsolescence.
Dépôts institutionnels	Plateformes de dépôt, d'archivage et de diffusion des publications scientifiques et données de recherche.	Archive Ouverte, Fedora, dépôts institutionnels ou nationaux	Conservation, valorisation et accessibilité des productions scientifiques. Conformité aux exigences de diffusion, indisponibilité, atteinte à l'intégrité scientifique.	3	2	Perte ou altération des données, non-conformité aux exigences de diffusion, indisponibilité, atteinte à l'intégrité scientifique.
Équipements numériques/stockage	Systèmes de stockage centralisé ou distribué pour héberger les données critiques de la bibliothèque.	NAS, SAN, Infra, voir Schéma	Stockage sécurisé et accessible des ressources numériques, dépôts, et données d'usage.	4	1	Perte de données, panne critiques, ransomwares ciblant le stockage, mauvaise configuration, défaillance de redondance.

CC BY NC Stephen Valot 2025

Chaque actif doit être analysé en fonction de sa criticité (Tableau 3) pour les missions de la Bibliothèque, de son mode d'hébergement (local, cloud public, mutualisé), de ses

dépendances techniques (API, protocoles, authentification), de son niveau de maîtrise (contrôle direct, hébergement par un fournisseur, intermédiation par un consortium), ainsi que de l'existence de mesures de secours ou de préservation (sauvegardes, export pérenne, archivage via LOCKSS ou autres services tiers). L'identification des actifs constitue une étape de l'appréciation des risques. Il s'agit de recenser l'ensemble des éléments de valeur pour l'organisation. Chaque actif doit être documenté avec son propriétaire, garant de sa gestion et de sa protection. Le niveau de détail retenu pour l'identification doit être adapté aux besoins de l'analyse de risques et pourra être affiné au fil des itérations.

Le détail des ressources électroniques, quant à lui, comprend trois catégories de données complémentaires :

- Les données de gestion, liées aux contrats d'acquisition, aux droits d'accès et aux modalités financières.
- Les métadonnées bibliographiques, qui décrivent, indexent et rendent accessibles les contenus.
- Les contenus eux-mêmes, c'est-à-dire les textes intégraux.

Les deux premières catégories sont généralement centralisées, structurées et maîtrisées par le système interne de gestion documentaire (Alma, Primo). Elles constituent le catalogue de la collection puisqu'elles sont le recueil des ressources dont on dispose et contient aussi les données relatives aux collections imprimées (localisation). En revanche, les contenus en texte intégral, qui constituent la valeur informationnelle des ressources, sont majoritairement hébergés à distance, sur les serveurs des éditeurs, rendant leur préservation dépendante des conditions contractuelles et de l'interopérabilité technique des plateformes commerciales.

La distinction des actifs informationnels nativement produits par l'institution et déjà versés dans l'Archive Ouverte institutionnelle conduit à les exclure du périmètre de l'étude. Les thèses et les publications pourvues d'un DOI, en tant que patrimoine universitaire bénéficient déjà de mécanismes de protection dédiés. Le dépôt des thèses dans Archive Ouverte est d'ailleurs une condition préalable à l'obtention du diplôme. Si la plateforme repose actuellement sur *Fedora* et ne satisfait pas l'ensemble des exigences d'un véritable système d'archivage les risques résiduels sont atténués par plusieurs mesures complémentaires. Une analyse d'impact sur l'activité (BIA) intègre le service numérique au plan de reprise d'activité (PRA) de l'UNIGE. Les contenus sont ensuite répliqués dans le réseau *SAFE Private LOCKSS Network* (SAFE-PLN, 2024), une initiative internationale de préservation distribuée reposant sur la technologie open source LOCKSS (*Lots of Copies Keeps Stuff Safe*). Il permet de conserver des copies redondées réparties sur plusieurs serveurs hébergés par des universités membres (Beagrie 2013). Ce réseau repose sur une structure légère basée sur un protocole d'accord, une gouvernance fédérée, et l'autonomie technique de chaque partenaire, qui conserve le contrôle sur ses contenus et peut en surveiller l'intégrité (SAFE-PLN 2024). Enfin un versement dans le programme *e-Diss* de la Bibliothèque Nationale Suisse (BNS), le répertoire national des thèses numériques produites par les universités, assure un archivage pérenne et donc une redondance supplémentaire à l'échelle nationale (Bibliothèque Nationale 2019). L'accès aux documents varie selon les politiques institutionnelles. Certaines publications sont librement consultables, d'autres accessibles uniquement sur place à la BN, ou parfois restreintes.

Les ressources humaines constituent également un paramètre dans l'analyse d'un système d'information de bibliothèque. Derrière chaque infrastructure technique se trouvent des

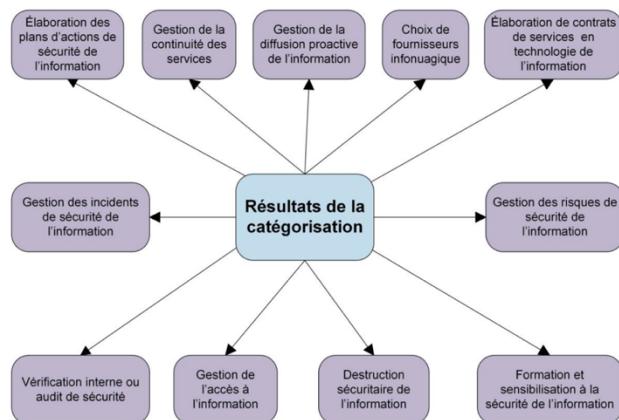
compétences humaines, souvent implicites et dispersées. Les connaissances tacites, qui ne sont ni documentées ni aisément transférables représente un risque sous-estimé. On parle alors du « *bus factor* ». Le nombre minimal de personnes qui, si elles venaient soudainement à quitter l'équipe (changement de poste, maladie, retraite), entraîneraient l'arrêt ou la paralysie du service faute d'expertise suffisante (Jabrayilzade et al. 2022). Dans le contexte des bibliothèques numériques, ce risque concerne la configuration des systèmes d'information, la gestion des métadonnées et des licences électroniques, ainsi que la mise en œuvre de solutions de préservation numérique. La centralisation des savoirs techniques entre quelques spécialistes accroît la vulnérabilité organisationnelle. Des actions telles que la documentation des procédures, le croisement des compétences, la formation continue et l'automatisation des processus permettent de limiter ces risques.

Le système de gestion des ressources électroniques (que l'on appellera ici le catalogue conceptuel bien qu'il n'existe pas en tant que tel) représente l'élément central du système documentaire, à l'intersection des enjeux d'accès, de gestion, de préservation et de gouvernance décrite dans cette partie. En tant que référentiel, il conditionne la continuité des services et la maîtrise des actifs numériques, les solutions traiteront prioritairement de sa sauvegarde et de son accès.

#### 4.6.2 Catégorisation des actifs

La catégorisation est présentée comme le « Processus permettant de déterminer le niveau de criticité des actifs informationnels, compte tenu de l'impact que peut engendrer un bris de disponibilité, d'intégrité ou de confidentialité de ces actifs sur l'organisme et sa clientèle ou sur d'autres organismes [...] Le choix du niveau de granularité est tributaire du contexte de l'organisation et du degré de précision souhaité pour répondre à ses besoins en matière de sécurité de l'information »(Gouvernement du Québec 2016).

Figure 11 - Exemple de cas d'usage des résultats du processus de catégorisation



(Guide de catégorisation de l'information, 2016)

Cette classification des actifs permet d'adapter les priorités de gestion des risques, de guider le choix des prestataires et de structurer les réponses organisationnelles (Figure 11). Dans la pratique, ce processus repose sur :

- La définition des actifs numériques critiques, applications métier, bases de données, archives, catalogues, etc.

- La cartographie détaillée des processus (cf. partie 5) pour identifier les flux d'information et les dépendances.
- Une méthodologie d'évaluation de la criticité fondées sur la valeur scientifique, le coût et l'unicité des ressources (cf. partie 4.6.4).
- Des stratégies de protection différenciées (cf partie 6) alignées sur le niveau de criticité, afin de garantir la disponibilité, l'intégrité et la confidentialité des actifs essentiels de l'institution (Gouvernement du Québec 2016).

Tableau 4 - Critères de classification de l'information et des données

Sensibilité faible	Sensibilité moyenne	Sensibilité élevée
Pas de secret de fonction	Secret de fonction simple <sup>1</sup>	Secret de fonction qualifié <sup>2</sup>
Les actifs sont classés comme à faible risque s'ils ne sont pas considérés comme à risque modéré ou élevé, et:  1. Les actifs sont destinées à la divulgation publique, ou 2. La perte de confidentialité, d'intégrité ou de disponibilité des actifs n'aurait aucun impact <sup>3</sup> négatif sur la mission, la sécurité, les finances ou la réputation de l'UNIGE.  Pour les données destinées au public, des garanties en termes d'intégrité et de disponibilité des données sont nécessaires.	Les actifs sont classés comme à risque modéré s'ils ne sont pas considérés comme à haut risque, et:  1. Les actifs ne sont généralement pas accessibles au public, ou 2. La perte de confidentialité, d'intégrité ou de disponibilité des actifs pourrait avoir un impact <sup>3</sup> négatif limité sur la mission, la sécurité, les finances ou la réputation de l'UNIGE.  L'accès à ce type d'actifs est limité à la communauté universitaire ou à un sous-ensemble de celle-ci, ou à des tiers clairement identifiés et légitimes.	Les actifs sont classés comme à haut risque si:  1. L'Université doit protéger les actifs en vertu d'une loi, d'un règlement, d'un contrat, d'une entente de confidentialité ou de par leur valeur stratégique 2. L'UNIGE est tenue de déclarer des accès inappropriés à ces données 3. La perte de confidentialité, d'intégrité ou de disponibilité des actifs pourrait avoir un impact <sup>3</sup> négatif important sur la mission, la sécurité, les finances ou la réputation de l'UNIGE.  <b>Sensibilité très élevée (secret)</b> Information qui doit être connue de l'utilisateur lui-même, ou d'un ensemble très restreint d'utilisateurs.

(UNIGE, 2024)

La gestion sécurisée de l'information consiste à évaluer son niveau de sensibilité (Tableau 4). L'UNIGE distingue quatre grandes catégories, allant des données publiques sans enjeu particulier, jusqu'aux données personnelles strictement privées, selon leur impact potentiel en cas de perte de confidentialité, d'intégrité ou de disponibilité. Une fois la catégorie déterminée, l'utilisateur peut s'appuyer sur un tableau de correspondance (UNIGE 2021c) pour sélectionner les outils compatibles avec le niveau de sensibilité requis.

Selon la grille de classification, les publications sous licence et autres ressources électroniques contractuelles doivent être considérées comme des informations à sensibilité élevée, en raison des obligations juridiques et contractuelles qui les encadrent. En revanche, les catalogues, dans leur composante bibliographique publique, relèvent d'une sensibilité faible, tandis que les données associées à la gestion contractuelle nécessitent un niveau de confidentialité plus important. Bien que leur compromission puisse avoir un impact négatif modéré sur les missions, la sécurité, les finances ou la réputation de l'UNIGE, ces actifs doivent faire l'objet de mesures de protection appropriées. Dans le contexte des bibliothèques académiques et de leurs collections numériques, la conceptualisation des ressources en tant qu'actifs informationnels constitue une approche utile pour l'élaboration d'une stratégie de cybersécurité. Cette classification repose sur la reconnaissance que ces ressources représentent une partie importante du patrimoine stratégique de la Bibliothèque.

#### 4.6.3 Priorisation des actifs

La priorisation des actifs du système d'information constitue une des étapes les plus complexe dans la réflexion autour de notre sujet. Elle doit pouvoir distinguer hiérarchiquement les

composantes métier à différents niveaux, de l'infrastructure, aux applications jusqu'aux données et les ordonnées selon leur criticité pour la continuité des services. Cette hiérarchisation réfère à des pratiques de gestion de collections patrimoniales et guide l'exploration vers des solutions techniques pour la préservation. Le résultat constitue une réflexion sur la pertinence de cette démarche résolument non-triviale (Annexe 13, 14).

Tout comme dans les collections imprimées, la priorisation dans un contexte de volumes croissants de données et de ressources limitées, devient incontournable. Elle permet de concentrer les moyens de préservation et de sécurité sur les actifs les plus sensibles ou stratégiques, et renforce ainsi l'efficacité globale des dispositifs. Cependant l'archivage numérique est souvent négligé car les coûts de stockage semblent insignifiants. L'absence de visibilité de cette contrainte conduit parfois à une gestion laxiste des données numériques, ce qui peut avoir des conséquences en termes de perte d'information ou de difficulté à récupérer des données après un incident majeur (Entretien P.L'Hostis, 2025). Il devient impératif d'appliquer une rigueur similaire à la gestion de l'espace assortie d'une réflexion précise sur ce qui doit être sauvegardé et la durée de conservation des données, selon des critères légaux, académiques ou d'intérêts stratégiques.

Dans le contexte de la bibliothèque de l'UNIGE une forme de priorisation est déjà nécessaire pour faire face aux restrictions budgétaires qui forcent à restreindre la richesse des licences. Les indicateurs mobilisés pour ces arbitrages incluent principalement le nombre de consultations, ce qui tend à défavoriser les disciplines moins représentées en nombres d'étudiants au profit des facultés ayant plus d'effectifs. D'autres critères tels que le nombre d'inscrits par faculté, le nombre de publications affiliées, ou encore des indicateurs bibliométriques des journaux sont également utilisés pour pondérer les choix. Ces approches ne sont pas sans effets pervers qui peuvent limiter la diversité, fragiliser les ressources moins visibles ou minoritaires, et peuvent aussi conduire à écarter des revues prestigieuses dans le cas ou peu de chercheurs locaux y publient. En d'autres termes, les objectifs économiques à court terme entrent en contradiction avec les missions académiques et patrimoniales à long terme. Cela soulève une question stratégique : vaut-il mieux tout archiver, au risque d'une forte consommation de ressources à long terme, ou opter pour une sélection raisonnée, plus exigeante en amont mais plus soutenable sur les plans technique, économique et organisationnel ?

Si l'on transpose cette réflexion à l'exemple des collections physiques, force est de constater que les principes d'application des codes Préservation and Conservation (PAC) sont difficiles à respecter, notamment à la Bibliothèque de Genève (BGE), où le volume des saisies et le niveau d'information disponible demeurent insuffisants pour rendre le dispositif véritablement exploitable en situation de crise (Entretien VdG, 2025). Un constat similaire peut être dressé pour les collections physiques de la Bibliothèque de l'UNIGE, où la masse des documents désignés comme prioritaires excède largement les capacités opérationnelles des équipes de sauvetage, rendant l'intervention difficile, risquée et parfois irréaliste (Entretien ELSE, 2025). Cela illustre la nécessité de repenser les critères de sélection, en intégrant une logique de faisabilité logistique et de hiérarchisation, qui pourrait également inspirer la gestion des ressources électroniques.

Cette priorisation s'applique exclusivement aux ressources en texte intégral, dans la mesure où ce sont elles qui nécessitent des arbitrages en matière de stockage et de préservation. En

revanche, s'agissant du catalogue, c'est l'exhaustivité qui demeure impérieuse. L'intégrité des métadonnées bibliographiques et de gestion doivent être pleinement conservées. Cependant l'information de localisation, repose encore trop sur le résolveur de liens, ce qui limite actuellement les possibilités d'extraction complète et autonome des données. Dans les cas où la sauvegarde du texte intégral s'avère impossible, l'extraction des résumés et leur appariement aux notices bibliographiques peut constituer une alternative partielle, permettant de préserver une trace exploitable du contenu. Cela réfère au dépôt légal électronique qui se heurte à ces limites techniques et budgétaires, empêchant une collecte exhaustive comme pour les imprimés. L'archivage du web requiert une sélection avec deux grandes stratégies : la collecte sélective, ciblée mais profonde, qui privilégie des contenus jugés patrimoniaux selon des critères précis ; et la collecte large, plus automatisée et étendue, mais souvent moins détaillée, qui vise à documenter l'évolution globale du web (Pennock 2013).

La mise en œuvre d'une politique de priorisation doit permettre d'objectiver les choix et de formaliser la sélection. Il s'agit d'un outil stratégique d'aide à la décision pour la préservation mais n'a pas vocation à être un instrument de réduction budgétaire. Cette politique doit définir des orientations cohérentes, indépendamment des contraintes financières répétées et immédiates sur les acquisitions. Chaque site de la Bibliothèque est consulté quant à la pertinence de l'effort nécessaire pour la sauvegarde d'une licence, lorsqu'une ressource est identifiée comme prioritaire dans la stratégie de préservation. La réussite du plan de sauvegarde des ressources électroniques à l'UNIGE comme ailleurs doit être une démarche collective. La priorisation repose sur une grille multicritère combinant trois dimensions complémentaires : techniques, quantitatives et qualitatives. Cette approche permet d'optimiser les efforts de sauvegarde en fonction des risques, des valeurs et des capacités techniques et opérationnelles de l'institution. En articulant ces critères inspirés de plusieurs travaux (Konstantelos, Yan 2023; DPC 2024b; Guirlet 2020; Tavernier, and Carlson 2021), cette approche vise à bâtir une stratégie de préservation sélective présentée dans le tableau 5, alignée sur les missions de recherche, d'enseignement et de services de la Bibliothèque.

Tableau 5 - Méthode de priorisation des ressources électroniques

Critères	Catégorie	Description	Note (0-5)	Pondération (1-3)	Score
Techniques	Format des fichiers	Les fichiers sont-ils dans un format ouvert, lisible et documenté (ex : PDF/A, XML, MARC, Dublin Core) ? JHOVE?			
	Interopérabilité des métadonnées	Les métadonnées sont-elles récupérables via des standards ouverts (OAI-PMH, API, FTP) ?			
	Identifiant perenne	La ressource possède un identifiant perenne ISSN, DOI, ISBN, ARK, Handle, PMID...?			
	Accessibilité hors ligne	Peut-on recréer une version consultable sans dépendre d'un accès à la plateforme ?			
	Complexité d'extraction	Existe-t-il des outils ou scripts permettant d'automatiser l'extraction des données ?			
	Conditions d'exploitation	Le fournisseur accepte le text mining, le data-mining, et sous quelle condition ?			
	Taille estimée des données	Volume des données à sauvegarder (influence la capacité de stockage et la fréquence de sauvegarde).			
Quantitatifs	Fréquence d'utilisation	Nombre de consultations, téléchargements ou usages académiques par an.			
	Taux de citation ou de référence	Le contenu est-il souvent cité dans les publications ou cours de l'institution ? Utilisation du JCR Q1			
	Nombre de titres ou d'objets	Combien d'unités documentaires sont concernées (ebooks, articles, documents) ?			
	Nombre d'accès simultanés autorisés	Mesure l'importance du service pour les usages collectifs ou pédagogiques.			
	Durée d'accès post-résiliation (PCA)	Nombre d'années pendant lesquelles l'accès est garanti après résiliation du contrat.			
	Historique d'utilisation	La ressource est-elle utilisée de manière constante dans le temps ou de façon ponctuelle ? Taux d'usage par effectif facultaire			
	Nombre de départements concernés	Combien d'unités académiques utilisent ou dépendent de la ressource ?			
Qualitatifs	Durée de conservation souhaitée	Combien de temps la ressource doit-elle être conservée (court, moyen, long terme) ?			
	Valeur stratégique	Le contenu est-il essentiel à la mission de recherche, d'enseignement ou documentaire ?			
	Exclusivité du fournisseur	La ressource est-elle disponible uniquement via un fournisseur ou est-elle redondée ailleurs ?			
	Conditions d'accès en temps normal	La ressource est-elle en open-access, en freemium, protégée par DRM spécifique, nécessite une plateforme d'accès?			
	Présence dans les archives mutualisées	Le contenu est-il déjà conservé dans CLOCKSS, Portico, SafePLN ou similaire ? Voir DOAJ ? Voir Keepers Registry?			
	Clauses contractuelles explicites (PCA)	Existence de clauses précises autorisant l'archivage local ou via un tiers de confiance.			
	Stabilité du fournisseur	Le fournisseur est-il financièrement et structurellement stable ? Présence stable dans les bouquets, title list ?			
	Valeur patrimoniale ou légale	Le contenu doit-il être conservé pour des raisons juridiques, historiques ou institutionnelles ?			
	Disponibilité de copies exportables	Est-il possible d'obtenir des copies locales par export régulier (XML, MARC, fulltext) ?			
	Clarté des droits de conservation	Les droits de conservation sont-ils clairement définis dans les licences/contrats ?			
	Impact pédagogique	La ressource est-elle intégrée dans des cours, des modules de formation ou Moodle ?			
	Langue et accessibilité	La ressource est-elle disponible dans une langue et un format accessibles à la majorité ?			
	Criticité en cas de perte	Perdre cette ressource aurait-il un impact majeur sur l'enseignement ou la recherche ?			

Adapté de (Konstantelos, Yan 2023; DPC 2024b; Guirlet 2020; Tavernier, and Carlson 2021)

Au niveau technique, la priorité est donnée aux formats ouverts, interopérables, dotés de métadonnées standardisées et d'identifiants pérennes (DOI, ISBN, ARK), facilitant une restauration indépendante des fournisseurs. Les contraintes d'extraction et le volume des données à traiter sont également pris en compte. Du point de vue quantitatif, l'usage réel, la fréquence des consultations, l'impact académique, et les modalités d'accès post-résiliation permettent d'identifier les ressources stratégiques tout en préservant la diversité documentaire et les contenus de niche vulnérables. Enfin, la dimension qualitative évalue la valeur institutionnelle, patrimoniale ou pédagogique des ressources, la clarté contractuelle, la stabilité du fournisseur et les possibilités de mutualisation. Il revient ensuite à l'institution de définir, selon son propre contexte stratégique, ses contraintes opérationnelles et ses engagements contractuels, le poids relatif à accorder à chaque critère de la grille. L'analyse suppose donc de croiser les informations issues des contrats de licence, des rapports d'usage, des outils de gestion documentaire (SIGB) et des référentiels extérieurs (DOAJ, Keepers Registry<sup>9</sup>, bibliométrie, archives existantes...).

Par exemple, l'analyse des connexions via OpenAthens permet de prioriser les ressources électroniques les plus utilisées par les HUG, notamment celles essentielles à la pratique clinique. Cette approche, fondée sur les données de trafic, offre une base objective pour garantir un accès pérenne aux ressources les plus critiques si elles venaient à devenir indisponibles, en cohérence avec l'accord de service entre les HUG et l'UNIGE.

Ce travail peut être réalisé à l'échelle de la ressource (ebooks, revues, articles, plateformes), du fournisseur ou du bouquet documentaire, en tenant compte des interdépendances entre contenus, des accès partagés ou des duplications. L'objectif n'est pas d'atteindre une exhaustivité immédiate, mais de documenter des choix argumentés, fondés sur la réalité contractuelle, l'usage académique et les capacités techniques de sauvegarde, dans une perspective de pilotage progressif. Ce classement permet d'orienter les premiers efforts de sécurisation (exports, archivage local ou tiers, scénarios de contingence) sur les ressources les plus sensibles, tout en engageant une démarche pérenne de maîtrise des collections électroniques dans l'écosystème documentaire académique.

#### 4.6.4 Protection des actifs

La protection des actifs informationnels vise à garantir leur disponibilité, leur intégrité et leur confidentialité, en cohérence avec les principes énoncés par les normes ISO 27005 et ISO 27002 (ISO 2018; 2022a). Cette étape repose sur la mise en place coordonnée de mesures organisationnelles, techniques et contractuelles, adaptées selon le niveau de criticité défini lors de la priorisation des ressources. Elles doivent également être adaptées à notre contexte, afin d'assurer à la fois la protection de l'accès courant, la pérennité de l'accès à long terme, et la préservation numérique par l'archivage. Sur le plan organisationnel, la désignation explicite d'une personne responsable par catégorie d'actifs, ainsi que la mise en place d'un comité de pilotage transversal, permettent une gouvernance claire et réactive.

---

<sup>9</sup> Le Keepers Registry est un registre initié par le JISC et géré par l'ISSN International Centre qui recense, pour chaque revue électronique identifiée, les programmes de préservation chargés de son archivage à long terme. En agrégeant ces données, il permet aux bibliothèques de vérifier la couverture archivistique des collections, d'identifier les titres non protégés et d'orienter leurs négociations ou les investissements en conservation.

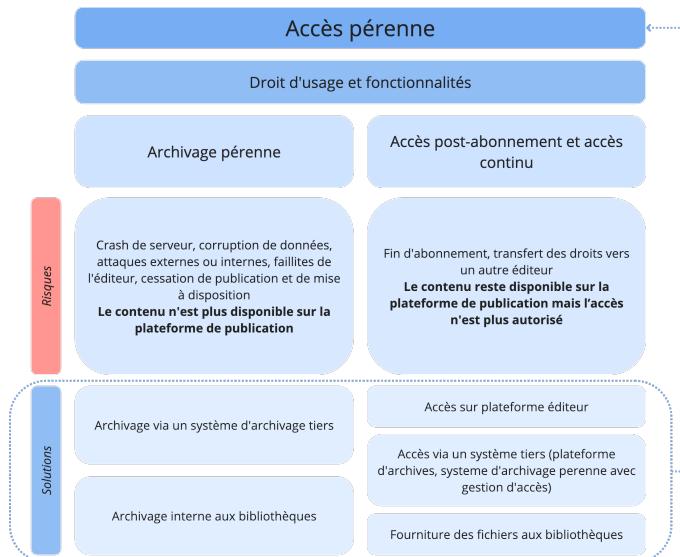
D'une part, la mise en œuvre de dispositifs techniques tels que la sécurité renforcée, la réPLICATION et les sauvegardes externalisées, l'archivage pérenne et de moyens d'accès alternatifs est essentielle. D'autre part, la création et la gestion indépendante d'un registre recensant les clauses contractuelles établies avec les fournisseurs de ressources électroniques et les prestataires de services, encadre les engagements pour prévenir les risques liés aux défaillances du système principal. Ainsi, il est recommandé d'intégrer des clauses explicites de disponibilité dans les accords de niveau de service (SLA) ainsi que les clauses stipulant les délais de récupération et d'indisponibilité maximales (RTO et RPO). Pour les fournisseurs de contenus électroniques, il est nécessaire d'inscrire dans ce registre mais d'abord dans les contrats des garanties précises relatives à l'accès pérenne aux ressources acquises. Ces clauses d'accès perpétuel, assurent la continuité de l'accès même après la fin d'un abonnement ou d'une licence, ou d'un « accès post-résiliation », permettant à l'institution de conserver un droit d'utilisation durable des contenus précédemment acquis (Ferracci 2016; Alexandre 2015; Metrat, Oury 2017). La notion d'accès pérenne recouvre deux dimensions :

- L'accès post-abonnement (*post-cancellation access*) concerne le droit d'accéder aux contenus souscrits après la fin de l'abonnement. Il dépend des clauses négociées et peut inclure des cas comme les transferts de droits ou l'arrêt de publication.
- La préservation à long terme va au-delà du cadre contractuel pour garantir la conservation durable des contenus numériques (ISO 2025a), en couvrant les risques technologiques et institutionnels. Un « événement déclencheur » justifie alors l'activation d'un accès alternatif.

(Beagrie 2013)

Les contrats doivent prévoir l'obligation contractuelle de livrer régulièrement les données sous des formats normalisés et ouverts qui garantit la réversibilité et l'indépendance à long terme de l'institution, la possibilité d'audits externes, ainsi que des clauses de sortie.

Figure 12 - Les composantes de l'accès pérenne des ressources électroniques

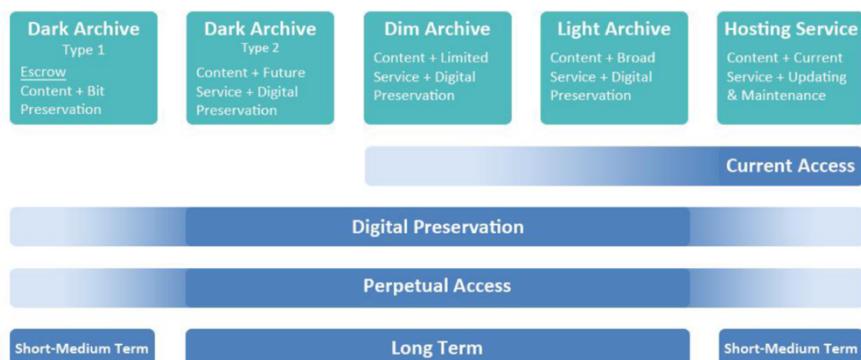


(Alexandre 2014)

L'ensemble de ces précautions vise à prévenir les risques de rupture de service ou de perte d'accès aux ressources critiques en cas de défaillance technique ou commerciale du prestataire comme présentée dans la Figure 12.

D'un point de vue technique, les ressources critiques exigent une protection comprenant notamment la redondance et la réplication des données, des contrôles réguliers d'intégrité via des vérifications automatisées des empreintes numériques (checksums), et des mécanismes robustes de chiffrement. En particulier, les actifs jugés critiques bénéficient d'une sauvegarde hors ligne indépendante et sécurisée. La préférence pour des formats ouverts et interopérables, ainsi que l'utilisation d'identifiants pérennes, renforce encore davantage la résilience documentaire face aux risques de dépendance (Eve 2024).

Figure 13 - Concepts et propriétés de solutions d'archives



(Charles Beagrie Ltd 2009)

L'archivage des revues repose sur plusieurs modèles (Figure 13), différenciés par le niveau d'ouverture des contenus et les garanties de préservation. On distingue généralement :

- Les *dark archives* assurent une conservation sécurisée, mais non accessible au public. Les contenus sont stockés en prévision d'un événement déclencheur, qui activerait leur diffusion. Les infrastructures reposant sur LOCKSS en sont des exemples.
- Les *dim archives* représentent un modèle intermédiaire, les contenus y sont préservés avec un accès restreint à certaines communautés (universités, chercheurs), et peuvent être rendus publics selon des conditions spécifiques.
- Les *light archives* garantissent un accès libre, immédiat et permanent aux contenus pour tous les utilisateurs. Ce modèle favorise la diffusion et la réutilisation des savoirs.
- Enfin, les services d'hébergement permettent la mise en ligne mais sans offrir les garanties associées à une archive. Ils assurent un accès continu (Metrat, Oury 2017).

Malgré la présence de clauses d'accès perpétuel dans les contrats, leur mise en œuvre dépend d'une gestion documentaire exigeante. Par exemple, à l'Université de Californie, l'interruption des négociations avec Elsevier a soulevé la question du maintien de l'accès aux archives. Si l'éditeur garantissait un accès perpétuel, il incomberait à l'établissement de reconstituer la liste exacte des titres concernés pour activer la récupération (Polchow, NASIG 2020). À l'Université du Colorado, un éditeur a fourni des contenus sur clé USB, sans que l'université ne dispose d'un système adéquat pour les héberger (Polchow, NASIG 2020). Un autre point d'attention concerne les mécanismes d'archivage tiers. Si des organisations telles que Portico, CLOCKSS assurent une forme de pérennité, les bibliothèques ne sont souvent pas directement impliquées dans les accords de conservation. Le contenu n'est accessible qu'en cas d'« événement déclencheur » et l'accès effectif dépend du respect de clauses restrictives. L'intégration du contrôle de l'accès perpétuel dans les pratiques professionnelles est un levier qui suppose de conserver les preuves d'acquisition, de surveiller les modifications contractuelles, et d'inclure les services d'archivage dans les flux de traitement. L'accès

perpétuel repose aussi sur une stratégie incluant gouvernance, suivi des ressources, et coopération interinstitutionnelle (Polchow, NASIG 2020).

La proposition de ce mémoire s'attache à la sauvegarde du catalogue qui est l'actif critique permettant de rassembler les données issues des applications identifiées comme les plus critiques. Bien qu'elle puisse venir dans un second temps, la question de la sélection raisonnée des contenus à préserver devient rapidement la suite logique des démarches à entreprendre. Il s'agit d'adopter une posture curatoriale : tout ne peut ni ne doit être conservé indéfiniment. La notion de « *scholarly record* » implique une évaluation des contenus jugés significatifs pour les générations actuelles et futures, dans une logique de durabilité aussi bien scientifique qu'environnementale (Hedley 2025). Dans un contexte d'explosion du volume de données numériques, la préservation ne peut être qu'un processus de tri, et non un archivage exhaustif (Kastellec 2012).

La question de la priorisation ne peut être tranchée de manière univoque et ne trouvera pas de réponse définitive dans le cadre de ce mémoire (Annexe 13). Cette démarche doit concilier les impératifs de préservation du patrimoine documentaire avec les contraintes et les ressources disponibles. Une mutualisation des efforts mérite d'être envisagée afin de promouvoir une approche communautaire. L'archivage pérenne en bibliothèque reste encore peu développé, relégué derrière des priorités plus immédiates et freiné par sa technicité et son coût (Ferracci 2016). L'archivage est un acte de mémoire mais aussi un acte de choix. La sélection devient ainsi une fonction stratégique de la bibliothèque, la plus compétente pour engager des arbitrages, en concertation avec les parties prenantes pour garantir que les ressources critiques soient effectivement disponibles en situation d'urgence et transmises aux générations futures.

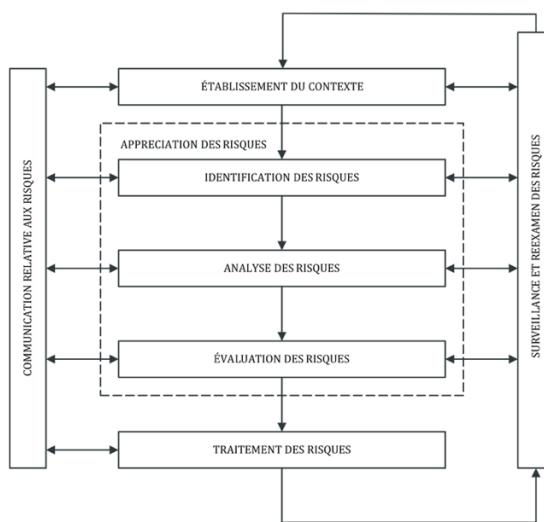
## 5. Gestion des risques et gouvernance de l'information

Maintenant que l'on a pu identifier les vulnérabilités, comprendre les menaces qui pèsent sur les systèmes d'information des bibliothèques et prioriser les actifs qu'il convient de protéger ; il s'agit de convertir ces éléments en risques compromettant les objectifs de sécurité (ISO 2020). « Le risque est fonction de la probabilité qu'une menace donnée exploite une vulnérabilité donnée, et de l'impact potentiel de cet événement sur l'organisation » (Ross et al. 2021). Le choix entre une approche proactive ou réactive en matière de gestion des risques dépend de la posture de l'organisation face à l'incertitude. Une démarche proactive repose sur l'identification préalable des actifs à protéger et l'analyse des risques (Ghernaouti, Aghroum 2012). Elle vise à prévenir les incidents, à réduire leur occurrence et à en limiter les effets. À l'inverse, une démarche réactive se concentre sur la réponse à l'incident, elle consiste à contenir l'événement, à limiter les pertes et à restaurer les capacités opérationnelles. Dans un contexte où le risque zéro n'existe pas, il est indispensable de combiner prévention et réaction pour garantir la continuité et la résilience des activités.

### 5.1 Appréciation des risques

La gestion du risque permet l'analyse, l'évaluation, l'appréciation et le traitement des risques, afin d'identifier, estimer, comparer et atténuer les menaces pesant sur l'organisation et de maintenir celles-ci sous contrôle (ISO 2020; Ghernaouti 2022). Les menaces les plus graves étant souvent imprévues, aucune méthode ne garantit l'exhaustivité, mais elles offrent un cadre qui doit être mobilisées de façon adaptée au contexte (Cordel 2019). Si les bibliothèques apparaissent souvent comme des victimes, elles n'en demeurent pas moins juridiquement responsables des données qu'elles traitent. Il convient d'identifier, d'analyser et d'évaluer les risques encourus. L'approche proposée (Figure 14) permet de guider les choix stratégiques de sécurité à mettre en place au niveau de la DIS.

Figure 14 - Processus de gestion des risques ISO 27005



(ISO 2018)

La gouvernance interne en matière de sécurité impose une répartition des responsabilités entre la gestion de la sécurité des données et l'évaluation de la criticité des services informatiques. Chaque entité métier est ainsi tenue d'évaluer la sensibilité de ses propres opérations. Ce travail repose sur une méthode d'analyse de l'impact sur l'activité (BIA ou

*Business Impact Analysis*). Elle consiste à interroger les services sur les impacts concrets d'une interruption de leurs outils numériques (Annexe 15). Ces évaluations permettent de déterminer le niveau de criticité réel des services et d'établir, les objectifs de temps de rétablissement (RTO ou *recovery time objective*) et les objectifs de point de reprise (RPO ou *recovery point objective*) adaptés. Ce processus conduit à une classification des services numériques essentiels, prérequis indispensable à la mise en œuvre cohérente de mesures de continuité. La maturité est variable selon les services, certains domaines ont déjà entrepris une démarche avancée d'identification des données sensibles et des services numériques critiques, souvent dans le cadre d'une refonte de leurs SI et donc d'une proximité plus étroite avec les services IT. La résilience vise à maintenir la continuité sans interruption, tandis que la récupération intervient après un incident ; les objectifs RTO/RPO doivent être définis en fonction des besoins métier, et non selon des standards uniformes (Wright 2024).

A l'UNIGE, un service numérique essentiel est une application fournie par la DiSTIC aux équipes métiers, dont l'interruption pourrait compromettre la mission de l'institution. Il s'agit de services applicatifs, identifiés comme indispensables à la suite des bilans d'impacts sur les activités (BIA) (UNIGE 2021b). La proposition est d'inclure les actifs de notre système mais également la solution imaginée dans la notion de services numériques essentiels, d'abord par leur identification, leur caractère indispensable à la réalisation de la mission et leur criticité impactant la continuité de l'activité de la bibliothèque (Annexe 15). L'institution pourra ainsi intégrer ces éléments au plan de reprise d'activité. Nous redéfinirons alors un service numérique essentiel comme toute composante technologique, applicative ou informationnelle dont l'interruption ou l'altération compromettrait directement la continuité des missions fondamentales de la Bibliothèque universitaire, l'accès à l'information scientifique, le soutien à l'enseignement et à la recherche, ou la préservation du patrimoine académique.

Les dépendances techniques comme les plateformes d'authentification, les mécanismes de sauvegarde, de restauration des données et les dépôts institutionnels sont actuellement déjà couvertes par un BIA validé ou en attente de validation par le comité de pilotage PRA. Par ailleurs, le PRA n'inclut pas les services externes non hébergés dans les centres de données de l'UNIGE, lesquels sont supposés rester opérationnels durant un sinistre. Les services numériques essentiels basés sur le cloud, les applications SaaS sont hors du périmètre du PRA. Malgré l'externalisation du SIGB qui suggère le transfert du risque au fournisseur la bibliothèque demeure responsable de l'évaluation des impacts métiers en cas d'indisponibilité. La réalisation d'un BIA est alors indispensable pour déterminer les conséquences concrètes sur les activités documentaires et les publics concernés. Ce processus permet de définir les seuils de tolérance, de formuler les exigences contractuelles et d'anticiper des mesures de continuité, procédures de secours ou accès alternatifs.

### 5.1.1 Identification des risques

L'identification des risques permet de repérer les événements ou situations susceptibles d'empêcher le système ou l'organisation d'atteindre ses objectifs (Cordel 2019). Elle consiste à reconnaître, analyser et enregistrer les sources de menaces potentielles, en évaluant leur nature, leur localisation, leur temporalité et les pertes qu'elles pourraient engendrer (ISO 2018). Elle permet ainsi de fournir une vision des vulnérabilités du système et des facteurs pouvant compromettre sa sécurité ou sa performance globale.

La méthode retenue (Annexe 16) s'appuie sur une approche intégrée, afin d'assurer une couverture aussi large que pertinente de l'univers des risques. Les entretiens individuels, ont permis l'expression nuancée des situations rencontrées, et de capter une information contextualisée (Cordel 2019). Ce matériel qualitatif a ensuite été croisé avec des référentiels (Annexe 1) ainsi qu'avec les études de cas (Annexe 8), afin d'objectiver les scénarios (Annexe 22) et d'identifier des événements redoutés réalistes.

La cartographie des risques s'appuie sur norme ISO/IEC 27005 et la méthode EBIOS Risk Manager. Le cadre du NIST Cybersecurity Framework v2.0(NIST) a été mobilisé pour structurer l'ensemble de la démarche de sécurité métiers elle est articulé autour de cinq fonctions qui ont inspirés et construit la démarche employée pour ce travail :

- *Govern* : définir les politiques, responsabilités, priorités et processus de gouvernance
- *Identify* : identifier les actifs et les risques,
- *Protect* : mettre en œuvre des mesures de protection,
- *Detect* : détecter les événements,
- *Respond* : réagir aux incidents,
- *Recover* : rétablir les capacités après une attaque.

La structure de la cartographie est quant à elle un emprunt du modèle de référence COSO II (annexe 16) qui dans le contexte de la gouvernance de l'information, permet de structurer l'analyse des risques liés aux actifs, d'identifier les points de vulnérabilité, et de concevoir des dispositifs de contrôle. Utilisé par la Ville de Genève dans la gestion de risques liées à la gouvernance de l'information et la Bibliothèque de Genève pour les phases préventives d'analyse de risques pour ses collections physiques (Entretien VdG, 2025). L'analyse intègre également les vulnérabilités critiques recensées dans le Top 10 OWASP (OWASP 2021), les scénarios issus des processus SSI internes, ainsi que les rapports de veille de l'*European Union Agency for Cybersecurity* (ENISA), en particulier le *Threat Landscape Reports* (ENISA 2024), qui offrent une vision des principales menaces pesant sur les infrastructures y compris dans le secteur de l'éducation et de la recherche.

Nous intégrons également la nature des risques de la préservation numérique qui doivent être appréhendés de manière globale et croisée. Ceux-ci incluent des risques environnementaux, organisationnels, technologiques, ainsi que ceux liés aux supports d'enregistrement ou à l'accessibilité technique (Banat-Berger, Duplouy, Huc 2009). On distingue notamment les risques physiques, les pannes d'infrastructure ou les catastrophes naturelles. Les risques humains, qu'ils soient accidentels ou intentionnels, et les risques techniques liés à l'obsolescence rapide des formats et des supports. À cela s'ajoutent les risques organisationnels, tels que les faillites financières, juridiques ou managériales (Rosenthal et al. 2005 ; Alexandre 2014). En croisant ces risques avec ceux d'origine cyber, il devient possible d'identifier des points de convergence dans les stratégies de mitigation, et d'envisager des mesures partagées. Les résultats identifient 48 éléments de risques regroupés dans neuf typologies (Annexe 16) de risques recensés :

- Cyber : liés aux intrusions, attaques, malwares, et compromissions du SI.
- Technologiques, d'infrastructure : défaillances matérielles, logicielles, réseau.
- De dépendance : concentration, externalisation ou services critiques tiers.

- Politiques et géopolitiques : instabilité réglementaire, sanctions, conflits internationaux.
- Internes : erreurs humaines, malveillance interne ou insuffisance des procédures.
- Informationnels : la qualité, la confidentialité, l'intégrité ou la disponibilité des données.
- Opérationnels, logistiques : les processus, l'approvisionnement ou la continuité.
- Gouvernance : absence de pilotage stratégique, de cadre normatif, de supervision.
- Émergents : évolutions technologiques, sociétales, environnementales peu maîtrisées.

Une fois identifiés, les risques doivent être réévalués de façon continue grâce aux fiches individuelles de suivi des risques (annexe 16) qui prend en compte le niveau d'exposition aux risques bruts et conditionne les choix stratégiques pour leur traitement (Cordel 2019).

### 5.1.2 Analyse des risques

L'objectif de l'analyse est de déterminer le niveau d'impact (Tableau 6) pour mesurer la gravité des conséquences qu'un incident de sécurité portant sur un actif peut engendrer pour l'UNIGE, ses usagers ou ses partenaires.

Tableau 6 - Niveaux d'impact sur l'organisation

	Impacts d'une interruption de l'activité (synthèse)
Niveau 1	<b>Faible ou aucune nuisance interne sur l'activité</b> <ul style="list-style-type: none"> <li>ou une dizaine à cent utilisateur-trice-s standards concerné-e-s</li> <li>ou impacts sur l'image limités à quelques personnes (internes)</li> <li>ou aucun impact juridique</li> <li>ou impacts financiers (couverts par le budget etc.) faibles à l'échelle de</li> </ul>
Niveau 2	<b>Désorganisation significative et temporaire sur les activités</b> <ul style="list-style-type: none"> <li>ou cent à plusieurs centaines utilisateur-trice-s ou un VIP concerné-e-s</li> <li>ou impacts modérés sur l'image (internes ou externes)</li> <li>ou impacts juridiques faibles ou incertains (non confirmés)</li> <li>ou impacts financiers à court terme (perte de revenue, retard de paiement,</li> </ul>
Niveau 3	<b>Désorganisation majeure et durable sur les activités</b> <ul style="list-style-type: none"> <li>ou plusieurs centaines à un millier d'utilisateur-trice-s ou un/plusieurs</li> <li>ou impacts forts sur l'image (internes et/ou externes)</li> <li>ou impacts juridiques forts confirmés (responsabilité de l'UNIGE engagée)</li> <li>ou impacts financiers à court terme (perte de revenue, retard de paiement,</li> </ul>
Niveau 4	<b>Désorganisation critique et durable sur les activités impactant l'UNIGE ou</b> <ul style="list-style-type: none"> <li>ou plusieurs milliers d'utilisateur-trice-s un/plusieurs VIP concerné-e-s</li> <li>ou impacts très forts sur l'image de marque de l'UNIGE (internes et externes)</li> <li>ou impacts juridiques forts confirmés (responsabilité de l'UNIGE engagée)</li> <li>ou impacts financiers à court et/ou long terme (plan budgétaire etc.) forts à</li> </ul>

(UNIGE, 2024)

Une compromission peut affecter la capacité à assurer la mission institutionnelle, à respecter les obligations légales ou contractuelles, à préserver la réputation de l'institution, à maintenir la confiance des parties prenantes, à garantir les droits fondamentaux à la vie privée, ou encore à éviter des effets en cascade sur des entités dépendantes. L'analyse des besoins des utilisateurs permet de déterminer le niveau d'impact les activités et le niveau de disponibilité attendu pour chaque application pour concevoir des solutions de continuité proportionnées. Dans cette logique, la mise en œuvre du BIA (Annexe 15) constitue une étape déterminante. La continuité des activités métiers dépend de ressources de différentes natures, il a pour objet d'obtenir une compréhension des services clés des entités métiers concernées, de déterminer les priorités et les délais pour la reprise des activités et d'identifier les ressources nécessaires à la reprise d'activité. Elle permet d'identifier les processus critiques, d'en évaluer la dépendance aux actifs et d'estimer les conséquences d'une interruption sur les plans opérationnel, financier ou juridique.

À partir de cette analyse, et de la criticité relevée deux indicateurs sont définis pour orienter la stratégie de continuité. Le RTO qui détermine le délai maximal acceptable d'interruption d'un service, et le RPO qui fixe la durée maximale de perte de données tolérable entre deux sauvegardes. Un troisième indicateur peut être utilisé la Durée d'interruption maximale admissible (DIMA), qui correspond au seuil critique au-delà duquel l'indisponibilité d'un service compromet de manière irréversible les capacités opérationnelles ou stratégiques de l'organisation. Ensemble, ces paramètres constituent une planification de la continuité d'activité. Ils permettent de choisir les solutions techniques les plus adaptées aux besoins de sécurité. Celles permettant de redémarrer rapidement une activité, en minimisant la perte de données sont généralement les plus couteuses (Adenium 2018). Elles doivent correspondre à l'équilibre entre la valeur de l'actif et la dépense en ressources nécessaire à sa protection (Wright 2024).

L'analyse des risques appliquée aux ressources électroniques présente une spécificité. Contrairement à d'autres secteurs comme la santé ou l'industrie, l'impact d'une indisponibilité ne se traduit pas directement par une perte de vies humaines (Poupart 2018) ou une chute mesurable de chiffre d'affaires (Déon 2023). Cette absence d'enjeu vital ou financier immédiat complique la quantification du risque. Il en résulte une difficulté à établir des seuils de criticité ou de tolérance à l'indisponibilité. L'analyse d'utilisation peut devenir ainsi un indicateur de criticité indirect. Pour valoriser la perte on peut tenter de déterminer le taux horaire perdu des ETP si leur outil de travail principal est rendu inutilisable. Cette démarche indicative, nécessiterait d'être approfondie pour obtenir une métrique précise et la mettre en avant auprès des décideurs.

### 5.1.3 Évaluation des risques

Le résultat des risques identifiés dans le contexte des bibliothèques académiques peut être résumés de la manière suivante :

- Perte définitive : vol, destruction, défaillances sans possibilité de récupération.
- Indisponibilité temporaire : mêmes types d'incidents avec la possibilité de restauration.
- Détérioration des données : virus, défaillances, ou erreurs humaines.
- Accès non autorisé : sécurité insuffisante, intrusions malveillantes, erreurs humaines.
- Modification non autorisée : altérations, mêmes vecteurs que les accès illicites.
- Lecture impossible : obsolescence des formats des équipements.
- Compréhension impossible : mauvaise organisation, absence de documentation, ou perte du contexte informationnel, dissociation.

(Mesguich, Bermès, Saby 2023)

L'analyse de l'impact doit prendre en compte ces effets, et les répercussions financières, juridiques, réputationnelles ou celles liées à la protection des données personnelles. La démarche repose sur l'utilisation d'une matrice d'évaluation ou matrice de Farmer (Annexe16), outil visuel permettant de croiser ces deux axes pour positionner chaque risque selon son niveau de criticité (Cordel 2019). Une distinction est opérée ensuite entre le risque brut évalué avant l'application de mesures de sécurité et le risque net estimé après la prise en compte des dispositifs existants. Cette analyse permet ainsi de mettre en évidence les risques résiduels soit les risques persistants à la suite de leurs traitements. En parallèle, l'organisation doit

déterminer son seuil d'acceptabilité des risques, c'est-à-dire le niveau au-delà duquel une réponse doit impérativement être engagée. Cette étape renvoie à 13 risques critiques au sein de l'organisation cible (Annexe 17).

#### 5.1.4 Traitement des risques

Le traitement du risque ISO 27005 et ISO 31000 vise à déterminer et à mettre en œuvre les mesures appropriées pour modifier et agir sur le risque, en fonction de son niveau de criticité et de la tolérance de l'organisation. Quatre stratégies sont envisagées (ANSSI 2024b) :

- L'évitement du risque ou suppression
- La réduction ou mise en place de contrôles pour diminuer la probabilité ou l'impact
- Le transfert ou l'externalisation ou assurance
- L'acceptation ou le choix de ne pas intervenir, le risque est jugé acceptable

Le choix de la stratégie dépend du niveau de risque résiduel, des ressources disponibles, des obligations réglementaires et des impacts potentiels sur les activités. Les mesures mises en œuvre doivent être documentées, suivies et réévaluées pour s'adapter à l'évolution du contexte, des menaces ou des vulnérabilités. Ces risques spécifiques doivent également être replacés dans le cadre de la gouvernance des données numériques, tout système d'information repose sur l'équilibre entre accessibilité, sécurité, intégrité et pérennité des contenus.

La gouvernance des données implique de pouvoir garantir, sur le long terme, l'intégrité et la disponibilité des fichiers, mais aussi leur intelligibilité et leur traçabilité (contexte, provenance, historique des modifications). Cela suppose de maîtriser des risques transversaux, tels que :

- L'obsolescence technologique : disparition des supports matériels, des formats de fichiers ou des logiciels nécessaires à l'ouverture des documents.
- La perte de contexte : absence de métadonnées descriptives, techniques ou administratives rendant les fichiers difficilement compréhensibles ou exploitables.
- La fragmentation des responsabilités : manque de clarté dans la répartition des rôles entre acteurs, qui nuit à la continuité de la gestion documentaire.
- L'absence de politiques de conservation numérique explicites : suppressions arbitraires, pertes involontaires ou traitements non conformes aux obligations.
- La dégradation progressive des supports : en particulier pour les supports de stockage physiques, sujets à des pannes ou à une usure accélérée.
- L'absence de redondance géographique : les données conservées sur un seul site sont vulnérables en cas de sinistre, panne majeure, attaque ciblée.
- Le manque de contrôle sur les solutions externalisées : notamment dans le cadre de l'archivage, de l'hébergement dans des clouds commerciaux, où les bibliothèques peuvent perdre la maîtrise des conditions techniques et juridiques de conservation.
- La non-conformité aux standards d'interopérabilité : qui limite la migration des données vers d'autres systèmes et compromet leur accessibilité future.
- Le défaut de financement pérenne : une absence de stratégie budgétaire à long terme peut interrompre les dispositifs de préservation en cas de restrictions économiques.

La préservation à long terme des contenus numériques requiert une gouvernance soutenue par des ressources techniques, humaines et financières adaptées. Pour se prémunir de ces

risques spécifiques, et à l'instar des plans de conservation mis en place pour les ressources papier, un projet préventif de préservation des documents numériques peut être envisagé. Un archivage pérenne envisage pour chaque risque une réponse technique ou une action liée au management, plan d'urgence, duplication hors site, plan de sécurité des systèmes d'information, veille, contrôles, alertes, formation, accompagnement au changement, choix de formats à risques limités, collecte d'informations, etc..

## 5.2 Cartographies

Dans ce cadre, la cartographie des risques (Annexe 16) constitue un outil qui permet d'identifier, de qualifier et de hiérarchiser les menaces pesant sur les données et les services numériques, en tenant compte de leur probabilité et de leur impact potentiel. Elle est ici le résultat d'une approche par la cartographie des processus (Annexe 11), l'identification des actifs et par la conformité (Annexe 1).

### 5.2.1 Une approche par l'analyse des processus

Si les normes EBIOS (ANSSI 2024b) et le NIST CSF 2 (NIST 2024) ont constitué le socle pour l'évaluation des risques cyber, il a été nécessaire d'élargir le périmètre d'analyse en intégrant la norme ISO 27005 (ISO 2018) qui permet de mieux prendre en compte les risques informationnels (Entretien A.Rossier, 2025). Le NIST CSF 2 (NIST 2024) insiste sur la nécessité de comprendre l'organisation à travers ses processus critiques afin d'identifier les actifs numériques essentiels et les dépendances associées. De même, la norme ISO 27005 et la méthode EBIOS RM encouragent l'évaluation des risques à partir des besoins de sécurité appliqués aux processus de l'organisation (ISO 2018; ANSSI 2024b). L'analyse s'est aussi davantage centrée sur les impacts des risques que sur leurs causes, n'ayant à notre niveau que peu de moyens d'action sur cette variable.

Dans le contexte d'une bibliothèque académique au sein d'une université où le SI est hétérogène, distribué et interconnecté ; adopter une approche fondée sur l'analyse des processus métier permet d'adapter la cybersécurité aux priorités concrètes de l'organisation et d'en renforcer l'efficacité. Cette analyse est aussi nécessaire pour établir un dialogue commun entre les directions métiers, les équipes informatiques et les responsables de la sécurité de l'information. Elle permet une lecture fonctionnelle du SI, en mettant en relation les outils numériques et les fonctions critiques qu'ils soutiennent. La démarche permet d'identifier les ressources humaines impliquées, d'évaluer les impacts potentiels d'une interruption et d'en déduire une estimation des pertes économiques indirectes. Enfin, cette approche facilite et confirme la hiérarchisation des actifs numériques selon leur criticité métier, clarifie les responsabilités et recentre les efforts de sécurisation dans le cadre de la mise en place d'un plan de continuité.

Le tableau (Annexe 11), analyse 13 processus métiers de la bibliothèque. Chaque ligne du tableau identifie un processus, en précisant ses systèmes associés, les rôles impliqués, les périodes critiques, les valeurs de RTO et RPO estimées pour le processus, les coûts d'indisponibilité, ainsi que les dépendances techniques et humaines.

Tableau 7 - Exemple de processus critique identifié

Code	Processus	Sous-processus	Systèmes impliqués *	Acteurs / rôles responsables	Utilisateurs finaux	Critique (UNGE)	Justification	Impact DICA (ISO-27005)	Période critique	RTO (estimé)	RPO (estimé)	Coût estimé d'indisponibilité (CHF)*	Dépendances	Procédures contournement	Ressources minimales	Responsable
P3	Accès aux ressources électroniques	Authentification Consultation Résolution de liens Routage via proxy Consultation hébergement sur les plateformes éditeurs	Primo VE / Swisscovery Réservation de liens Prise de rendez-vous Plateformes éditeurs HP (AAI / SWITCH-edu-ID, OpenAthens) EZproxy Reverse-proxy Hébergement sur les plateformes éditeurs (ScienceDirect, Wiley, PubMed Central,...) - Saisi externes DNS interne (réseau)	Responsable ressources électroniques Data librairien Ingenieur IAM / IdP (DSI) Administrateur réseau (DSI)	Étudiants Chercheurs Enseignants Hébergeur Personnel signant	4	Interruption > 4 h bloque cours, recherche et support clinique pour potentiellement plus de 10 000 usagers. Toute la recherche et l'enseignement sont impactées. L'accès indisponible compromet directement l'activité pédagogique, la recherche et l'activité clinique.	C, I, D, A	Rentrée Examens Recherche Appel de financement Soumission de projets	4h	2h	12000. (productivité perdue + pénalités éditeurs + surcoût support)	Authentification Fédération SWITCH Accès IP Sécurité & DNS Certificats TLS Contrats éditeurs valides	Guides imprimés URLs alternatives Diffuser URLs directes + VPN Guides PDF hors-ligne	VPN, URLs directes VM IAP & EZproxy actives 1 admin réseau 1 bibliothécaire d'astreinte	Resp. e- ressources

CC BY NC Stephen Valot 2025

Il permet de confirmer les actifs informationnels critiques et les capacités de résilience de l'organisation. L'analyse identifie 5 processus critiques (niveau 4 de la grille d'impact), et fournit une base exploitable pour bâtir le plan de continuité. Les résultats confirment le rôle central du SIGB (revenant dans 9 des 13 processus) et de l'outil de découverte (6 occurrences) dans l'écosystème de la bibliothèque, en particulier pour la gestion et les accès à la collection. Elle identifie également la disponibilité en premier lieu puis l'intégrité comme les caractéristiques les plus critiques pour les processus de la bibliothèque. Les services d'authentification se révèle en réalité les plus critiques plus de 10 occurrences, mais sont déjà traités par une analyse d'impact au niveau de la division informatique.

### 5.2.2 Une approche par la conformité

Les bibliothèques peuvent s'appuyer sur un ensemble riche de normes et de cadres méthodologiques issus des domaines de la cybersécurité, de la continuité d'activité et de la préservation numérique (Annexe 1). En matière de gestion des risques, des approches comme EBIOS RM (ANSSI 2024b) et ISO 27005 (ANSSI 2024) sont conçues pour être adaptable et tenir compte des spécificités des environnements. Pour structurer la continuité d'activité, les normes ISO 22301, ISO 27031 et les guides opérationnels comme ceux de l'ANSSI ou du NIST sont pertinents pour planifier la reprise des services critiques après un incident. Pour le contrôle et l'amélioration continue dans une optique de management de la sécurité de l'information, les référentiels ISO 27001 (ISO 2022a) et 27002 (ISO 2022b), ainsi que le NIST 800-53 (NIST 2024), apportent des lignes directrices solides pour organiser les politiques de sécurité informationnelles, les contrôles d'accès et la gestion des incidents. Les normes ISO 27001 et 27002 notamment à travers l'usage des check-lists en annexes, permettent de formaliser la démarche a posteriori des exigences de sécurité et de révéler des vulnérabilités parfois non identifiées par une analyse uniquement contextuelle.

La préservation numérique s'appuie sur des standards reconnus comme OAIS (ISO 14721, 2025) pour le cadre général, METS et PREMIS pour les métadonnées, ISO 16363 pour l'audit de dépôts de confiance, ou encore les normes françaises NF Z42-013 et NF Z42-026 pour l'archivage électronique sécurisé et les systèmes d'archivage électronique (SAE).

Peu d'associations professionnelles dans le monde des bibliothèques se sont pleinement saisies des enjeux de cybersécurité. L'*International Federation of Library Association* (IFLA) a publié, une série de lignes directrices visant à structurer une culture de la sécurité numérique adaptée. Son « *Statement on Cybersecurity* » traite de la cybersécurité comme une exigence technique et un impératif institutionnel et éthique. Les bibliothèques sont des vecteurs d'accès équitables à l'information et doivent, ce faisant, « garantir la sécurité de leurs infrastructures, la protection des données personnelles et la résilience de leurs services » (IFLA 2020). La déclaration insiste sur la nécessité d'adopter des politiques de gestion des risques, de confidentialité et d'usage des ressources numériques, en prenant en compte l'environnement

technologique, les obligations réglementaires, mais aussi les principes fondamentaux de liberté intellectuelle (IFLA 2020). Elle recommande la mise en œuvre de politiques de minimisation des données, l'application du principe de moindre privilège, le chiffrement des communications, et le renforcement de la sécurité des points d'accès. Lorsque les bibliothèques ne disposent pas d'un contrôle total sur leurs systèmes, l'IFLA appelle à une action de plaidoyer auprès des institutions hôtes et des fournisseurs tiers pour garantir l'alignement avec les normes et bonnes pratiques (Welch 2019). La déclaration encourage la formation des personnels et la montée en compétence des usagers à travers des programmes d'éducation à la sécurité numérique. Les bibliothèques sont bénéficiaires et relais actifs d'une culture de cybersécurité. Ces recommandations concordent avec les standards de la série ISO 27000, qui constitue un socle pour structurer une approche résiliente, responsable et respectueuse des droits dans les systèmes informationnels. (IFLA 2022). Comme nous l'avons vu la cybersécurité n'est pas une thématique uniquement technique et réservée aux seuls départements IT, elle engage la responsabilité de chacun des acteurs en contact avec le système d'information (Ghernaouti 2022).

Une approche exclusivement normative peut paradoxalement masquer de réelles vulnérabilités, en favorisant une vision juridique et administrative de la sécurité au détriment d'une gestion proactive et individualisée des risques cybernétiques (NIST 2024). En effet les risques cyber ne doivent pas être appréhendés comme des événements isolés, mais comme des enchaînements structurés au sein d'une véritable chaîne d'attaque. Le modèle de la *Cyber Kill Chain*, développé par Lockheed Martin (Jiang et al. 2025), ordonne les différentes étapes nécessaires à la réussite d'une attaque (exemple dans l'étude de cas, Annexe 8), depuis la reconnaissance jusqu'aux actions sur l'objectif, exfiltration, destruction ou chiffrement des données. Ce modèle a été ensuite enrichi par le *framework* MITRE ATT&CK<sup>10</sup> (MITRE ATT&CK® 2025) qui permet la modélisation d'attaques et les moyens de les contrecarrer (Jiang et al. 2025). Les incidents majeurs résultent rarement d'une vulnérabilité exploitée isolément. Elles sont le produit d'un enchaînement d'étapes exploitant des failles multiples dans les processus, les configurations ou les comportements humains (Ghernaouti 2022).

La portée des *frameworks* demeure limitée sans adaptation. Chaque référentiel constitue une modélisation imparfaite d'une réalité technique et organisationnelle complexe, dont l'interprétation peut varier (Dellac 2024). Se contenter de répondre à des exigences normatives ou réglementaires centrées sur des contrôles statiques et déclaratifs ne permet pas de faire face à la complexité et à l'évolution rapide des modes opératoires adverses (Barnum 2022). La conformité est nécessaire, mais insuffisante prise seule. Une posture de sécurité résiliente suppose une capacité à détecter, interférer, contenir ou ralentir l'attaque à chaque maillon de la chaîne. Il s'agit de passer d'une logique de contrôle formel à une logique d'anticipation tactique. Leur efficacité dépend de la capacité des responsables à les adapter avec discernement aux spécificités de leur environnement pour une stratégie capable d'intégrer la nature évolutive et combinée des risques encourus.

---

<sup>10</sup> Le référentiel MITRE ATT&CK constitue une base de connaissances qui recense les tactiques, techniques et procédures (TTP) observées chez les cyber-adversaires. Il permet de modéliser leur comportement et de définir des contre-mesures. Dans cette taxonomie : les tactiques décrivent l'objectif général de l'attaquant ; les techniques précisent la méthode employée pour atteindre cet objectif. Les procédures détaillent l'implémentation concrète.

### 5.2.3 Lecture croisée par typologie et criticité

L'analyse présentée dans le registre de risques repose sur la volonté de hiérarchisation, appliquée à un large spectre de menaces susceptibles d'affecter la continuité, la sécurité et la pérennité des actifs numériques. Chaque risque est documenté selon un modèle incluant : les causes (facteurs déclenchants ou contextuels), les conséquences (effets sur la disponibilité, l'intégrité, la confidentialité, la réputation), une estimation de la probabilité de survenue, ainsi qu'une quantification de l'impact, décomposée en quatre dimensions : fonctionnelle (F), humaine (H), réputationnelle (R) et sur la prestation (P) (Tableau 8). Cette analyse produit une criticité brute par un score agrégé permettant de classer les risques selon leur gravité.

Tableau 8 - Échelle de criticité des risques

Critère	Niveau 1 (Faible)	Niveau 2 (Modéré)	Niveau 3 (Important)	Niveau 4 (Critique)
Financier	Impact absorbable par le budget courant.	Coût notable mais gérable sans mesures exceptionnelles.	Coût élevé nécessitant ajustements budgétaires ou projets reportés.	Coût très élevé (>100 kCHF) mettant en péril d'autres activités ou projets.
Humain	Aucun impact direct sur les personnes.	Stress ou surcharge temporaire pour certains personnels.	Impact important : fatigue, démotivation, tensions dans les équipes.	Atteinte grave : risques pour la santé mentale, turnover ou crise interne.
Réputationnel	Aucune atteinte ou atteinte minime locale.	Atteinte locale ou auprès d'un petit public ; impact gérable en communication.	Dégénération significative de l'image auprès de partenaires et du public.	Atteinte massive à la crédibilité institutionnelle nationale ou internationale.
Prestation	Service légèrement ralenti, sans blocage visible pour les usagers.	Dégénération du service perceptible mais alternatives disponibles.	Suspension partielle des services critiques, forte gêne pour les usagers.	Suspension totale de services essentiels (SIGB, accès numérique, plateformes pédagogiques).
Probabilité	Rare (<1 fois par 10 ans).	Occasionnel (1 fois tous les 5-10 ans).	Fréquent (1 fois tous les 1-5 ans).	Très fréquent (>1 fois par an).

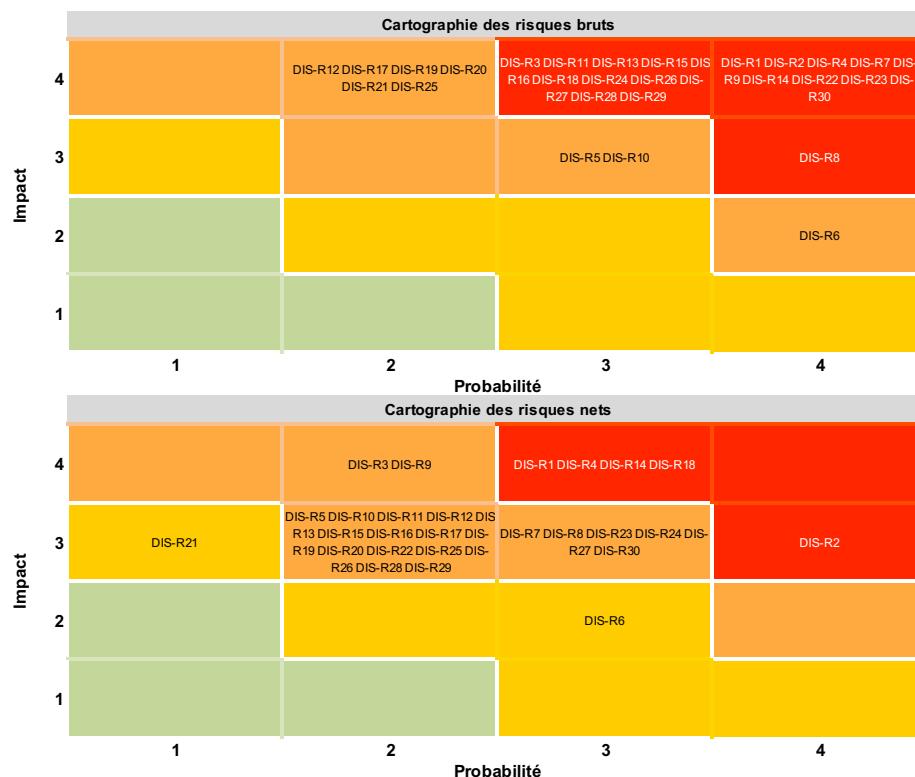
CC BY NC Stephen Valot 2025

Une relecture du risque et de sa criticité résiduelle est ensuite opérée à la lumière des mesures de sécurité envisagée. Cette criticité réévaluée permet d'apprecier l'efficacité du dispositif de maîtrise du risque. Deux indicateurs complémentaires peuvent renforcer l'analyse : La cinétique ou vitesse d'apparition de l'impact (instantanée, haute, basse) soit la vitesse de déroulement du phénomène avec laquelle les mesures doivent être compatibles. Et la priorité d'action, construite sur la base de la criticité résiduelle et du temps de réaction disponible.

### 5.2.4 Les risques prioritaires

Dans le cadre de la gestion des risques liés à la sécurité des services numériques de la bibliothèque, l'exemple de deux risques prioritaires aide à comprendre la structure de la grille d'analyse élaborée. Le risque d'attaque par *ransomware*, et les attaques par déni de service distribués. Le niveau de criticité initial (brut) est élevé pour les deux événements, atteignant un score de 16/16, puis recalculé après intégration des mesures de protection éventuelles pour aboutir à une criticité résiduelle encore significative (12/16). Cette modélisation permet d'objectiver les vulnérabilités critiques de l'écosystème et de prioriser les efforts en matière de prévention, de continuité et de réponse à incident, notamment en mobilisant les scénarios réels récents observés dans d'autres institutions académiques et en développant nos propres scenarios. Les traitements envisagés permettent de réduire la probabilité ou l'impact du risque. Enfin la responsabilité du risque est attribuée à l'entité en charge de son traitement. Ce travail d'analyse permet de positionner l'ensemble des événements identifiés sur la matrice de Farmer distinguant les risques bruts avant traitement et nets ou résiduels (Tableau 9) après mise en œuvre des mesures de maîtrise envisagées.

Tableau 9 - Matrices de criticité des risques bruts et nets



Adapté de (Inventaire des risques COSO II, Ville de Genève 2025)

La matrice offre une vision de l'exposition initiale de l'organisation et de l'efficacité des dispositifs, pour faciliter la priorisation, établir la planification des actions correctives, ainsi que l'optimisation des investissements de sécurité nécessaire pour renforcer la résilience globale et ajuster les dispositifs de continuité et de reprise. Les **13 risques critiques** identifiés pour la résilience des services numériques et la préservation du patrimoine de la Bibliothèque sont :

- *Ransomware et cryptolocker*
- Attaques par déni de service distribué (DDoS, DoS)
- Intrusion et *phishing*
- Robots et pratiques de *scrapping* automatisé, notamment via l'IA
- Obsolescence technologique
- Insuffisance des dispositifs de sauvegarde
- Dépendance aux solutions SaaS/IaaS
- PCA/PRA insuffisants
- Faillite d'éditeurs ou d'agréateurs de contenus numériques
- Erreurs humaines
- Pratiques de *Shadow IT* et négligences internes
- Perte de contexte et d'intelligibilité des contenus
- Problèmes de préservation numérique
- Fragilité du financement pérenne
- Restrictions budgétaires

Les solutions proposées pour répondre aux menaces prioritaires sont celles dérivées des études de cas et des entretiens dans une approche globale de la sécurité et de la résilience. Sur le plan technique, des mesures de protection sont intégrées, telles que la stratégie de sauvegarde 3-2-1, l'automatisation des restaurations, la segmentation réseau, et l'intégration de solutions d'analyse pour détecter et bloquer les comportements malveillants. La lutte contre les attaques DDoS repose sur des dispositifs de services de filtrage, architecture redondante, gestion de la charge, et détection comportementale. En matière d'authentification et de lutte contre le phishing, le recours systématique à l'authentification multi-facteurs, à la formation continue, à la surveillance des accès et à des politiques de mots de passe renforcées contribue à réduire les vecteurs d'intrusion. Pour répondre aux enjeux d'obsolescence, une veille active, la migration vers des formats ouverts ont été intégrées, tout comme l'adoption de solutions certifiées. La gestion des dépendances contractuelles s'appuie sur des clauses de sauvegarde et de récupération des données, la participation à des solutions d'archivage mutualisées et une diversification des fournisseurs. Par ailleurs, une attention particulière est portée à la continuité d'activité, sujet central de cette étude. Les plans formalisés, exercices réguliers, cellules de crise, et responsabilités doivent être en place et bien attribuées. Sur le plan organisationnel, la formation continue, la sensibilisation aux risques, et l'amélioration des processus interservices permettent de renforcer la sécurité et la fiabilité des pratiques. Enfin, des stratégies économiques diversifiées sont imaginées, la mutualisation des coûts entre services, facultés et entre institutions visent à assurer la pérennité du modèle, dans un contexte marqué par l'incertitude budgétaire.

## 5.3 Modèles et leviers de gouvernance

Il s'agit de penser un modèle de gouvernance qui s'inscrit dans la droite ligne des ambitions stratégiques de l'Université de « faire de la cybersécurité une priorité » (Ambition 4) et de soutenir un « numérique responsable, sobre et souverain » (Ambition 3). Cette démarche s'inscrit dans la feuille de route 2025–2030 sur la souveraineté numérique (UNIGE 2025b). Le mémoire répond aux exigences de résilience face aux menaces numériques, mais il promeut aussi une approche durable et responsable, fondée sur l'indépendance technologique, la gouvernance renforcée des données critiques et l'usage raisonné de solutions open source.

### 5.3.1 Appuis institutionnels

La DiSTIC, en tant que division informatique centrale de l'Université, constitue l'interlocuteur de référence pour toute intervention technique en situation d'urgence. Chargée de la coordination opérationnelle des services numériques, elle assure la gestion des incidents touchant les infrastructures internes et agit comme point de contact privilégié pour relayer les démarches vers les prestataires externes. Son rôle est essentiel pour assurer une réponse rapide, structurée et conforme aux procédures en particulier dans le cadre des plans de continuité d'activité et de reprise après sinistre

Plusieurs structures peuvent constituer des appuis à la gouvernance de la sécurité pour la bibliothèque. L'Office fédéral de la cybersécurité (OFCS), est chargé d'être le premier interlocuteur des milieux économiques, de l'administration, des établissements d'enseignement et de la population pour toutes les questions portant sur cette thématique. Il assure la mise en œuvre de la Cyber-Stratégie Nationale (ESRI 2024) pour rendre la Suisse plus sûre dans le cyberespace. Il contribue à l'élaboration des politiques publiques numériques cantonales en cybersécurité, fournissant un cadre stratégique suivi par l'Université, y compris

pour la Bibliothèque. En cas d'incident majeur affectant plusieurs institutions, l'OFCS peut faciliter une coordination logistique et technique. Par ailleurs, ses interactions régulières avec les services de sécurité informatique de l'UNIGE favorisent le partage d'informations et de bonnes pratiques. L'OFCS n'offre pas de soutien opérationnel direct, à la différence de SWITCH-CERT, le *Computer Emergency Response Team* du secteur académique, spécialisée dans la gestion des crises cyber, qui est un interlocuteur privilégié en cas d'attaque. Ce service est un atout stratégique, et offre une capacité de réponse face aux attaques ciblant les infrastructures éducatives et culturelles. SWITCH propose également un environnement cloud souverain, adapté aux standards du monde académique suisse, pouvant être envisagés dans des projets de redondance ou d'hébergement alternatif alignée avec des garanties en matière de sécurité et de conformité.

À ces appuis s'ajoutent d'autres acteurs à mobiliser selon la nature de l'incident : l'Office fédéral de la justice ou le Préposé fédéral à la protection des données pour les aspects réglementaires, et la police cantonale en cas d'actes de cybercriminalité. En Suisse, la Loi fédérale sur la protection des données (LPD), en vigueur depuis septembre 2023, aligne la législation sur le RGPD. Elle renforce les droits des personnes et impose aux responsables de traitement des obligations strictes en matière de sécurité, de transparence et de notification en cas de violation de données (Confédération Suisse 2024). La gouvernance de la cybersécurité des bibliothèques universitaires repose donc sur une coordination étroite entre ces différentes instances.

### 5.3.2 Le cadre légal

En vertu de l'article 74b, de la Loi sur la Sécurité de l'Information, les universités sont désormais soumises à l'obligation d'annoncer toute cyberattaque susceptible d'avoir un impact sur la disponibilité, l'intégrité ou la confidentialité de leurs systèmes (Conseil Fédéral 2024). Cette récente obligation est précisée par la nouvelle ordonnance sur la cybersécurité (OCyS) entrée en vigueur le 1er avril 2025. Elle impose aux institutions concernées de notifier l'OFCS dans un délai de 24 heures après la détection d'un incident, avec un ensemble d'informations techniques et organisationnelles détaillées. Cette évolution réglementaire renforce le rôle des universités dans l'écosystème national de résilience numérique, et formalise son positionnement au sein des infrastructures critique du pays. Elle implique également une coordination plus étroite entre les dispositifs de sécurité internes et les autorités fédérales, ainsi qu'un effort accru de conformité, de documentation et de réactivité. Cette inscription dans le périmètre légal des infrastructures critiques confère une responsabilité qui inclus les enjeux de souveraineté et de responsabilité publique (Tistoune, Fischer 2025).

En matière de préservation il est nécessaire également d'avoir en considération la loi sur le droit d'auteur (LDA) (Conseil Fédéral 2020). L'article 24 (Conseil Fédéral, 2020) autorise, à des fins de conservation, la réalisation de copies d'archives ou de copies de sécurité d'œuvres, à condition qu'elles soient conservées dans des fonds non accessibles au public. Le paragraphe 1bis étend cette autorisation aux bibliothèques, musées, établissements d'enseignement, et archives publics ou accessibles au public. L'article 24d autorise la reproduction d'œuvres à des fins de recherche scientifique, lorsque celle-ci est rendue nécessaire par un procédé technique et que l'accès à l'œuvre est licite. Les copies ainsi produites peuvent être conservées à des fins d'archivage. Néanmoins, ces dispositions restent conditionnées par une territorialité, une finalité non commerciale, et imposent des modalités strictes d'archivage et de conservation, excluant toute diffusion publique.

L'article 24e LDA (Conseil Fédéral 2020) introduit une exception et permet aux institutions culturelles d'insérer, dans leurs catalogues en ligne destinés à valoriser leurs collections, de courts extraits d'œuvres ou d'exemplaires détenus, à condition que cette utilisation ne porte pas atteinte à l'exploitation normale de l'œuvre. Cette disposition vise à équilibrer les impératifs de valorisation patrimoniale avec les droits des créateurs. Elle constitue un fondement légal important pour les bibliothèques numériques, en permettant une visibilité minimale des œuvres dans les catalogues, tant que l'usage reste limité et non-commercial.

Pour aller plus loin dans une optique de plaidoyer pour l'*Open Science* la question de l'extraction du plein texte nécessiterait une loi comme celle adoptée au Pays-Bas.

« L'amendement de 2015 à la loi néerlandaise sur le droit d'auteur établit un droit inaliénable pour les auteurs d'articles scientifiques financés, par des fonds publics néerlandais, de rendre ces travaux librement accessibles après un délai dit "raisonnable" suivant leur première publication. Cette disposition, inscrite à l'article 25fa de la loi, implique que les chercheurs ne doivent plus négocier ou réserver ce droit auprès des éditeurs dès lors que le contrat relève du droit néerlandais » (Copyright Act 2015)

Cette disposition s'inscrit dans la dynamique de reconnaissance du savoir comme bien commun, en tension avec les logiques d'appropriation éditoriale, et renforce le rôle des universités comme vecteurs d'ouverture, d'intégrité scientifique et de souveraineté informationnelle.

### 5.3.3 La question du coût et la notion de confiance

Au niveau de la sécurité il convient de trouver un compromis optimal entre la rigueur des mesures de sécurité, la flexibilité requise par les utilisateurs, le niveau d'investissement consenti et le degré de protection attendu. La cybersécurité ne peut plus être appréhendée comme un frein opérationnel ou une contrainte budgétaire car elle constitue un facteur différenciant de compétitivité et de résilience (Ghernaouti 2022).

Une organisation dotée d'un dispositif de sécurité plus robuste que celui de ses homologues devient mécaniquement une cible moins attrayante pour les cyberattaquants, qui privilient les failles les plus accessibles (Hughes 2024). Le niveau de sécurité conditionne directement la confiance des utilisateurs, partenaires et autorités dans la pérennité et la fiabilité des services numériques offerts. Néanmoins, le calcul du retour sur investissement demeure difficile, en raison de l'absence de métriques normalisées permettant de mesurer objectivement les pertes évitées ou les bénéfices générés d'autant plus dans un secteur qui n'a pas vocation à générer du profit. L'ampleur des activités cybercriminelles, la diversité des profils impliqués et la portée transnationale de leurs actions rendent complexe toute tentative d'identification des acteurs de la cybercriminalité, ainsi que l'estimation précise des coûts qu'elle engendre pour la société (Ghernaouti 2022). La cybersécurité, loin d'être une dépense isolée, doit être envisagée comme un levier stratégique de résilience. Sa mise en œuvre soulève toutefois des enjeux budgétaires, dans un contexte de financements fragmentés, exigeant une évaluation de la criticité des missions numériques à protéger. L'allocation des ressources repose sur l'analyse des risques et des vulnérabilités propres à l'organisation, il s'agit d'évaluer les impacts potentiels d'une attaque réussie sur les fonctions critiques de l'institution. Négliger l'investissement dans la prévention, c'est choisir à terme le coût excessif et souvent irréversible de la reconstruction (ESRI 2024).

La contrainte financière affecte également la capacité des institutions à assurer une préservation numérique à grande échelle de leur patrimoine. Si des avancées significatives sur le plan technologique ont été faites en termes de stratégies de migration, de normalisation, ou encore de redondance, ces solutions, demeurent coûteuses, incomplètes, et soumises à des taux d'erreurs non négligeables à très long terme. À mesure que les limites techniques deviennent mieux maîtrisées, les freins non technologiques prennent une importance croissante. (Kastellec 2012). Chaque niveau, technologie, accessibilité, cadre juridique, sélection documentaire, est lui-même conditionné par le facteur financier, qui est la restriction la plus déterminante. Cette « préservation sous contrainte » appelle un équilibrage des efforts de recherche et d'investissement, vers des modèles durables de gouvernance et de financement, pour préserver un patrimoine numérique accessible et pérenne (Kastellec 2012).

Dans les domaines liés de la cybersécurité et de la préservation numérique, la notion de confiance occupe une place transversale. En cybersécurité, la confiance ne saurait être considérée comme acquise ; elle est au contraire mise en tension avec les principes mêmes de la sécurité, qui reposent souvent sur des mécanismes de contrôle, de vérification et de défiance. Comme le rappelle Ghernaouti (2022), « la sécurité suppose, en quelque sorte, une non-confiance ». La construction d'un environnement sécurisé implique une vigilance constante, où la confiance n'exclut pas le contrôle, et où les dispositifs doivent rester auditables, compréhensibles et soumis à une gouvernance claire. Dans ce cadre, la confiance est avant tout un effet perçu, qui dépend moins de l'intuition des utilisateurs que de la lisibilité et de la traçabilité des dispositifs de sécurité. Chaque atteinte à la disponibilité entame cette notion de confiance que l'on veut promouvoir via les usages numériques (Poupard 2018). Cette logique résonne dans le domaine de la préservation numérique. La durabilité de l'accès aux contenus repose sur un ensemble complexe d'interdépendances entre acteurs. La confiance y est également centrale et ne se limite pas à la robustesse technique des dépôts, mais englobe aussi la transparence des procédures, la qualité de la gouvernance, la résilience opérationnelle, et la capacité à documenter, auditer et prouver les engagements pris (Beagrie 2013). Des cadres normatifs tels que le Trusted Digital Repository Standard (ISO 2025b) ou le Data Seal of Approval (Harmsen 2024) offre des référentiels objectifs permettant d'évaluer la fiabilité des systèmes d'archivage électroniques (ISO 2025a). Ces démarches visent à réduire l'écart entre la confiance perçue et la confiance démontrable, et d'allier croyance, preuve et engagement mesurable. La confiance n'est pas un postulat, mais une construction active entre les parties, conditionnée par leur capacité à dialoguer, à documenter les responsabilités et à rendre les infrastructures compréhensibles et vérifiables.

### **5.3.4 Gestion data-centrée des collections électroniques**

L'accès pérenne aux périodiques scientifiques électroniques soulève des enjeux spécifiques qui vont au-delà des problématiques de conservation des imprimés ou des données numériques classiques. Il nécessite une approche intégrant des dimensions juridiques, techniques et organisationnelles (Alexandre 2015). L'archivage pérenne fondé sur le modèle OAIS constitue une réponse adaptable à toute collection ou institution, indépendamment de leur nature ou de leur échelle (Ferracci 2016).

Si la gestion documentaire a longtemps constitué le socle des pratiques organisationnelles en matière de gestion de l'information, elle montre aujourd'hui des limites face aux transformations induites par le numérique (Banat-Berger, Duplouy, Huc 2009). L'essor des publications électroniques, la fragmentation des supports, l'évolution des formats exigent de

repenser nos cadres d'analyse et de gestion. Dans ce contexte, il devient nécessaire de dépasser la logique classique du document pour adopter une approche centrée sur les données, sur leur usage, leur circulation, leur valeur stratégique. Dans le cœur de la réflexion, les ressources électroniques doivent être envisagées à la fois comme des actifs informationnels pour permettre leurs sécurisations au sein du SI, et doivent être envisagées comme des données pour en garantir leur préservation sur le long terme.

Cette double approche implique de dépasser la logique héritée du support physique, encore largement maintenue par les éditeurs pour des raisons commerciales. Repenser les publications comme des ensembles de données ouvre la voie à une gestion fondée sur le cycle de vie des données, mieux adaptée aux réalités contemporaines. Une telle perspective favoriserait l'intégration des principes d'archivage dès la production ou l'acquisition, tout en renforçant la pérennité, l'interopérabilité et la valorisation des contenus. Elle s'inscrit dans la continuité des politiques de gestion du cycle de vie des données actuellement en développement à l'UNIGE, tant pour les données administratives que pour les données de recherche dans le cadre du projet de *Data-Stewardship*. La sécurité comprise comme la capacité à assurer l'accès pérenne et la résilience du SI peut être renforcée par une telle approche. Comme le rappellent Banat-Berger, Duplouy et Huc (2009, p. 21), « la donnée est une représentation formalisée de l'information » : qu'il s'agisse d'un texte, d'une image ou d'un graphique, elle constitue un support d'information à part entière. Dès lors, considérer les collections électroniques comme des fonds de données, indépendamment de leur support ou de leur format, permet d'élargir le cadre de réflexion et de mettre en place des stratégies de préservation mieux alignées avec les exigences.

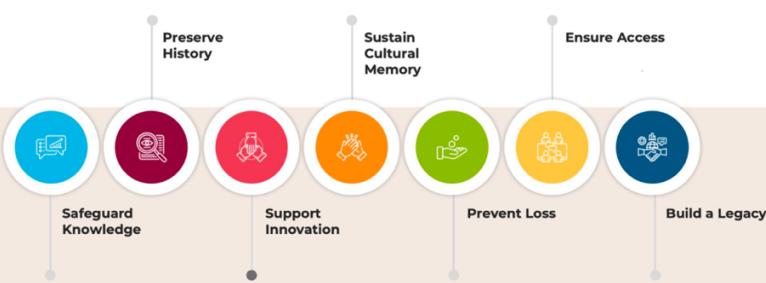
« La représentation de l'information ne sera sûrement plus binaire. Il ne sera alors plus nécessaire de conserver cette information dans des objets numériques sous leurs formes d'origine » (Banat-Berger, Duplouy, Huc 2009). L'utilisation des dépôts de données de recherche conformes au modèle OAIS pour leur sauvegarde et leur archivage devient alors possible, et permet d'assurer une gestion des objets numériques tout au long de leur cycle de vie. L'institution cible possède les capacités techniques pour la gestion de ce type d'objet. Elle facilite la définition de responsabilités, l'implémentation de métadonnées descriptives, administratives et techniques indispensables à la pérennité, tout en garantissant la traçabilité, l'authenticité et l'accessibilité des données sur le long terme, des conditions pour répondre aux exigences juridiques, scientifiques, opérationnelles mais également sécuritaire. Elle imposerait aussi dans les négociations avec les éditeurs de nouvelles conditions qui seraient au bénéfice des institutions.

La protection des données recouvre des acceptations multiples que l'on parle de sécurité, de confidentialité, d'intégrité ou de conservation. Dans une perspective orientée stockage, elle vise principalement à garantir l'intégrité, la disponibilité et la capacité de restauration des données, à travers des dispositifs techniques (sauvegardes, rétention, immutabilité, destruction sécurisée). Elle se cumule avec celle de la sécurité de l'information, fondée sur la préservation de la confidentialité, de l'intégrité et de la disponibilité, et avec la notion d'« assurance informationnelle », qui y ajoute des dimensions de résilience, de détection et de reprise, en mobilisant les principes de la dépendabilité. Tandis que la sécurité cible les menaces intentionnelles, la dépendabilité s'intéresse aux défaillances accidentelles. Une politique cohérente de protection des données doit donc intégrer ces logiques pour assurer conformité, continuité et résilience à long terme (SNIA 2025).

### 5.3.5 Une mutualisation des efforts pour des objectifs communs

Dans une perspective de rationalisation, une mutualisation des infrastructures et des efforts, en interne comme avec des partenaires externes, serait à envisager. Cela pourrait s'accompagner d'un recentrage budgétaire, via une facturation des services offerts par la DISTIC, afin de favoriser une centralisation accrue des systèmes d'information et par extension un renforcement de leur sécurité. L'environnement numérique caractérisé par la volatilité des contenus, la multiplication des menaces et l'exigence croissante de disponibilité permanente, renforce l'idée que la préservation des ressources ne puisse plus être envisagée de manière isolée. Dans cette logique de fédération, la participation de la BNS en tant qu'actionnaire de SLSP témoigne d'un engagement en faveur de cette coopération entre institutions patrimoniales et scientifiques autour d'une infrastructure partagée (SLSP 2025).

Figure 15 - Pourquoi préserver les ressources électroniques



(Clockss, 2025)

Bibliothèques académiques, institutions patrimoniales, éditeurs, auteurs et tiers archiveurs partagent une responsabilité collective pour garantir la préservation (Figure 15), la sécurité et l'accès du savoir. Cette démarche exige des politiques cohérentes de sauvegarde et d'archivage par les bibliothèques, un cadre juridique et patrimonial assuré par les institutions nationales, des standards qualitatifs et interopérables adoptés par les éditeurs et les auteurs, ainsi que des solutions techniques certifiées proposées par les tiers archiveurs. Ce partenariat forme une responsabilité mais aussi une infrastructure mutualisée, distribuée et résiliente. Cette ambition implique de renforcer les liens entre sauvegarde, archivage et cybersécurité, les trois aspects complémentaires d'une politique globale de continuité d'activité. Dans cette perspective, les bibliothèques sont appelées à jouer un rôle de coordinateurs dans la mise en œuvre de ces solutions. L'intégration de services distribués, permet de préserver les contenus en *dark-archives*, et de garantir leur réactivation contrôlée en cas d'interruption d'accès. Ces systèmes renforcent la cyber résilience documentaire, en assurant qu'aucune attaque, panne ou défaillance isolée ne puisse compromettre durablement l'accès à l'information scientifique. Si les capacités locales des bibliothèques restent inégales, le besoin de garantir la disponibilité des publications numériques stimule ce développement de solutions collaboratives. Toutefois, la réussite de ces dispositifs repose également sur l'expertise du personnel, notamment des bibliothécaires spécialistes des ressources électroniques, qui jouent un rôle important dans la négociation des licences, la veille technologique, et la mise en œuvre de stratégies de préservation alignées sur les capacités et les priorités locales (Polchow 2021). Cette vision élargie de la continuité documentaire réaffirme la place des bibliothèques : à la fois dépositaires du savoir dans l'environnement numérique, mais aussi catalyseurs des dynamiques de mutualisation pour sa disponibilité et sa fiabilité dans le temps.

## 6. Plan de sauvegarde des collections électroniques

Cette section présente un plan de sauvegarde des collections électroniques fondé sur une architecture résiliente, combinant outils internes, redondance et accès dégradé. Il vise à garantir la continuité des services documentaires en cas de crise, via un jeu de données interopérable assurant l'exploitation, la portabilité et la réversibilité du système. Ce dispositif s'inscrit dans le Plan de Continuité d'Activité, en précisant les responsabilités et les objectifs de reprise. Il est adapté au Plan de Reprise d'Activité intégrant restauration, redondance et priorisation des services critiques. Conformément au cadre NIST CSF, il prévoit une gestion de crise encadrant les scénarios pour renforcer la résilience du système.

### 6.1 Extraction des données

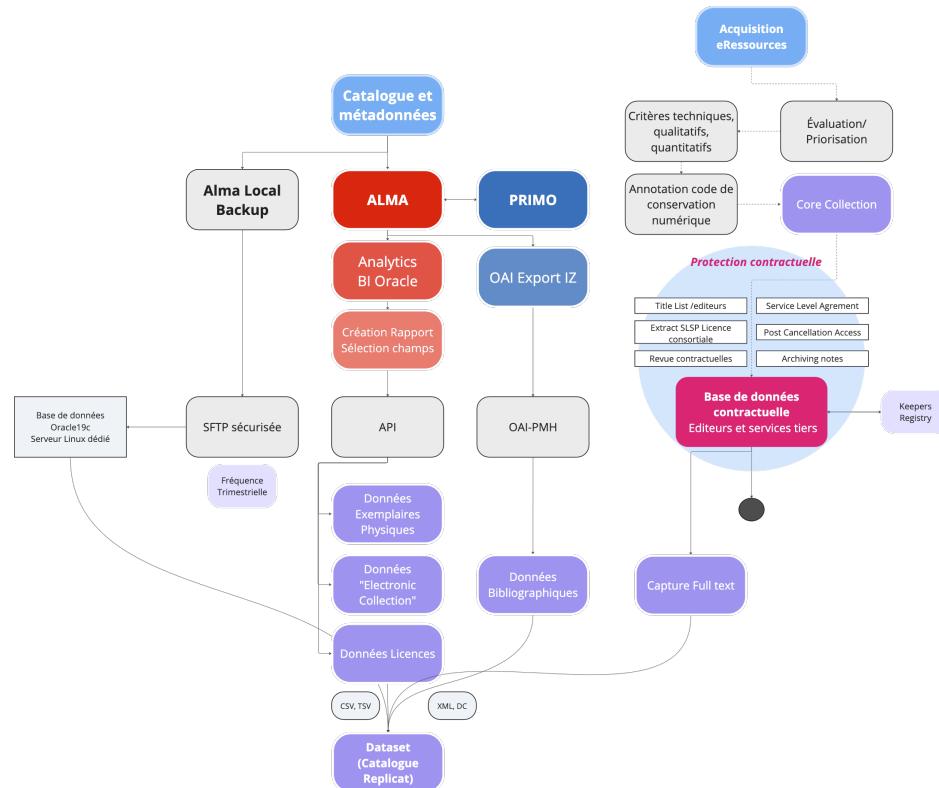
Il s'agit de modéliser le cycle d'extraction, de protection et de mise à disposition des métadonnées bibliographiques issues du SIGB Alma. Il articule les trois niveaux adaptables pour leur bonne gestion comme forme de sécurisation graduée. La solution doit garantir que les métadonnées du catalogue, considérés comme un actif critique, soient sécurisées contre la perte accidentelle (sauvegarde), mais également préservées dans un état stable et exploitable permettant la récupération (conservation), puis archivées dans une perspective d'accès à long terme (archivage pérenne). Cette étape préparatoire permet ensuite de pouvoir envisagée des solutions d'accès pérenne.

Dans le cadre de la constitution d'un réplica du catalogue destiné à l'évaluation, au suivi ou à la préservation, deux canaux techniques principaux peuvent être mobilisés au sein de l'environnement documentaire existant :

- Les données bibliographiques sont moissonnées via le protocole OAI-PMH depuis la zone institutionnelle (IZ) d'ALMA, permettant de récupérer des métadonnées normalisées du catalogue de la Bibliothèque en format XML (Dublin Core ou MARCXML).
- Les données de gestion, celles liées aux licences électroniques, aux modalités d'acquisition, ou restrictions contractuelles, sont récupérées via ALMA Analytics (BI Oracle). Des rapports personnalisés sont créés à partir de requêtes ciblant les champs pertinents à des fins de suivi des droits d'accès ou de gouvernance contractuelle. Ils peuvent être importés de manière séquentielle via l'API Analytics pour l'automatisation de la procédure (données tabulaires en XML).

L'agrégation de ces deux sources doit ensuite être normalisé pour la constitution d'un jeu de données consolidé. Le réplica du catalogue constitue la base technique nécessaire à la mise en œuvre de la stratégie de préservation mais également une reprise de contrôle en local sur nos données documentaires. Ce croisement permet d'obtenir une vision consolidée des ressources électroniques, de leurs conditions d'accès, de leur valeur stratégique et de leur statut de conservation.

Figure 16 - Cycle d'extraction du catalogue



CC BY NC Stephen Valot 2025

Les extractions, figure 16, peuvent être configurées de manière incrémentales, différentielles ou totales, avec la fréquence d'actualisation déterminée par le RPO défini dans le BIA. Les métadonnées bibliographiques issues de Alma sont exportées au format DublinCore ou MARC XML, pour garantir leur interopérabilité avec des systèmes d'archivage, de moissonnage ou de diffusion. Ces métadonnées comprennent notamment :

- Titre, créateur, contributeurs
- Date de publication, éditeur
- Sujet, langue, description
- Identifiants normalisés (ISBN, ISSN, DOI ...)
- Droits d'accès, type de ressource, format
- Relations documentaires et source d'origine

Les exports via Analytics permettent d'enrichir le réplica avec des informations nécessaires pour la gouvernance et la préservation :

- Informations contractuelles : type de licence (abonnement, achat), statut (actif/expiré), périmètre d'accès, clauses spécifiques (PCA, TDM, archivage, accès distant), liens contractuels.
- Collections électroniques : nom de collection, fournisseur, plateforme, type de contenu (base, bouquet, titres isolés), couverture disciplinaire, disponibilité, URL, MMS ID.
- Exemplaires physiques : statut, localisation, type de support, cote, nombre, code-barres, politique de conservation (réserve, exemplaire unique...).

Ce modèle de métadonnées (Annexe 18) permet d'identifier et de documenter les ressources critiques, prioriser les mesures de sauvegarde ou d'archivage, réaliser le suivi contractuel et technique et également d'évaluer la conformité aux bonnes pratiques de conservation numérique. Il ouvre la voie à une intégration progressive de la préservation dans le cycle de vie documentaire. Une limite importante doit être soulignée. La localisation exacte d'un article n'est pas toujours extractible, car elle est générée dynamiquement par le résolveur de liens en fonction de plusieurs paramètres techniques qui figurent dans la base de connaissance propriétaire d'Ex Libris (identifiants, plateforme, schéma dans l'URL). Par conséquent, l'URL enregistrée dans les métadonnées n'est, dans de nombreux cas, qu'un lien générique vers la plateforme de l'éditeur, et non un accès direct au document. Il est également essentiel de conserver les identifiants MMS propres à Alma, afin de pouvoir réintégrer les données saisies en mode local durant une situation de crise, dans le système d'origine.

D'un point de vue de la préservation numérique, la question de la pérennité des liens d'accès pour les objets ne disposant pas d'identifiants pérennes comme les DOI ou les ARK est toujours ouverte et justifie la nécessité de pouvoir capturer le texte intégral des ressources acquises. La stratégie est alors de pouvoir anticiper la signalisation d'une *core collection* pour pouvoir capter dès le processus d'acquisition la représentation de l'article dans la base de données qui sera utilisée pour la pérennité de l'accès.

En fusionnant les données d'Alma, il est possible de relier chaque titre à son statut de licence et d'accès, d'identifier les ressources ayant un double support, de cartographier les ressources « en danger » selon les disciplines ou les éditeurs et d'évaluer la couverture des licences par rapport aux usages ou à l'exposition aux risques. On peut ainsi envisager des enrichissements externes du catalogue local, en s'appuyant sur des sources comme le DOAJ, Lens ou Dimensions, afin de croiser, qualifier et compléter les métadonnées existantes. L'amélioration de la recherche et de l'accès aux ressources, mais également la dimension analytique du pilotage documentaire serait renforcée. En intégrant des indicateurs bibliométriques, des statistiques de citation, ou encore des informations contextuelles telles que l'affiliation institutionnelle des auteurs ou les collaborations scientifiques, la bibliothèque se doterait d'une capacité supplémentaire pour évaluer l'impact réel de ses collections.

À plus long terme, ces enrichissements pourraient soutenir des stratégies avancées de veille, d'analyse prédictive des besoins académiques. L'exploitation dynamique de ces jeux de données externes ou l'entraînement d'un modèle d'IA locale représenterait une opportunité pour renforcer et optimiser la gestion des ressources.

## 6.2 Une protection contractuelle des ressources électroniques

Les résultats obtenus convergent sur l'importance de l'établissement d'un registre contractuel. L'analyse de l'échantillon des contrats de licences consortiales menée à partir de l'extraction des métadonnées des contrats fournies par SLSP révèle des lacunes significatives en matière de garanties d'archivage inscrite sur les contrats. Sur les 137 licences analysées, seules 3 comportaient une mention explicite "Archiving Right", dont 2 positives et 1 négative. En revanche, 122 licences comportaient une "Archiving note", parmi lesquelles 81 précisaien l'absence de clause contractuelle sur ce sujet. Ces chiffres mettent en évidence une protection contractuelle, à première vue lacunaire, particulièrement problématique dans le contexte de la pérennisation des accès numériques post-abonnement. Néanmoins, l'absence d'informations dans les métadonnées de gestion ne veut pas dire qu'elles sont absentes dans les véritables

contrats mais que le suivi est perfectible et, au vue de la dépendance du SI à Alma nécessiterai la tenue de ce registre hors de l'application.

Les éléments contractuels tels que le « Post-Cancellation Access », les clauses d'archivage explicites, les droits de text and data mining, ou encore les conditions de réversibilité, sont trop souvent absents ou insuffisamment négociés (Eve 2024). La collecte systématique des bases de données contractuelles et la vérification croisée avec le Keepers Registry (Beagrie 2013) permettent toutefois d'identifier que certains éditeurs garantissant une conservation via des tiers-archiveurs. La base externe de suivi dédiée doit être structurée autour de champs normalisés permettant de centraliser l'information contractuelle stratégique. Chaque ligne correspondant à un éditeur pourrait contenir les attributs suivants :

- Éditeur,
- URL de la ressource,
- Première année d'abonnement,
- Contenu acquis (volumes, années, types de documents),
- Type d'acquisition (licence nationale, consortiale, achat ponctuel),
- Présence d'un accès post-abonnement (PCA),
- Mention de "perpetual access" dans la licence,
- Présence de frais de plateforme (platform fees),
- Mention de l'archivage via tiers-archiveur,
- Coûts éventuels liés à cette archive,
- Solution alternative si non couvert,
- Modalités d'accès effectives (IP, authentification fédérée, etc.).

Cette structuration peut sécuriser les investissements documentaires, anticiper les risques de coupure d'accès, et orienter les négociations futures vers des modèles plus résilients et conforme à la préservation numérique.

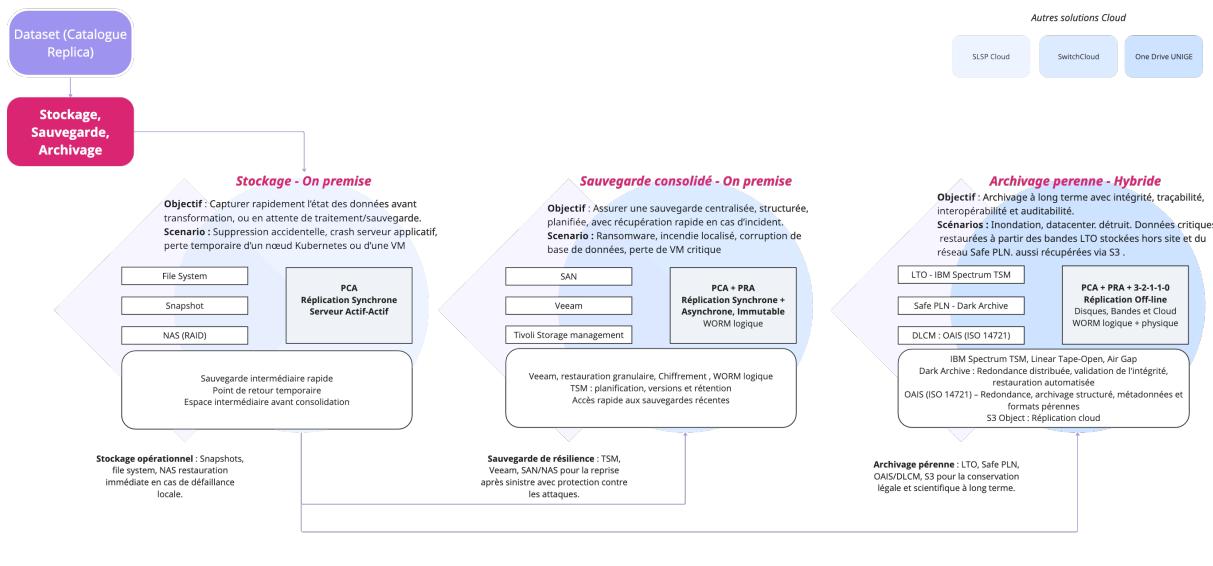
La dimension de couverture contractuelle ne peut être dissociée du processus d'acquisition. L'introduction de critères techniques, qualitatifs et quantitatifs dès la phase de sélection des contenus par les responsables de collection permettrait de renforcer la traçabilité des décisions, et d'anticiper la stratégie de préservation. L'évaluation systématique de chaque ressource conduit à une priorisation documentaire dès son acquisition ou renouvellement (partie 4.6.3). À cette fin, l'intégration d'une annotation de conservation numérique *Core Collection* dans le processus d'acquisition co-défini par les responsables de collection et les référents techniques représente un levier de transformation. Cette nouvelle métadonnée, attribuée à des ressources jugées essentielles, activerait une série de mécanismes dont la vérification des clauses contractuelles, enrichissement de la base de connaissance, compatibilité technique avec l'extraction du texte intégral, et, si toutes les conditions sont réunies, déclenchement de la capture des contenus pour conservation pérenne. Ce processus suppose toutefois un travail fastidieux, notamment pour les bouquets de périodiques ou les plateformes de publications.

## 6.3 Stratégie de sauvegarde et de préservation des actifs

Une façon de rendre le stockage et la gestion numérique plus efficaces est d'utiliser des systèmes de préservation en plusieurs niveaux, pour protéger l'extraction de l'intégralité du catalogue de la zone institutionnel. Ainsi de sélectionner des options de stockage offrant différents niveaux de réPLICATION, de diversité des supports et de coût.

Inspiré des archives de l'Université de Yale l'utilisation d'un système à trois niveaux permet une sécurisation et également une adaptabilité de la méthode. Le niveau actif stocke les données sur les serveurs avec un temps de récupération rapide ou moyen, le niveau archive stocke également les données sur les serveurs mais avec un temps de récupération lent, et le niveau cloud utilise une combinaison de technologies de stockage réparties dans plusieurs lieux, avec un temps de récupération lent (Hedley 2025). Ces trois niveaux sont redéfinis selon la dénomination Stockage, Sauvegarde, Archivage dans la Figure 17.

Figure 17 - Modélisation de la stratégie de sauvegarde – Sauvegarde pérenne



CC BY NC Stephen Valot 2025

Ce système n'est pas sans rappeler la théorie des trois âges du document même si « la distinction entre le court et moyen terme d'une part (archives courantes et intermédiaires) et le long terme (archives patrimoniales) s'amenuise avec le numérique »(Banat-Berger, Duplouy, Huc 2009). Penser l'archivage comme une solution opérationnelle n'est pas forcément le plus évident il faut en dévoiler sa fonction et sa mission première.

Aujourd'hui, Ex Libris définit des niveaux de sinistre selon la gravité. Panne mineure jusqu'à 48h, majeure 48h à 7 jours, et catastrophique plus de 7 jours. En cas d'incident critique, le Recovery Time Objective varie de quelques heures à plusieurs jours selon le scénario, tandis que le Recovery Point Objective est fixé à 24 heures, impliquant que les restaurations peuvent s'appuyer sur des sauvegardes remontant à un jour maximum. Actuellement, la stratégie adoptée délègue la responsabilité principale de la sauvegarde et de la reprise à Ex Libris bien qu'une base de données externe contenant une copie des métadonnées bibliographiques a été développée à leur niveau pour permettre une restauration ciblée en cas de perte de données. Son extension aux données de la zone institutionnelle (IZ) est prévue, sans échéance définie (Échanges SLSP, 2025).

### **6.3.1 Niveau 1 – Stockage opérationnel**

Ce niveau assure une restauration rapide en cas d'incident mineur, actuellement assuré à l'UNIGE grâce à des snapshots synchrones et le NAS local. Il permet de récupérer en quelques minutes à deux heures des extractions récentes ou des fichiers supprimés. Accessible aux équipes, cette sauvegarde opérationnelle vise la continuité immédiate des activités en cas de défaillance locale. Elle repose sur un stockage local et des captures régulières de l'état des données avant toute transformation ou transfert vers des dispositifs de sauvegarde distants. Plusieurs mécanismes techniques sont mis en œuvre :

- Snapshots réguliers du File System : Ces instantanés fréquents permettent de capturer l'état exact des données à intervalles courts (heures), limitant la quantité d'informations perdues en cas d'incident.
- Stockage NAS : Un Network-Attached Storage (NAS) est déployé localement pour stocker ces snapshots. Cet élément permet la gestion sécurisée des sauvegardes à court terme, et facilite un accès rapide et direct aux données pour leur restauration.
- RéPLICATION synchrone (serveurs actif-actif) : Les données sont systématiquement répliquées en temps réel sur deux serveurs configurés en mode actif-actif. Cette configuration permet une disponibilité continue et transparente des données, même en cas de panne matérielle ou logicielle d'un des serveurs, sans interruption du service.

Grâce à ce dispositif de stockage opérationnel la Bibliothèque possède une couverture immédiate contre les incidents mineurs, pour garantir la continuité des activités documentaires courantes et réduire les délais et coûts associés à la restauration des données. Les scénarios couverts par cette couche comprennent typiquement les suppressions accidentelles de fichiers, les crashes d'applications serveur, les pertes temporaires d'instances virtuelles (VM), ou encore les interruptions ponctuelles de nœuds de virtualisation. Le stockage est configuré en réPLICATION synchrone et garantit une continuité des services et une disponibilité optimale, une restauration rapide et fiable réduit l'impact opérationnel d'incidents sur la disponibilité.

### **6.3.2 Niveau 2 - Sauvegarde consolidée**

Le deuxième niveau assure la continuité d'activité après un incident majeur, tel qu'une cyberattaque, une compromission du système ou la perte d'une machine virtuelle. Il repose sur des sauvegardes asynchrones, immuables, et répliquées sur un site secondaire sécurisé. Ces copies, isolées du système principal, permettent une restauration en 4 à 24 heures. Ce niveau protège les actifs critiques, notamment les bases de données issues des extractions, contre les *ransomwares*, *wipers* ou erreurs humaines, en assurant une reprise structurée et fiable, tout en préparant un éventuel déport vers l'archivage long terme. Les technologies comprennent :

- Stockage SAN/NAS centralisé : Le Storage Area Network (SAN) et le Network-Attached Storage (NAS) sont utilisés pour la centralisation des sauvegardes.
- Protection contre les *ransomwares* par immutabilité (WORM logique) : La mise en œuvre du principe Write Once Read Many (WORM) logique permet une immutabilité des sauvegardes, empêchant l'altération, la suppression malveillante des données sauvegardées, pour une protection contre les *ransomwares* et les tentatives de compromission.
- RéPLICATION synchrone et asynchrone : La combinaison de réPLICATION synchrone et asynchrone permet de sécuriser les sauvegardes en temps réel sur les sites distants.

La réPLICATION synchrone garantit une redondance immédiate, tandis que la réPLICATION asynchrone protège contre des incidents à plus grande échelle.

- Utilisation conjointe des solutions Veeam et Tivoli Storage Management (TSM) :
  - Veeam : Permet une restauration granulaire et rapide (fichier par fichier, VM par VM), tout en assurant la protection par chiffrement des sauvegardes et une gestion efficace de l'immuabilité des données.
  - TSM (Tivoli Storage Management) : Offre des capacités de planification, gestion des versions, et définition de politiques de rétention des sauvegardes, soit une conservation fiable des données sur le moyen et long terme.

Cette couche de sauvegarde est directement intégrée à la stratégie de continuité et de reprise des activités capable de répondre de façon coordonnée et rapide en cas d'incident majeur. Les procédures de reprise exploitent directement les sauvegardes consolidées pour restaurer les environnements critiques dans les délais définis. En combinant ces stratégies, ce niveau assure la protection complète des actifs numériques, et garantit leur récupération après un incident, et met en place une défense contre les menaces internes ou externes susceptibles de compromettre l'intégrité des données critiques de la Bibliothèque.

### 6.3.3 Niveau 3 - Archivage pérenne

Conçu pour la conservation à long terme, il s'appuie sur les dépôts conformes aux modèles standards comme OAIS (ici DLCM) et certifié TDR ISO 16363(ISO 2025b). Ce niveau s'appuie sur des supports hors-ligne sur bandes de type Linear Tape Open (LTO), les services d'archivage cloud, et les réseaux de préservation distribués reposant sur le logiciel open source LOCKSS. Avec un temps de récupération lent 1 à 5 jours il permet pour les archives, et les données à valeur scientifique une forte résilience, la conformité légale, et la durabilité sur plusieurs décennies. Il garantit ainsi la reconstitution après sinistre total grâce à l'archivage sur bandes. Il met l'accent sur l'intégrité des données, leur traçabilité, l'interopérabilité des formats et la capacité d'audit. Cette stratégie s'appuie sur des technologies internes pour répondre aux menaces cyber de grande ampleur, en garantissant une sauvegarde indépendante, durable et vérifiable. Ce niveau se décline selon ces méthodes :

- Archivage sur bandes : Les sauvegardes bénéficient d'une réPLICATION offline sur bandes LTO, qui constitue la protection contre les attaques par *ransomware* et garantit une protection physique complète contre les crises majeures. L'utilisation combinée de WORM logique et physique prévient toute modification ou suppression non autorisée des archives.
- Réseau Safe PLN (*Dark Archive*) : Le recours au réseau distribué de type « Dark Archive » Safe PLN permet une réPLICATION basée sur la redondance géographique intrinsèque du système et garantit l'intégrité permanente des données par des validations périodiques automatisées. Cette approche décentralisée diminue significativement le risque de perte totale d'information en cas de catastrophe locale.
- Archivage structuré selon le modèle OAIS (ISO 14721) DLCM : Le modèle OAIS offre un cadre robuste reconnu pour structurer, stocker et préserver les ressources numériques à très long terme. Le développement de la technologie DLCM au sein de l'institution permet d'envisager son recours pour l'archivage pérenne du data-set. Il intègre de plus la gestion complète du cycle de vie des données archivées, des mécanismes de contrôle d'accès, ainsi qu'une interopérabilité grâce à des métadonnées normalisées et des formats ouverts et pérennes.
- Stockage cloud sur S3 (Object Storage) : La réPLICATION des données via un service de stockage objet cloud renforce encore davantage la résilience, offrant une capacité de

récupération à partir d'une source distante, même dans des scénarios de catastrophe où les ressources locales et les bandes seraient inaccessibles. Ce dispositif est déjà utilisé pour la redondance dans la technologie DLCM.

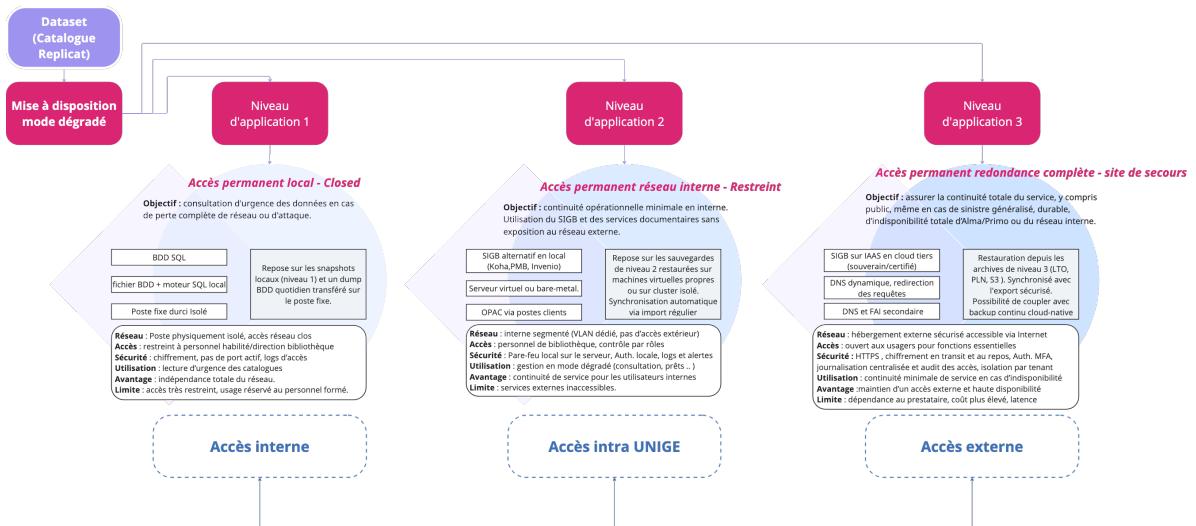
Par rapport aux couches précédentes, ce niveau offre un avantage en termes de pérennité et de sécurité contre les cyber-risques les plus critiques déjà évoqués. Son approche d'archivage offline, la redondance distribuée, hybride et une gestion des métadonnées, rend quasiment impossible la destruction ou l'altération définitive des données critiques. De plus, la répartition géographique et la variété des supports (bandes, disques, cloud) assurent une résilience face aux catastrophes de toute nature.

Pour garantir l'efficacité et la robustesse de cette architecture en trois couches, plusieurs bonnes pratiques doivent être intégrées. L'usage de formats standardisés et interopérables pour l'archivage (PDF/A, METS, BagIt), l'automatisation des flux entre les niveaux, la validation régulière de l'intégrité des données (via checksums et audits), une documentation claire des responsabilités à chaque étage, ainsi que des tests de restauration périodiques pour vérifier les délais et la fiabilité du dispositif.

## 6.4 Stratégie d'accès dégradé aux données préservées

Afin d'assurer une protection en adéquation avec les risques identifiés, il est indispensable de mettre en œuvre au minimum un niveau de sauvegarde équivalent au niveau *Sauvegarde Consolidée*. Une fois les données sécurisées, l'enjeu se déplace vers leur restauration effective. Il s'agit alors de garantir la capacité à récupérer les données sauvegardées et à les rendre accessibles via une solution de repli ou une infrastructure alternative (Boulet 2008). La modélisation présentée (Figure 18) se veut graduelle.

Figure 18 - Mise à disposition des données sauvegardées – Accès perpétuel



CC BY NC Stephen Valot 2025

### 6.4.1 Niveau A - Accès permanent, local

Ce premier niveau d'accès dégradé répond au scénario de perte complète du réseau ou d'attaque rendant indisponibles les systèmes habituels. Il s'appuie sur une infrastructure locale autonome, permettant la consultation d'urgence des données critiques préalablement

sauvegardées. Techniquement, cet accès repose sur des snapshots locaux fréquents (déscrits au niveau 1), ainsi qu'un dump quotidien de la base de données SQL transféré et chargé sur un poste fixe isolé dédié. Ce poste, spécialement configuré et sécurisé, embarque un moteur SQL local capable d'assurer une exploitation minimale des données. Le poste peut être alimenté quotidiennement par une extraction automatisée et sécurisée depuis le système de production et réalisée via un transfert manuel sécurisé (clé USB chiffrée ou média sécurisé équivalent), effectué par un personnel habilité. Après chargement des données, le média est systématiquement retiré du poste et sécurisé, et limitant le risque d'infection ou de compromission externe. Les caractéristiques sont les suivantes :

- Isolation physique et réseau : Le poste dédié est physiquement et électroniquement isolé, sans connexion active au réseau institutionnel ou externe, éliminant ainsi tout risque de contamination ou de compromission depuis l'extérieur.
- Sécurité renforcée : L'accès à ce poste est restreint exclusivement à un personnel formé et habilité, notamment à la direction et la coordination de la Bibliothèque. Le poste bénéficie d'un chiffrement complet, d'une désactivation physique des ports USB et réseau inutilisés (activé pour l'opération d'alimentation), et d'un système de journalisation des accès.
- Usage strictement encadré : Ce dispositif ne permet qu'une consultation limitée des données sauvegardées, essentiellement le catalogue pour garantir la continuité minimale des services bibliographiques essentiels en cas de crise majeure.

L'avantage réside dans l'indépendance totale vis-à-vis du réseau, pour la disponibilité immédiate et sécurisée des données critiques en toutes circonstances. Sa principale limite est l'accès restreint et la lecture seule, réservé exclusivement au personnel autorisé et entraîné pour de telles situations, rendant cette solution adaptée à des situations exceptionnelles.

#### **6.4.2 Niveau B - Accès permanent, réseau interne**

Ce second niveau prévoit la continuité opérationnelle minimale en cas de coupure du réseau externe ou d'attaques majeures isolant l'institution de ses ressources habituelles. Il vise à fournir aux équipes une plateforme de gestion documentaire alternative fonctionnelle. Cette solution repose sur la restauration régulière des données issues des Sauvegardes *Consolidées* (niveau 2 précédent) sur un serveur virtuel ou une machine physique dédiée. Un système de gestion documentaire alternatif (SIGB open-source Koha, PMB ou Invenio) est installé localement sur cette infrastructure et régulièrement alimenté via des importations automatisées des données sauvegardées. La restauration des sauvegardes vers cette infrastructure est effectuée périodiquement sur des machines virtuelles propres ou sur un cluster dédié pour une synchronisation régulière. Ce processus automatisé minimise les pertes de données et facilite la reprise rapide d'activités internes (circulation, gestion des exemplaires). Les caractéristiques techniques prévoient :

- Isolation réseau : Le réseau interne utilisé est strictement segmenté via un VLAN dédié sans aucune exposition externe. Un pare-feu local permet un filtrage renforcé du trafic et une sécurité étendue.
- Contrôle d'accès : L'accès au SIGB alternatif est strictement réservé aux membres autorisés du personnel de la Bibliothèque. L'authentification locale, la gestion par rôles et une traçabilité détaillée des accès via logs et alertes de sécurité renforcent la protection contre les accès non autorisés.

- Usage opérationnel : L'interface utilisateur est déployée sur des postes clients internes, permettant aux bibliothécaires et aux usagers de poursuivre leurs activités en mode dégradé sans interruption des services internes de recherche.

L'objectif est de permettre la continuité des services internes même en cas d'attaque ou de panne majeure. Les processus opérationnels critiques au sein de la Bibliothèque sont sécurisés. Toutefois, sa principale limite réside dans l'absence de connectivité externe, empêchant l'accès aux ressources externes ou les mises à jour dynamiques pendant la durée de l'interruption.

#### **6.4.3 Niveau C - Accès permanent, redondance sur site de secours**

Ce troisième niveau constitue le dispositif de secours le plus avancé, permettant la continuité intégrale du service, y compris pour les usagers externes, en cas de sinistre généralisé (ex. : panne prolongée du réseau interne, perte du datacenter principal, cyberattaque paralysante sur les systèmes locaux). Il permet d'assurer un fonctionnement minimal mais stable et sécurisé, même en dehors des infrastructures institutionnelles. Le dispositif repose sur le déploiement d'un SIGB alternatif sur une infrastructure IaaS souveraine ou certifiée (par exemple via Switch Cloud, BibLibre ou d'autres prestataires compatibles avec les exigences). Cette instance est alimentée à partir des archives de niveau 3, via des exports sécurisés et réguliers. Le système peut être couplé à une stratégie de sauvegarde cloud-native continue, pour un delta minimal entre les données sources et les données répliquées. Il s'appuie sur :

- Hébergement cloud sécurisé : le SIGB fonctionne dans un environnement cloud mutualisé ou dédié, isolé par tenant, avec chiffrement des données au repos et en transit, authentification forte (MFA), et journalisation centralisée des accès pour répondre aux exigences de traçabilité et d'audibilité.
- Redirection dynamique : en cas de panne du site principal, des règles DNS dynamiques permettent de rediriger automatiquement les requêtes vers l'instance de secours, via un DNS secondaire et un prestataire indépendant du réseau principal (FAI tiers).
- Accessibilité : l'interface est disponible via HTTPS uniquement, fournit un accès public contrôlé aux fonctionnalités essentielles (catalogue, authentification, consultation des notices).

Ce dispositif assure un accès permanent aux services pour les usagers, même en cas d'indisponibilité d'Alma, de Primo, ou du réseau institutionnel. Il permet la reprise rapide des opérations, sans dépendre d'un retour immédiat à la normale sur site. La disponibilité du service en cloud, associée à une architecture en redondance géographique et technique, réduit fortement l'exposition aux risques critiques évoqués. Mais cette solution implique une nouvelle dépendance envers un prestataire externe, avec un coût d'exploitation potentiellement plus élevé que les niveaux précédents. Des tests de *failover* réguliers ou de bascule sont à prévoir pour assurer la fiabilité du système. Cette couche représente le niveau le plus haut de résilience dans la chaîne de préservation et d'accès. Elle se distingue des niveaux A et B par sa capacité à maintenir un service externe disponible, même dans des scénarios de crises majeures.

Sur le plan technique, l'UNIGE dispose de serveurs en haute disponibilité, d'un stockage immuable et de sauvegardes via Veeam et TSM, notamment sur bandes. Cependant, ces sauvegardes manquent de formalisation et d'automatisation, compromettant la capacité à restaurer le système ou à maintenir l'accès en cas de perte de connexion réseau ou au cloud.

Une stratégie hybride, combinant infrastructures internes et solutions tierces, apparaît nécessaire pour renforcer la résilience. L'élargissement du recours à des tiers archiveurs certifiés permettrait d'assurer la redondance, la pérennité et l'intégrité des collections numériques critiques. L'adaptation de DLCM pour ce type d'usage permettrait aussi à terme de l'utiliser comme infrastructure de stockage pour l'Archive Ouverte UNIGE et ainsi de l'aligner avec les impératifs de préservation numérique.

Ex Libris propose un service « *Alma Local Backup* », qui permet aux institutions abonnées de recevoir, jusqu'à une fois par trimestre, une copie des données essentielles de leur environnement de production. Ces données sont transférées via un canal sécurisé (SFTP) vers une base de données Oracle locale (version 19c Enterprise) de l'institution, à des fins de résilience et de continuité. Le fichier, fourni au format Oracle Dump, contient les données bibliographiques, les inventaires physiques, électroniques et numériques, les acquisitions, les métadonnées, ainsi que l'historique des prêts et demandes. Ce service est conçu comme une assurance complémentaire face aux limites d'un environnement SaaS multi-locataire, où les sauvegardes standard sont mutualisées. Alma réalise quotidiennement plusieurs snapshots et une sauvegarde complète, stockée sur site et en lieu distant sécurisé, pour une restauration complète possible en cas d'incident. Ex Libris applique une stratégie de continuité d'activité, qui incluent des dispositifs de redondance actifs/passifs, des audits réguliers, ainsi que des tests annuels du BCP, en conformité avec la norme ISO 22301. En cas de sinistre majeur, Ex Libris s'engage à restaurer l'environnement du client aussi rapidement que possible, avec un RTO de quelques heures à plusieurs jours et un RPO basé sur plusieurs points de sauvegardes journalières. Néanmoins le choix de cette solution porterait un peu plus loin les considérations de risques relatifs aux dépendances à un fournisseur unique.

## 6.5 La continuité d'activité

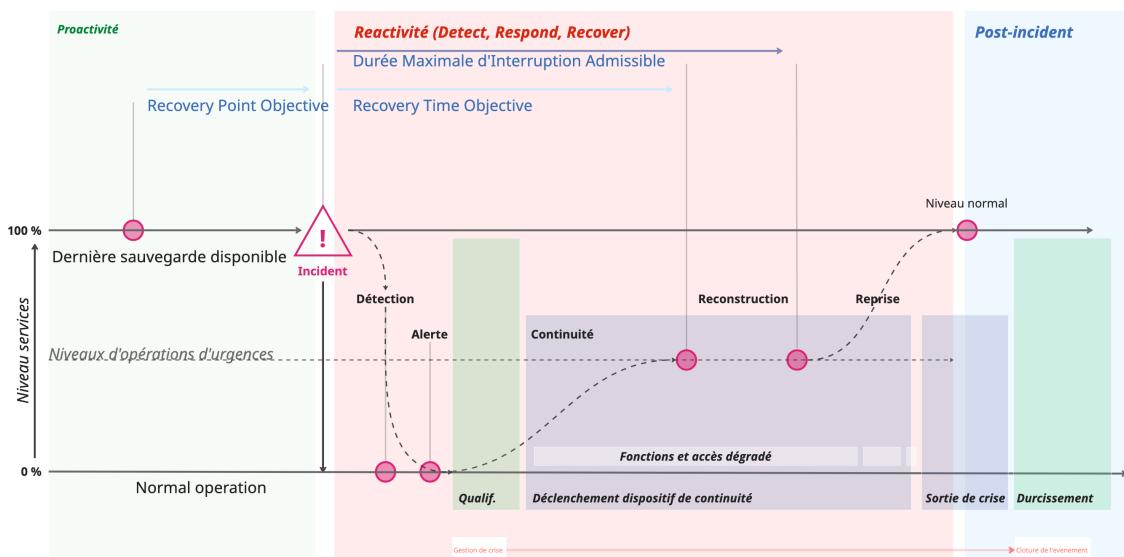
Le PCA vise à anticiper et à encadrer la réponse à une crise majeure en assurant la reprise des activités essentielles dans un délai acceptable. La stratégie de continuité découle de l'analyse des impacts métier, des risques et des processus critiques, associée à l'évaluation des ressources essentielles et à la définition des seuils acceptables de perte et de reprise des données.

La continuité implique la mise en place d'une cellule de crise capable de coordonner les actions, d'assurer la reprise des activités critiques dans les délais fixés et de planifier le fonctionnement en mode dégradé selon les scénarios de sinistre identifiés. Cette stratégie s'appuie sur les mesures de traitement des risques réparties en plusieurs catégories : préventives (réduction de la probabilité d'incident), protectrices (limitation des impacts), détectives (déttection précoce), correctives (restauration des services), transfert (assurances), ou acceptation si les autres options sont inadaptées (InterCERT 2024a; 2024b). Le PCA métier ainsi défini doit être formalisé dans un document structuré, régulièrement mis à jour et testé. Ce document précise le périmètre, les objectifs, les scénarios critiques, les procédures dégradées, les responsabilités, les ressources mobilisables, les circuits d'information, ainsi que les modalités d'alerte et de communication (Adenium 2022). Des tests réguliers (exercices de simulation, reprise après sinistre, validation des solutions) sont indispensables pour l'efficacité du dispositif. La documentation associée (procédures, supports, plans, annuaires) doit être conservée dans des formats accessibles et durables, y compris en cas de perte des systèmes principaux.

### 6.5.1 Alignement du plan de continuité et de reprise d'activité

Le plan de reprise après sinistre vise quant à lui à restaurer, dans les meilleurs délais, l'infrastructure et les applications critiques de l'organisation lorsqu'un sinistre rend l'un des deux centres de données inopérants. Ce dispositif est conçu en support du plan de continuité des activités métier, tel que défini dans la directive institutionnelle (UNIGE 2021b). Les équipes métiers doivent formaliser leur propre PCA, en décrivant les procédures de fonctionnement alternatifs, l'accès en mode dégradé (Figure 19) et les modalités de récupération des données une fois les services restaurés.

Figure 19 - Chronologie, dispositifs de continuité et jalons d'un incident critique



CC BY NC Stephen Valot 2025

Durant l'indisponibilité des services numériques essentiels, des procédures alternatives ou dégradées doivent être prévues par les métiers pour assurer la continuité minimale des activités. Le PRA doit anticiper les grandes catégories d'événements identifiés dans l'analyse des risques. Tout comme le PCA au niveau métier, il se compose de plusieurs volets. Une définition du périmètre, ses objectifs, les tests réguliers à effectuer, les procédures de récupération, la désignation du personnel responsable, ainsi qu'un inventaire des équipements et services critiques. Les indicateurs définis précédemment le RTO et RPO guident la stratégie de sauvegarde et de restauration. Le plan doit également documenter précisément les méthodes de restauration selon les supports utilisés, les lieux de stockage et les technologies mobilisées. Il prévoit une conservation alternative de la documentation du processus, par exemple sur papier permanent stocké de manière sécurisé par les responsables et les acteurs identifiés de la cellule ainsi que dans des archives patrimoniales. Des tests réguliers assurent son efficacité opérationnelle et l'identification des documents vitaux est essentiel. Leur perte peut entraîner des dysfonctionnements majeurs. Leur protection s'inscrit dans une logique de continuité institutionnelle et de résilience informationnelle.

Il est important de formaliser le PCA métier pour couvrir la gestion opérationnelle en situation de crise. La gestion de la continuité des activités constitue l'objectif principal menant à la résilience organisationnelle face aux crises. En période de perturbation, les contrôles internes peuvent être contournés et les exigences en matière de sécurité de l'information compromises.

La stratégie de sauvegarde en début de chapitre constitue un des éléments garantissant la disponibilité des informations. Il permet d'identifier les mesures de fonctionnement à prendre entre la détection de l'attaque, la qualification de la crise et la reprise du niveau normal de service. La gestion de la continuité permet ainsi de limiter les interruptions, et de protéger les processus métiers essentiels, contribuant à la pérennité et à la sécurité globale de l'organisation (Ghernaouti 2022; Boulet 2008).

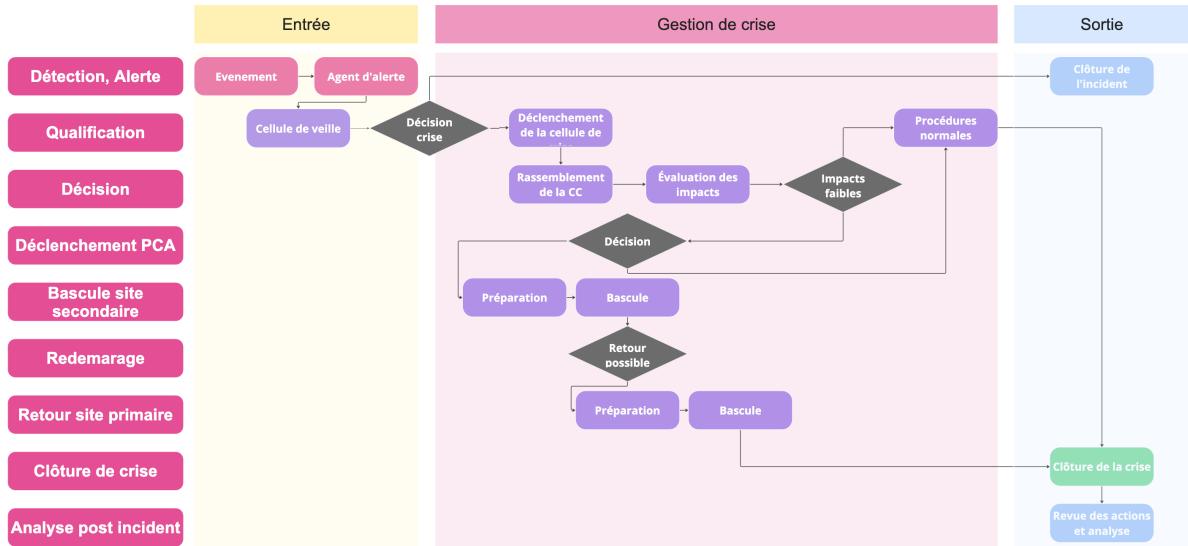
Faire face à des catastrophes susceptibles de paralyser l'ensemble des activités comme une cyberattaque massive ou une coupure prolongée de l'infrastructure critique n'est pas sans conséquence sur les équipes. La frontière entre incident et crise n'est pas toujours claire. Certains événements, présentent un impact suffisamment important pour nécessiter une réponse intermédiaire, sans pour autant déclencher le PCA (Boulet 2008). La gravité perçue d'un incident varie aussi selon la nature et la taille de l'organisation. Ce qui est considéré comme un simple désagrément technique pour l'UNIGE peut constituer un sinistre critique pour une structure plus modeste. Ainsi, dans une bibliothèque académique, l'indisponibilité temporaire d'un catalogue ou d'un système de prêt automatisé pourrait représenter un dysfonctionnement mineur, tandis qu'une perte d'accès prolongée aux ressources numériques ou à l'authentification centralisée serait perçue comme une crise majeure nécessitant l'activation de ce plan. La définition des responsabilités n'a pas été formalisée sous la forme d'une matrice RACI dans le cadre de ce travail, mais il est recommandé de l'intégrer en phase de déploiement, afin de clarifier les rôles entre responsables techniques, fonctionnels et institutionnels. L'outil a pour but d'identifier, pour chaque tâche, qui est Responsable (R), Autorisé à valider (A), Consulté (C) et Informé (I).

### **6.5.2 Mise en œuvre du plan de continuité d'activité, la gestion de crise**

Lorsqu'un incident survient, il est décisif de le reconnaître immédiatement comme tel, de le qualifier (InterCERT 2024a; 2024b) et d'activer sans délai une procédure prévue. La centralisation des informations techniques et décisionnelles doit permettre à l'organisation de garder le contrôle de la situation et d'adopter une posture proactive. Enfin, une communication cohérente doit être pensée, efficace et transparente en interne, pour éviter toute désinformation ou perte de confiance interne et externe. Elle doit être apte à maintenir le dialogue avec les parties prenantes et préserver la réputation institutionnelle. Si aucun canal de communication de secours est préétabli il est possible de se tourner vers les moyens personnels pour pouvoir communiquer. En ce sens la constitution d'un groupe de discussions sur une messagerie chiffrée via les terminaux personnels peut être un moyen de fortune pour assurer la liaison. Dans ce cas la liste des interlocuteurs contenue dans le plan de sauvetage des collections imprimées est suggérée dans un premier temps.

La capacité à identifier rapidement un incident, à contenir sa propagation et à organiser une bascule des services critiques constitue le premier pas d'une réponse. En raison de l'interdépendance entre les composantes du système d'information, une coordination transversale est indispensable dès les premières actions : isolement du réseau, protection des sauvegardes, conservation des journaux de traces, et rétablissement progressif des services essentiels (InterCERT, 2024). Ces opérations sont à prendre de façon collective en réunissant une cellule de crise qui sera en charge des étapes de décision (ANSSI 2021a).

Figure 20 - Gestion de crise et chaîne de décisions



CC BY NC Stephen Valot 2025

Lorsqu'une crise résulte d'une attaque cyber une cellule de crise dédiée à la cybersécurité est activée par la DIS, en collaboration avec la DiSTIC et le rectorat, lorsque les processus standards de gestion des incidents ne suffisent plus. Cette cellule est chargée de coordonner une réponse structurée (Figure 20). Elle assure plusieurs fonctions de l'analyse des solutions techniques, coordination des opérations, mobilisation des ressources nécessaires, et gestion de la communication interne de crise (ANSSI 2021b). Elle s'appuie sur deux niveaux d'intervention, un pilotage stratégique (définition des priorités, validation des plans d'action, arbitrages), et une coordination opérationnelle (mise en œuvre des mesures de défense, synthèse des retours terrain, accompagnement des communications). Cette organisation est indispensable pour limiter les impacts et assurer une reprise rapide des fonctions critiques.

La gestion de crise cyber repose sur l'anticipation d'événements exceptionnels compromettant le fonctionnement normal des services numériques. Une crise de ce type se caractérise par une interruption brutale des systèmes critiques (accès documentaire, plateformes pédagogiques, données de recherche), une perte de contrôle organisationnel et une forte incertitude décisionnelle (ANSSI 2021a). Une réponse efficace suppose une coordination rapide, des procédures préétablies, une communication, ainsi qu'un pilotage de la communication est aussi nécessaire avec l'appui des référents techniques et métiers.

En cas d'attaque confirmée par la cellule de crise classée de gravité 3,2 ou 1 selon l'échelle présentée ci-après (Tableau 10), une mesure d'isolement du réseau externe est déclenchée, entraînant la coupure de l'accès à Internet.

Tableau 10 - Niveau de mobilisation et évaluation d'impacts en cas de crise

Niveau d'incident	Description	Communication	Impacts	Exemple
1	Crise cyber critique – attaque majeure paralysant des services essentiels, nécessitant le déclenchement immédiat du PCA/PRA.	Communication officielle vers les usagers, partenaires, autorités et médias. Coordination avec les cellules de crise institutionnelles. Activation d'un canal unique d'information.	Paralysie de plusieurs services critiques ; perte potentielle de données ; atteinte à la réputation ; interruption d'activités pédagogiques ou de recherche. Impact CRITIQUE, combinaison de plusieurs scénarios à effets dominos avec atteinte massive à la continuité	(ex : ransomware à propagation rapide, compromission massive de données, attaque sur les systèmes de sauvegarde)
2	Incident cyber majeur nécessitant la mobilisation d'équipes pluridisciplinaires .	Information ciblée vers les services impactés, la direction, et les parties prenantes internes. Communication structurée pour éviter la panique.	Dysfonctionnement important d'un ou plusieurs systèmes ; risque de perte ou de fuite de données ; mise en œuvre de mesures correctives urgentes. Impact ÉLEVÉ à CRITIQUE, scénario composé ou amplification mutuelle	(ex : compromission d'un serveur stratégique, atteinte à l'intégrité des données, compromission d'identifiants à grande échelle)
3	Incident cyber significatif impliquant des ressources transverses .	Notification interne aux équipes concernées, documentation de l'incident et briefing post-incident. Rapport au RSSI.	Perturbation ponctuelle ou localisée ; impact limité à certains utilisateurs ou services ; menace maîtrisée. Impact ÉLEVÉ, affecte des services critiques de manière circonscrite	(ex : compromission d'un compte administrateur, tentative d'exfiltration de données, malware localisé)
4	Incident cyber modéré géré par une équipe restreinte .	Signalement au RSSI, documentation technique, gestion via les procédures standards.	Impact limité, sans atteinte grave aux données ; gestion en interne par les responsables techniques. Scénario isolé, impact limité, ne déclenche pas de scénario secondaire	(ex : phishing ciblé, détection d'activités suspectes, scan réseau anormal)
5	Situation normale – veille active et gestion quotidienne des alertes de sécurité	Pas de communication externe ; incidents enregistrés dans les outils de gestion et suivis par le SOC interne ou le prestataire MSSP.	Aucun impact ou impact négligeable sur les activités ; maintien des services avec surveillance continue. Activité de surveillance préventive – détection précoce, incidents sans impact significatif	(ex : tentatives de connexion échouées, mises à jour de sécurité, analyse de journaux, Tentatives de scan, phishing isolé, mises à jour critiques).

CC BY NC Stephen Valot 2025

Une fiche d'urgence ad hoc (Annexe 21) a été élaborée afin de structurer une réponse complète et pragmatique à l'un des scénarios les plus critiques identifiés au cours de ce travail : l'attaque par *ransomware*. Conçue comme un outil transversal, elle synthétise les actions à mener avant, pendant et après un incident de cybersécurité majeur, en cohérence avec les recommandations de référence (ANSSI 2020, 2021 ; CIGREF 2023 ; OFCS/DDPS 2024). Elle repose sur une sélection raisonnée de bonnes pratiques adaptées aux réalités des bibliothèques, et intègre la faisabilité opérationnelle, la culture de la résilience et la logique de continuité documentaire. En amont de l'incident, la fiche insiste sur les mesures préventives : mise en œuvre d'une politique de sauvegarde, mise à jour régulière des systèmes, cloisonnement du réseau, surveillance des accès, journalisation, sensibilisation des utilisateurs et gouvernance anticipative. Elle prévoit aussi des mécanismes d'alerte et de communication hors SI, la constitution d'une cellule de crise, et la centralisation de la documentation critique en format durable. En phase d'attaque, elle fournit une trame d'endiguement prévoyant un isolement immédiat des postes, l'ouverture d'une main courante, la préservation des preuves numériques, l'activation des partenaires techniques et pilotage coordonné de la crise. En sortie de crise, elle décrit les étapes d'une reconstruction comme la réinstallation des systèmes, la sécurisation renforcée, la révision des accès, et les retours d'expérience pour renforcer la posture globale de l'organisation.

Cette fiche s'adresse à un large éventail d'acteurs, dont l'impact de la crise sur les comportements peuvent être déroutants. Les responsables informatiques, équipes de cybersécurité, gestionnaires de la coordination et des collections, décideurs institutionnels, mais aussi personnels non-spécialistes et en contact quotidien avec le SI doivent être préparés à ce type d'incident. La procédure sert de socle pour des exercices de simulation, des formations ciblées, et des campagnes de sensibilisation. Ce livrable propose un référentiel opérationnel adapté au contexte, il relie la continuité d'activité, la préservation documentaire et la cybersécurité, afin de renforcer la résilience des bibliothèques et inscrire la sécurité dans les pratiques professionnelles.

### 6.5.3 Remédiation et analyse post incident

La remédiation constitue une phase exceptionnelle dans la gestion des incidents de sécurité. Elle s'inscrit dans un temps de rupture, distinct du cycle d'amélioration continue habituel, et vise à restaurer un état de fonctionnement opérationnel après une compromission. Dans cette étape instable (SNIA 2025; Wright 2024), la vigilance est de mise pour faire face à la possibilité de nouvelles attaques durant la reprise et limiter le risque de suraccident. Selon la norme ISO 27035, cette phase englobe quatre étapes distinctes (ANSSI 2023a):

- Endiguement : ralentir l'attaquant en introduisant de la friction dans ses actions pour permettre aux défenseurs de gagner en temps et en visibilité.
- Éviction : retirer durablement l'adversaire des zones sensibles du système.
- Éradication : Le nettoyage du système pour éliminer toute persistance de l'attaque, y compris les artefacts mineurs.
- Reconstruction : En soutien aux trois étapes précédentes, consiste à remettre en place des environnements sécurisés, et la fiabilité et l'intégrité du système.

La remédiation ne s'achève qu'avec le rétablissement des services critiques et l'assurance que l'adversaire est définitivement écarté. Elle doit être accompagnée d'une réflexion technique pour éviter toute récidive et rétablir la posture de sécurité initiale et la renforcée.

Dans une perspective intégrée de cybersécurité et de préservation, la criminalistique numérique ou *digital forensics* occupe aussi une position importante en tant que dispositif juridique, informatique et archivistique. Elle désigne un ensemble de techniques et de normes permettant d'identifier, de collecter, de préserver, d'analyser et de présenter des données numériques en tant que preuves, dans le cadre d'enquêtes pénales ou de procédures d'archivage à valeur probatoire (ISO 27037 :2012 ; ISO 30121 :2015). Dans notre contexte, la criminalistique numérique s'applique notamment à la sécurisation des infrastructures documentaires, à l'audit post-incident et à la reconstitution des environnements en cas de sinistre. Elle mobilise des outils techniques tels que le hachage, l'imaging, l'analyse mémoire ou réseau, ainsi que la documentation des chaînes de preuves. Ces pratiques peuvent s'intégrer à des dispositifs de réponse aux incidents, à l'image d'une « BERCE numérique » ou d'un poste sécurisé d'intervention s'appuyant sur des outils *open-source* comme Autopsy. En assurant la traçabilité, l'authenticité et l'intégrité des ressources numériques critiques, elle constitue un maillon essentiel de la résilience et est particulièrement utile pour reconstituer la chronologie des événements, mais aussi pour collecter, analyser et conserver des preuves numériques dans le cadre d'enquêtes, que ce soit lors d'incidents localisés à la bibliothèque ou dans des situations de crise à plus grande échelle nécessitant une analyse approfondie. Le poste dédié au niveau A de mise à disposition des données pourrait héberger les outils pour les cas d'usages de forensiques et de décontamination.

## 7. Évaluation, formation et amélioration continue

En identifiant les processus de l'organisation, ses dépendances ainsi que les risques associés, il est nécessaire de les mettre en relation et de les confronter à des mesures adaptées aux applications métiers critiques, de les évalués, les faire adoptés et les améliorés.

### 7.1 Stratégie de cyber défense pour les bibliothèques

Nombre de bibliothèques numériques, y compris les plus réputées, ne disposent pas encore des moyens adéquats pour faire face à l'intensification des menaces cyber. Des outils largement déployés dans d'autres secteurs, les systèmes de gestion des incidents, les dispositifs de détection d'anomalies ou les analyses de vulnérabilités restent peu utilisés. Une évolution des pratiques est nécessaire, alliant modernisation des infrastructures, adaptation organisationnelle et renforcement des compétences en cybersécurité (Bellini, Tammaro 2024).

Si l'on reprend l'étude de cas à propos de la British Library (Annexe 8) nous pouvons déjà déterminer plusieurs recommandations (British Library 2024) :

- Segmentation du réseau pour permettre de circonscrire une intrusion
- Généralisation de l'authentification multi-facteur et la gestion des priviléges d'accès
- Modernisation et mise à jour continue de l'infrastructure technique
- Surveillance active et continue pour la détection d'anomalies, la traçabilité des actions et une meilleure réactivité face aux signaux faibles ou aux activités suspectes
- Stratégies de sauvegarde s'impose. Le modèle de sauvegarde recommandé s'inspire de la logique dite « 3/2/1 », « 4/3/2/1 » (voir 3-2-1-1-0<sup>11</sup>).
- Avoir des plans de continuité et de reprise d'activité intégrant l'ensemble des systèmes critiques, catalogues, bases de données, les outils de consultation, et de maintenir une cartographie à jour des dépendances.

(British Library 2024; Grove 2024)

En complément des dispositifs de stockage, de sauvegarde, d'archivage et des solutions de mise à disposition en mode dégradé, des mesures préventives d'analyse s'avèrent indispensables pour renforcer la posture de cybersécurité des bibliothèques. Dans ce cas de figure, l'intégration d'un *Security Operations Center* (SOC) basé sur des outils *open source* constitue une réponse aux institutions ne disposant pas d'infrastructures mutualisées. Ce modèle permet de structurer une capacité autonome de détection, d'analyse et de réaction face aux incidents de sécurité (Déon 2023). Le socle proposé repose sur un pare-feu (*firewall*) et un système de détection et de prévention d'intrusion (*IDS/IPS*), une plateforme de gestion des informations et des événements de sécurité (*SIEM*) pour la corrélation des journaux, ainsi qu'un outil de détection et réponse sur les terminaux (*EDR*) pour la protection des postes de travail. Un outil d'orchestration, d'automatisation et de réponse aux incidents (*SOAR*) permet quant à lui d'automatiser les actions. À cela s'ajoutent des mécanismes de détection avancée, des outils de gestion des vulnérabilités, ainsi que des dispositifs de gestion des accès à privilégiés (PAM). Cette architecture permet de développer une capacité interne de réponse

---

<sup>11</sup> La méthode 3-2-1-1-0 est une stratégie de sauvegarde avancée qui recommande de conserver trois copies des données sur deux supports différents, dont une hors site, une hors ligne et sans erreur c'est à dire testée

aux menaces, tout en favorisant la montée en compétences, un langage commun entre les équipes, et l'émergence d'une culture partagée de la cybersécurité (Tableau 11).

Tableau 11 - Proposition d'un SOC open source

Brique	Rôle	Outils open source	Utilité
Firewall externe et interne	Filtrage réseau entrant/sortant, contrôle des accès	OPNsense, pfSense	Base de toute architecture de sécurité réseau
IDS/IPS	Détection/prévention d'intrusions réseau	Suricata, Snort	Surveillance active des flux, alerte ou blocage automatique
Analyse & classification du trafic	Inspection du trafic réseau, détection de comportements suspects	Zeek (ex-Bro)	Compréhension fine du trafic pour enrichir les alertes
SIEM	Centralisation, corrélation et visualisation des logs	Wazuh, ELK Stack, Graylog	Visibilité globale, détection d'anomalies, alertes en temps réel
Threat Intelligence, CTI (Cyber Threat Intelligence)	Sources de renseignement sur les menaces (IOC, TTP...), corrélation et contextualisation des menaces	OpenCTI, MISP	Contextualise les alertes, enrichit l'analyse des incidents, Partage de renseignement, anticipation
EDR	Surveillance et réponse sur les terminaux	Wazuh (intégré), Velociraptor	Détection des menaces persistantes et post-infection
UEBA	Analyse comportementale des utilisateurs et entités	Apache Spot, Wazuh (extension)	Déetecte les comportements inhabituels ou suspects
SOAR (Orchestration & Réponse)	Automatiser les actions de réponse (blocage IP, déconnexion, isolation, ...)	TheHive + Cortex, ou Shuffle, ou StackStorm	Gagne en réactivité, réduit la fatigue analyste, structure les playbooks
Gestion des vulnérabilités	Scanner les systèmes à la recherche de failles connues	OpenVAS, Nessus Essentials (freemium)	Pour compléter l'EDR/IDS avec une vision proactive
Gestion des accès / PAM	Suivi, limitation et audit des accès privilégiés	Augeas, CyberArk Open Source, ou Vault	Mieux contrôler l'usage des comptes sensibles
Honeytoken / Honeypots	Leurre pour détecter les mouvements latéraux ou scans	T-Pot, Kippo, Canarytokens, HoneyDB	DéTECTER DES COMPORTEMENTS SUSPECTS "SILENCIEUX"
Backup et résilience	Sauvegarde régulière des journaux, configurations et preuves	BorgBackup, Restic, ou Rsync + GPG	Essentiel en cas d'attaque destructrice
Gestion de la preuve / Forensiques	Préserver et analyser les traces numériques en cas d'incident	Autopsy, Velociraptor, GRR	Investigations post-incident et les procédures juridiques

Adapté et enrichi de (Déon 2023 ; Ghernaouti 2022; Barnum 2022)

## 7.2 Scénarios d'attaques

Pour tester la robustesse et la pertinence de l'approche présentée, plusieurs scénarios de crise ont été élaborés (Annexe 22), couplés à un tableau croisé des scénarios pour anticiper les effets conjoints. En face de chaque scénario identifié sont opposés les mesures de mitigation modélisées dans la partie précédente et permettent de comprendre le fonctionnement de la solution en situation de crise.

Chaque scénario reçoit une mesure correspondante pour assurer la continuité de l'accès aux ressources documentaires. Ce dispositif met aussi en lien les différentes stratégies de stockage, de sauvegarde, et d'archivage en fonction des objectifs de récupération pour l'enrichissement des modes dégradés d'accès. Le choix du niveau d'accès et de la solution de repli à activer dépend directement du niveau de gravité de la crise, tel que défini dans la grille d'évaluation. C'est cette évaluation qui déclenchera la bascule vers l'architecture alternative appropriée, après confirmation de la cellule de crise, pour enclencher une réponse adaptée à la criticité de la situation. La cartographie imagine 13 scénarios qui se décomposent en

événements de scénarios critiques qui peuvent être cumulatifs, chacun structuré selon les types, actifs impactés, dépendances, processus métier affectés, les TTP MITRE ATT&CK<sup>12</sup>, contre-mesures MITRE D3FEND, les risques ENISA, les mesures renforcées applicables, etc. Elle synthétise ainsi l'ensemble des livrables, et permet de valider la démarche en croisant les menaces identifiées et les solutions proposées. La matrice des dépendances inter-scénarios (Annexe 23) complète ce dispositif en révélant les effets en chaîne susceptibles de survenir. Elle identifie les scénarios déclencheurs, les effets secondaires et les compositions critiques comme le « Blackout numérique » ou la « Crise contractuelle », et teste la couverture des trois niveaux de sauvegarde et d'accès. Enfin, le système introduit des seuils d'alerte en fonction du nombre et de la liaison entre les différents cas de figure pour envisager les recours possibles et la mobilisation de la cellule de crise en cas d'effets en cascade.

Cette synthèse de la réflexion joue un rôle de stress-test des solutions techniques proposées, en validant leur couverture face à des cas concrets, leur capacité à escalader selon la gravité, et leur intégration dans une stratégie de gouvernance documentaire et numérique. Ces scénarios peuvent être utilisés lors de tests et de sensibilisations visant à élaborer la méthode Ebios RM au sein de *working groups* dans des institutions désireuses d'adopter la démarche de sécurité à leur tour. Mais surtout ils visent à démontrer de façon théorique que la solution est cohérente, et dimensionnée contre les menaces identifiées dans le contexte étudié.

### 7.3 Système de management de la sécurité de l'information

L'efficacité d'une démarche de résilience repose sur la mise en œuvre régulière de tests permettant de valider les dispositifs de secours, d'optimiser les délais de reprise et de garantir la mobilisation adéquate des équipes lorsque des interventions humaines sont requises. Ces tests, organisés selon des niveaux croissants de complexité, peuvent inclure des simulations sur table, des exercices en environnement de test ou de production, jusqu'à des bascules complètes dans le cadre d'un plan de reprise. Pour maîtriser les risques associés et limiter les impacts d'éventuels incidents, les organisations mettent en place un Système de management de la sécurité de l'information (SMSI). Ce dispositif structuré, fondé sur les principes de la norme ISO/IEC 27001(ISO 2022a, p. 27001), s'appuie sur des politiques, des procédures et des mécanismes techniques évolutifs, alignés sur les priorités métier et soumis à une amélioration continue.

Comme la politique de sécurité constitue un levier de la gouvernance organisationnelle elle doit structurer la sécurité comme un processus de pilotage continu, aligné sur des objectifs stratégiques explicites. Elle découle de l'évaluation des valeurs à protéger, des risques identifiés, et définit les orientations à mettre en œuvre pour y répondre de manière cohérente et proportionnée (Ghernaoui 2022). Étroitement liée à la gestion continue des risques, la gestion continue de la sécurité repose sur les mises à jour de l'identification des actifs critiques, la reconnaissance des menaces et vulnérabilités, et l'estimation des impacts potentiels. Elle ne peut être engagée qu'une fois la politique de sécurité définie en fonction de ces éléments (Ghernaoui 2022). La stratégie de sécurité s'intègre dans une vision à long terme itérative et agile pour répondre aux besoins spécifiques de protection de la Bibliothèque, face à l'évolution constante des menaces, des vulnérabilités et de l'environnement informatique. La sécurité

---

<sup>12</sup> Les correspondances TTPs du cadre MITRE ATT&CK, et contre-mesures de l'ontologie D3FEND enrichissent la modélisation des scénarios d'attaque. L'ajout d'un score CVSS permet de prioriser les vulnérabilités, leur criticité, facilitant la prise de décision technique.

s'établit dans une démarche de gestion continue et n'est jamais acquise de façon définitive (Ghernaouti 2022).

## 7.4 Sensibilisation et formation du personnel

Une enquête menée par le *Scholarly Networks Security Initiative* (SNSI) révèle des lacunes dans la compréhension des cybermenaces par les bibliothécaires en milieu académique, malgré l'augmentation confirmée des attaques au Royaume-Uni et ailleurs (Winter 2022). Si la majorité des professionnels interrogés se montrent conscients des enjeux liés à la protection des données personnelles et à la réputation institutionnelle, leur niveau d'expertise varie selon la taille de leur établissement. Leurs rôles dans la chaîne de cybersécurité est souvent perçus comme secondaire. En cas d'incident, 96 % des répondants se tournent d'abord vers les services informatiques, mais peu envisagent une implication directe, en matière de sensibilisation des usagers ou de remontée proactive d'alertes. L'étude montre aussi une méconnaissance des risques associés à l'utilisation de plateformes de contenus piratés telles que *Sci-Hub* ou *Library Genesis*. Une part significative des répondants ne le considère pas explicitement comme une menace. Ce flou, doublé d'une sympathie envers la philosophie de libre accès au savoir, contribue à une banalisation de pratiques qui exposent les réseaux universitaires à des compromissions par hameçonnage ciblé et vol d'identifiants (SNSI, 2021 ; Winter 2022). Le renforcement de la sécurité des environnements documentaires repose avant tout sur une montée en compétence et sur l'intégration d'une véritable culture de la sécurité dans les pratiques métier. Cela implique l'introduction de formations à la cybersécurité qui peuvent être déployées auprès du personnel, d'exercices pratiques, de tests de résilience et de simulations d'incident. Il s'agit de dépasser la logique de réaction ponctuelle pour faire émerger une conscience partagée des risques numériques.

Cette démarche doit s'accompagner de la création de groupes de collaboration interinstitutionnelles, où les équipes peuvent échanger sur les bonnes pratiques, les incidents rencontrés et les stratégies d'atténuation. C'est en croisant les expertises documentaires et informatiques que l'on pourra réduire les silos, renforcés par des systèmes dont on ne peut avoir qu'une visibilité partielle. Cette complexité, combinée à une érosion des compétences techniques au sein des bibliothèques, peut nuire à la réactivité en cas de crise. Cela suppose que les fonctions de l'information et celles de l'informatique se coordonne vers une intégration de la sécurité, de la continuité et de la préservation dans la gestion des ressources.

Enfin, la pénurie de spécialistes en cybersécurité renforce l'urgence de cette démarche. Pour les bibliothèques, former, sensibiliser et valoriser les compétences internes en sécurité de l'information devient un enjeu, au même titre que peut l'être la conservation physique des documents dans une idée de convergence des démarches.

## 8. Discussion, évaluation, recommandations

Entre les quelques lignes du livret d'urgence en cas de cyberattaques, recommandant de couper la connexion Internet, d'alerter le support informatique et de suivre les consignes, et les plus de 150 pages dédiées à la sauvegarde des collections physiques, un vide subsistait. Ce travail s'inscrit dans cet entredeux et vise à renforcer la résilience de l'accès aux ressources électroniques et à assurer leur préservation, au service de la mémoire scientifique et de sa transmission durable dans le temps et l'espace.

Face aux risques croissants pesant sur la conservation pérenne des données et des publications scientifiques, la communauté de la recherche appelle à renforcer la résilience des dépôts numériques. La fermeture de plateformes, faute de financement, d'anticipation ou de planification de la relève, constitue une menace directe, critique pour l'intégrité du patrimoine scientifique international (Hedley 2025).

Cette perte ou disparition d'une richesse commune (Messarra, Freeland, Ziskina 2024) n'est plus tolérable, les experts recommandent l'élaboration de plans de continuité structurés comme ce mémoire le suggère. Mais demande un approfondissement thématique sur la mise en réseau des dépôts entre institutions similaires, l'établissement d'accords formels de transfert de données, et l'utilisation de services d'archivage distribués, jusqu'à la mise en commun des infrastructures de préservation numérique pour les institutions qui partagent des missions similaires. Elles doivent reposer sur une duplication des contenus entre serveurs, garantir une restauration des contenus en cas de perte, et ce en limitant les points uniques de défaillance. C'est aussi une vigilance partagée qu'il convient de cultiver. Il est redondant d'évoquer à nouveau le financement de ces infrastructures et des ressources nécessaires à leur maintien, cependant l'ampleur de la question doit remettre en perspective les moyens, qui, restreints dans tous les secteurs culturels, doivent pouvoir être dimensionnés et suivis. Ne plus représenter un risque mais un appui indéfectible pour la continuité d'activité et la résilience de notre savoir comme bien commun.

### 8.1 Recommandations stratégiques et résilience opérationnelle

À l'issu de ce travail, les bibliothèques académiques doivent repenser leurs pratiques de gestion documentaire à l'aune de la résilience. Certaines recommandations peuvent guider à conduire cet objectif.

- **Intégrer les ressources électroniques dans la gouvernance informationnelle.** Les ressources numériques doivent être inscrites dans les plans de continuité (PCA/PRA) et les politiques de gestion documentaire. Cela implique l'élaboration d'une politique institutionnelle de préservation numérique à long terme, incluant l'utilisation de technologies d'archivage certifiées, une charte de gestion des ressources numériques, et l'utilisation d'outils communautaires comme le *Keepers Registry* pour garantir leur préservation effective.
- **Renforcer les cadres juridiques et contractuels en faveur des institutions.** Les institutions doivent clarifier la propriété et l'exploitation locale des métadonnées, adapter les contrats en conséquence, et défendre une autonomie accrue avec le soutien des consortiums. Il est essentiel d'inclure des clauses d'accès perpétuel et d'archivage dans les licences, de tenir une base documentaire complète des abonnements, et d'évaluer la fiabilité des supports par les fournisseurs.
- **Mettre en œuvre des solutions hybrides de sauvegarde et d'archivage.** Le recours à des services tiers certifiés doit être privilégié, tout en développant des copies internes

(dark archives, dépôts institutionnels) et des protocoles de bascule en cas de rupture de service ou litige. L'évaluation des formats, supports et intégration système favorise l'interopérabilité et la mutualisation. L'extraction régulière de métadonnées pour la création de catalogues de secours, la duplication des contenus critiques, et l'hébergement sur des infrastructures validées renforcent la redondance. Des solutions hybrides alliant sauvegardes locales et archivage mutualisé permettent de garantir la disponibilité, l'intégrité et la traçabilité des ressources essentielles.

- **Adopter une approche différenciée de gestion des risques.** La stratégie repose sur une cartographie des actifs, une analyse d'impact (BIA), une matrice des risques, et une classification des contenus selon leur criticité. Le coût des mesures de protection doit être mis en regard de la valeur stratégique ou patrimoniale des données. Une sélection de ressources numériques à haute valeur patrimoniale ou scientifique devrait être établie, afin d'en assurer prioritairement la préservation et la sécurisation.
- **Déployer des mesures techniques robustes et évolutives.** Les dispositifs doivent inclure l'authentification forte, des contrôles d'accès basés sur les rôles, ainsi que des solutions de prévention des fuites (DLP), de surveillance et d'analyse comportementales. Ces mesures renforcent la sécurité au niveau des usages, des évolutions technologiques et permettent la disponibilité, l'intégrité et la traçabilité des événements sur le réseau de la bibliothèque.
- **Inscrire la cybersécurité dans les politiques documentaires.** La cybersécurité, la continuité d'activité et l'archivage doivent être reconnues comme une priorité, intégrées aux procédures métiers et soutenues par des audits, des tests de scénarios critiques, et un budget durable dédié au maintien des capacités d'archivage et d'accès pérenne.
- **Développer les compétences et la culture de la sécurité.** Des formations continues sur les outils techniques, les contrats, la sécurité numérique, et la préservation doivent être proposées. Tous les profils, professionnels, chercheurs, étudiants doivent intégrer et être sensibilisés aux risques numériques.
- **Structurer la coopération interinstitutionnelle et développer le langage commun.** La collaboration doit être renforcée entre bibliothèques, services informatiques et services d'archives, afin de partager expériences et protocoles à l'échelle sectorielle, et de mettre en place des accords inter-institutionnels. Les mutualisations techniques doivent être encouragées.
- **Promouvoir la transparence et la reconnaissance des bibliothèques comme infrastructures critiques.** La publication des incidents et des stratégies de réponse renforce l'apprentissage collectif. Les États et bailleurs doivent reconnaître leur responsabilité et considérer les bibliothèques comme des infrastructures stratégiques nécessitant un soutien actif.

Il convient de dépasser la conception traditionnelle des publications électroniques comme objets figés, pour les reconnaître comme des données évolutives, intégrables dans des cycles de vie complets. Cette approche favorise une gouvernance documentaire alignée sur les principes de la science des données, renforçant la souveraineté, l'interopérabilité et la capacité d'analyse. Elle permet également de traiter les ressources électroniques comme des actifs informationnels, tout en réaffirmant le rôle stratégique des bibliothèques dans la gestion et la sécurisation de l'information, des savoirs et de la connaissance à une échelle plus granulaire.

## 8.2 Analyse critique des résultats

Cette étude repose sur l'observation et l'analyse d'une institution de grande envergure et un contexte institutionnel privilégié, disposant de moyens humains, techniques et financiers leur permettant de mettre en œuvre des politiques pertinentes de cybersécurité et de préservation à long terme. L'Université de Genève est déjà fortement engagée dans le traitement et l'accès

aux ressources électroniques et numériques, et bénéficient de structures et de soutiens institutionnels. Les propositions concernant la sauvegarde et l'accès pérenne sont des formulations théoriques et une phase de test de la solution de l'extraction à sa mise à disposition devrait être testée sous forme de preuve de concepts pour valider sa faisabilité et sa fiabilité. Aussi, il serait hasardeux d'extrapoler directement certains constats ou recommandations à des structures plus modestes, dont les capacités de mise en œuvre sont d'autant plus restreintes par des contraintes budgétaires et organisationnelles. L'étude présente d'autres limites liées à la composition du panel de répondants, restreint et déjà sensibilisé, qui offre une vision partielle des pratiques. L'accès limité aux données, en raison de contraintes de sécurité des systèmes d'information et du modèle économique des éditeurs, a empêché de chiffrer précisément les volumes de données que pourrait représenter l'extraction du catalogue. La temporalité réduite ainsi que la réalisation individuelle de ce travail appellent également une poursuite collective et institutionnelle afin de consolider et d'approfondir les résultats. Enfin, il existe des solutions privées de préservation, à l'image de *Docuteam Cosmos* utilisé par la BNS, mais leur analyse ne relève pas du périmètre de ce travail, centré sur les solutions disponibles dans l'institution ; elles pourraient faire l'objet d'une étude complémentaire.

Toutefois, les enjeux de résilience documentaire, pérennité des accès, protection des contenus numériques, transcendent les différences d'échelle et de moyens. Ils concernent l'ensemble du paysage documentaire, y compris les bibliothèques patrimoniales, universitaires ou spécialisées de petite taille, souvent confrontées à une précarité structurelle. Dans cette perspective, l'étude tente également d'ouvrir des pistes de réflexion pour ces acteurs, en insistant sur l'importance d'une planification, où la sécurité et la préservation ne sont pas pensées comme des coûts supplémentaires, mais comme des composantes à intégrer en amont des projets, notamment dans les demandes de financement auprès des bailleurs de fonds. Il serait opportun, par exemple, que les projets de recherche prévoient explicitement le financement non seulement de la numérisation des corpus centraux, mais également des ressources périphériques consultées, afin de contribuer activement à l'enrichissement du patrimoine numérique collectif. Cette approche suppose que les enjeux de conservation, d'accès équitable et de valorisation à long terme soient pensés eux aussi dès la phase de conception du projet, en lien étroit avec les objectifs scientifiques, documentaires et sociétaux.

La mise en œuvre d'un registre des actifs critiques en bibliothèque représente une avancée conceptuelle qui invite les bibliothèques à dépasser une logique de gestion descriptive des collections, pour adopter une approche fondée sur la valeur stratégique, la criticité des contenus et leur rôle dans la continuité de la mission. L'élaboration d'un tel outil suppose un investissement en formation, en accompagnement du changement et en expertise, afin d'identifier, documenter et protéger les ressources dont la disparition constituerait une perte irréversible. Cet outil deviendra à terme un levier essentiel pour prioriser les efforts de sauvegarde, justifier les arbitrages budgétaires et garantir l'accès pérenne aux savoirs dans un environnement numérique incertain. La sécurité de l'information et la préservation du patrimoine documentaire doivent être considérées comme des objectifs collectifs, partagés, et portés par une vision stratégique commune.

### **8.3 Perspectives et discussion**

Une orientation prometteuse consisterait à créer à partir de l'existant ou rejoindre une infrastructure d'archivage à long terme mutualisée, portée par un consortium d'acteurs publics

tels que les hautes écoles, les bibliothèques nationales ou les archives cantonales. Ce modèle viserait à garantir la préservation pérenne des collections électroniques critiques, tout en réduisant la dépendance aux éditeurs commerciaux et prestataires SaaS. Conçue selon les normes ISO 14721 (OAIS) et ISO 16363, une telle plateforme assurerait les exigences de traçabilité, d'intégrité et d'interopérabilité, tout en mutualisant les coûts d'infrastructure, d'expertise et de maintenance. Cette approche renforcerait la souveraineté documentaire des institutions participantes, mais aussi leur capacité à faire face collectivement aux menaces pesant sur la conservation numérique du patrimoine scientifique.

Une autre piste prospective, discutée lors des réunions avec le pôle informatique documentaire ainsi qu'avec certains des participants aux entretiens, consisterait à entraîner un modèle d'intelligence artificielle local à partir d'un corpus sélectionné de publications jugées prioritaires par la Bibliothèque. Ce modèle, hébergé au sein même de l'institution, permettrait de garantir la souveraineté des données et d'assurer un usage interne, respectueux des cadres juridiques. Une telle infrastructure offrirait une double valeur ajoutée. Dans un contexte normal, elle permettrait de valoriser les collections à travers des fonctionnalités d'indexation, de résumé ou de recherche assistée et en cas d'interruption de service, d'incident cyber ou de rupture contractuelle, le modèle pourrait assurer un accès dégradé à la connaissance embarquée, constituant ainsi une extension résiliente de la collection. Cette approche doit s'inscrire dans une logique de préservation et de continuité informationnelle, en mobilisant les technologies émergentes de manière éthique.

Une piste de réflexion, plus inattendue, résulte des recherches sur certaines pratiques issues de la sphère cybercriminelle et des communautés *hackers*. Nous pouvons reconnaître comme efficace leur capacité à maintenir des plateformes en ligne dans des environnements fortement hostiles ou instables. L'exemple des places de marché illégales sur le darknet, ou des plateformes pirates telles que *Sci-Hub*, ou *Library Genesis*, prouvent leur résilience. Ces opérateurs ont adopté une stratégie de mirroring permanent, reposant sur la duplication systématique de leurs sites sur plusieurs instances redondantes, réparties à travers différentes zones du réseau superposé et décentralisé Tor. Cette approche leur permet de poursuivre leurs activités malgré les condamnations et interdictions, les attaques ou les saisies opérées par les autorités. Si le contexte est évidemment éloigné de celui des institutions publiques, l'interprétation technique de la continuité d'activité adoptée par ces groupes peut néanmoins inspirer certaines pratiques. L'usage de la redondance distribuée, de l'auto-hébergement, et de l'obfuscation stratégique applique une compréhension intéressante des enjeux de souveraineté technologique et de décentralisation des points de défaillance. Transposées dans un cadre légal et institutionnel, ces méthodes pourraient renforcer la robustesse des plateformes documentaires. Cette lecture « inversée » des pratiques adverses invite ainsi à reconsiderer certaines stratégies de résilience en s'inspirant de modèles agiles, décentralisés et techniquement inventifs. L'exploration de solutions de stockage distribuées, *blockchain-like* comme *Arweave* (2021), fondées sur des architectures décentralisées et de stockage permanent, pourrait offrir des alternatives pour la pérennité et la résilience des contenus numériques, en assurant une réplication décentralisée, résistante aux défaillances uniques ou aux censures. La science s'est déjà inspirée du protocole pair-à-pair avec *Academic Torrents* (Cohen, Lo 2014) pour la diffusion collaborative de données scientifiques. Alternatives plus ouvertes et communautaires, leurs potentiels méritent une attention dans les stratégies hybrides de préservation numérique durable.

Les archives jouaient un rôle passif dans les stratégies de gestion de données. Elles étaient perçues comme une obligation réglementaire, un coffre-fort numérique permettant de satisfaire les exigences de conformité sans valeur opérationnelle. Cette vision restrictive évolue et les archives numériques tendent à devenir une ressource stratégique exploitables, intégrée dans les dynamiques d'innovation et de valorisation (Donaldson, Bell 2018). Dans de nombreux secteurs, les organisations disposent désormais de volumes massifs de données archivées et stockées dans des formats économiques comme « *l'object storage*<sup>13</sup> ». Ces données constituent un patrimoine informationnel, scientifique et historique de grande valeur, exploitable dans plusieurs cas d'usage. Premièrement, à des fins analytiques, d'analyse décisionnelle, statistique, à travers l'identification de tendances ou la modélisation de comportements. Deuxièmement, elles permettent l'alimentation de modèles d'intelligence artificielle générative grâce à la richesse et à la profondeur temporelle des données archivées (Wright 2024). Enfin, c'est l'usage des archives comme un support de reconstruction des systèmes d'informations dont il est question. Les caractéristiques d'authenticité, de fiabilité, d'intégrité leurs permettent un rôle opérationnel pour la continuité d'activité des bibliothèques. L'information qualifiée de froide, acquiert une importance décisive dans les processus d'anticipation et de résilience.

Ainsi l'archivage à long terme devient une des composantes stratégiques de la cybersécurité. Les systèmes d'archivage électronique conformes garantissent les caractéristiques qui sont les qualités correspondantes à la résilience organisationnelle face aux cyberattaques. L'archivage ne constitue plus une fin de cycle, mais une mesure active de cyberdéfense (Velluet 2024). Le recours à ces technologies permettent de garantir la conservation de contenus augmentés de métadonnées auto descriptives, tout en répondant aux exigences de gestion, de diffusion et de contrôle d'accès. Elles sont complémentaires à une gouvernance de la sécurité de l'information structurée selon la norme ISO 27001 (Velluet 2024). Toutefois, cette sécurisation ne garantit pas à elle seule l'accès pérenne. Celui-ci dépend aussi de mécanismes de migration, de réversibilité, face à l'obsolescence technologique et la dépendance vis-à-vis des prestataires. Ces enjeux de préservation numérique doivent être renforcés par des compétences que bibliothèques, services d'archives, et services informatiques doivent impérativement développer conjointement.

La pérennité de l'archivage suppose d'intégrer son financement dès la conception des projets de recherche, en réservant une part des budgets d'acquisition et de cybersécurité au soutien des solutions de préservation. Mais elle repose également sur un plaidoyer renforcé en faveur de l'Open Science, afin de réduire la dépendance aux modèles commerciaux fermés, de garantir la disponibilité du patrimoine scientifique dans des infrastructures ouvertes et de valoriser la recherche comme un bien commun, soutenu par des compétences interprofessionnelles durables. La préservation numérique s'impose comme un élément stratégique de remédiation en contexte de cybersécurité. L'archive, lorsqu'elle est distincte et isolée des environnements de production et du réseau constitue la protection la plus fiable pour une récupération différée des données non corrompues. Il s'agit de conserver l'équilibre entre la protection de la disponibilité, de l'intégrité et de la confidentialité. La distinction entre sauvegarde et archivage, bien que théoriquement établie, tend à s'estomper, au regard des

---

<sup>13</sup> Le stockage objet enregistre chaque fichier sous forme d'un objet autonome, accompagné de métadonnées et d'un ID unique. Contrairement au stockage en fichiers ou en blocs, le stockage objet est non hiérarchique, scalable et adapté à la conservation de volumes importants de données non structurées

évolutions techniques et de la remise en question du modèle des trois âges documentaires. Au-delà de leur rôle traditionnel, les archives sont de plus en plus mobilisées à des fins d'analyses forensiques post-incident, ou de reconstitution d'environnements sains. Cette évolution positionne l'archive comme un actif dynamique au service de la résilience organisationnelle des bibliothèques. Dès lors, envisager l'archivage comme outil de remédiation face aux *ransomwares* valide l'hypothèse initiale, à condition de l'inscrire dans une gouvernance adaptée. Cela implique la mise en œuvre de politiques de conservation et d'archivage, le recours à des technologies fiables et de confiance, et l'automatisation de la gestion des accès. L'archivage à long terme dépasse son rôle de mémoire pour devenir un support actif de la stratégie de cybersécurité.

## 9. Conclusion

La cybersécurité est un domaine complexe, en raison de sa nature multidisciplinaire et de l'exigence technique qu'elle implique. Sa compréhension globale demeure fragmentée. Cette complexité tient à la fois à l'étendue de ses composantes, et à la profondeur d'expertise requise dans chacune d'elles. La pérennité des collections électroniques et des ressources numériques ne peut être envisagée sans une intégration de la cybersécurité dans la préservation. Elles poursuivent des objectifs convergents pour garantir l'intégrité, la disponibilité et la confidentialité des actifs informationnels dans la durée, et reposent sur des exigences communes en matière de résilience. Une stratégie fédérée de gouvernance informationnelle doit les mettre au service de la continuité d'accès au patrimoine scientifique.

Pour garantir la sécurité des collections, les institutions doivent disposer d'une vision partagée des risques, identifier les menaces, les actifs à protéger, les motivations des attaquants, ainsi que les vecteurs d'attaque potentiels. Cela implique de définir les responsabilités en matière de sécurité, les moyens techniques et organisationnels mobilisables, et d'inscrire cette démarche dans une temporalité cohérente, préparant les réactions immédiates, les stratégies de mitigation à moyen terme et les objectifs de résilience à long terme.

Les enjeux de cybersécurité ont été abordés à travers l'application des méthodes et pratiques issues de l'archivistique, de la bibliothéconomie et des technologies de l'information. Cela suggère une capacité d'abstraction, mais avant tout un recul critique sur les pratiques professionnelles établies. Dans le contexte marqué par la complexité croissante, et l'omniprésence des environnements numériques, cette réflexion est indispensable, salutaire, pour appréhender les problématiques de manière transversale et évolutive. La protection des systèmes d'information en bibliothèques requiert un langage commun entre professionnels de l'information, informaticiens et décideurs. Quant à l'évolution des menaces, ce sont les renforcements des compétences techniques, la sensibilisation des équipes et la reconnaissance de la valeur stratégique des ressources électroniques qui permettent l'instauration d'une culture de la résilience. L'émergence d'une gouvernance cohérente et concertée repose sur la coopération interservices et interinstitutionnelles.

La combinaison de dispositifs techniques de sécurisation, d'engagements contractuels et d'une implication humaine renforcée constituent les garanties d'un accès pérenne et résilient aux publications scientifiques. Ces conclusions légitiment le besoin de renforcement des compétences techniques et la valorisation des expertises en bibliothèque. Une protection effective requiert également une compréhension des enjeux sociaux et institutionnels, pour affirmer une souveraineté sur les données et les systèmes que les bibliothèques exploitent. Cela implique d'orienter le développement et l'administration des outils selon des choix et des valeurs, vers une vision du service public qui dépasse la portée à court terme. Un engagement durable doit être soutenu par des financements capables de répondre aux enjeux de la transition numérique. La sauvegarde seule ne suffit plus, l'archivage prend une nouvelle dimension, en s'imposant comme un actif opérationnel de remédiation pour la continuité d'activité. En reconfigurant la gestion des collections numériques dans une logique d'actifs stratégiques et intégrés aux cycles de vie des données, il est permis de repenser la conservation dès la conception et d'aboutir à un équilibre entre préservation, accessibilité et résilience, dans un continuum archivistique adapté aux exigences contemporaines.

## Bibliographie

ADENIUM, 2018. *Mettre en œuvre un PCI - PLAN DE CONTINUITE INFORMATIQUE* [en ligne]. Adenium-BRG. Guide Adenium . Disponible à l'adresse : [https://www.adenium.fr/wp-content/uploads/2018/07/Guide\\_Adenium\\_PCI\\_2018.pdf](https://www.adenium.fr/wp-content/uploads/2018/07/Guide_Adenium_PCI_2018.pdf) [consulté le 15 mars 2025].

ADENIUM, 2022. *Elaborer son PCA selon la norme ISO 22301 - PLAN DE CONTINUITE D'ACTIVITE* [en ligne]. Paris, France : Adenium-BRG. Guide . Disponible à l'adresse : <https://www.adenium.fr/wp-content/uploads/2021/02/Elaborer-son-PCA-selon-la-norme-ISO-22301.pdf> [consulté le 15 mars 2025].

ALEXANDRE, Aude, 2014. Archivage papier et/ou électronique et accès pérenne aux ressources documentaires électroniques en texte intégral en Fédération Wallonie-Bruxelles. .

ALEXANDRE, Aude, 2015. L'accès à long terme aux périodiques scientifiques électroniques dans les universités de la Fédération Wallonie-Bruxelles. Quelles solutions? [en ligne]. Disponible à l'adresse : [https://www.academia.edu/102537065/Lacc%C3%A8s\\_%C3%A0\\_long\\_terme\\_aux\\_p%C3%A9riodiques\\_scientifiques\\_%C3%A9lectroniques\\_dans\\_les\\_universit%C3%A9s\\_de\\_la\\_F%C3%A9d%C3%A9ration\\_Wallonie\\_Bruxelles\\_Quelles\\_solutions](https://www.academia.edu/102537065/Lacc%C3%A8s_%C3%A0_long_terme_aux_p%C3%A9riodiques_scientifiques_%C3%A9lectroniques_dans_les_universit%C3%A9s_de_la_F%C3%A9d%C3%A9ration_Wallonie_Bruxelles_Quelles_solutions) [consulté le 8 mars 2025].

ALMAHMOUD, Zaid et al., 2023a. A holistic and proactive approach to forecasting cyber threats. *Scientific Reports*. Vol. 13, no 1, p. 8049. DOI 10.1038/s41598-023-35198-1.

Amendment to Copyright Act, 2015 *openaccess.nl* [en ligne]. Disponible à l'adresse : <https://www.openaccess.nl/en/events/amendment-to-copyright-act> [consulté le 18 juin 2025].

ANSSI, 2020. *Attaques par rançongiciels, tous concernés. | Comment les anticiper et réagir en cas d'incidents ?* [en ligne]. Agence nationale de la sécurité des systèmes d'information. Disponible à l'adresse : <https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes> [consulté le 6 mars 2025].

ANSSI, 2021a. *Crise cyber, les clés d'une gestion opérationnelle et stratégique* | ANSSI [en ligne]. Agence nationale de la sécurité des systèmes d'information. Disponible à l'adresse : <https://cyber.gouv.fr/publications/crise-cyber-les-cles-dune-gestion-operationnelle-et-strategique> [consulté le 6 mars 2025].

ANSSI, 2021b. *Anticiper et gérer sa communication de crise cyber* [en ligne]. Agence nationale de la sécurité des systèmes d'information. Disponible à l'adresse : <https://cyber.gouv.fr/publications/anticiper-et-gerer-sa-communication-de-crise-cyber> [consulté le 6 mars 2025].

ANSSI, 2023a. *Cyberattaques et remediation* [en ligne]. Paris : Agence nationale de la sécurité des systèmes d'information. Remediation. Disponible à l'adresse : [https://cyber.gouv.fr/sites/default/files/document/20231218\\_Volet\\_operationnel\\_cyberattaque\\_setremediation\\_a5\\_v1j.pdf](https://cyber.gouv.fr/sites/default/files/document/20231218_Volet_operationnel_cyberattaque_setremediation_a5_v1j.pdf) [consulté le 7 juillet 2025].

ANSSI, 2023b. *Sauvegarde des systèmes d'information* [en ligne]. Agence nationale de la sécurité des systèmes d'information. Disponible à l'adresse : <https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation> [consulté le 1 avril 2025].

ANSSI, 2024a. Le CyberDico. *Agence Nationale de la Sécurité des Systèmes d'Information* [en ligne]. 2024. Disponible à l'adresse : <https://cyber.gouv.fr/le-cyberdico#M> [consulté le 14 juin 2025].

ANSSI, 2024b. *La méthode EBIOS Risk Manager* [en ligne]. Paris : Agence nationale de la sécurité des systèmes d'information. Version 1.5. Disponible à l'adresse : <https://cyber.gouv.fr/publications/la-methode-ebios-risk-manager-le-guide> [consulté le 6 mars 2025].

ARWEAVE, 2021. Arweave Wiki. [en ligne]. 2021. Disponible à l'adresse : <https://arwiki.arweave.net/#/en/karma> [consulté le 20 juillet 2025].

ATTWOOD, Teresa K., AGIT, Bora et ELLIS, Lynda B. M., 2015. Longevity of Biological Databases. *EMBnet.journal*. Vol. 21, no 0, p. 803. DOI 10.14806/ej.21.0.803.

BAILLARGEON, Diane et al. (éd.), 2019. *Typologie des documents des organisations, 2e édition : De la création à la conservation*. 2. Presses de l'Université du Québec. ISBN 978-2-7605-5177-0.

BANAT-BERGER, Françoise, DUPLOUY, Laurent et HUC, Claude, 2009. *L'archivage numérique à long terme : les débuts de la maturité?* La documentation française. ISBN 2-11-006942-2.

BARATEIRO, José et al., 2010. Designing digital preservation solutions: A risk management-based approach. *International Journal of Digital Curation* [en ligne]. Vol. 5, no 1, pp. 4-17. Disponible à l'adresse : <https://ijdc.net/ijdc/article/view/140> [consulté le 5 juillet 2025].

BARBEY, Grégoire, 2025. Voici la note sur laquelle le Conseil d'Etat genevois s'est appuyé pour valider le déploiement de Microsoft 365. *Le Temps* [en ligne]. Genève, 24 juin 2025. Disponible à l'adresse : <https://www.letemps.ch/cyber/exclusif-voici-la-note-sur-laquelle-le-conseil-d-etat-genevois-s-est-appuye-pour-valider-le-deploiement-de-microsoft-365> [consulté le 26 juin 2025].

BARNUM, Todd, 2022. *Cybersécurité : le guide du RSSI*. Paris : First interactive. ISBN 978-2-412-07356-8.

BEAGRIE, Neil, 2013. *Preservation, Trust and Continuing Access for e-Journals*. Digital Preservation Coalition. DOI 10.7207/twr13-04.

BELLINI, Emanuele et TAMMARO, Anna Maria, 2024. Cybersecurity for digital libraries: an interview with Emanuele Bellini. *Digital Library Perspectives*. Vol. 40, no 2, pp. 348-355. DOI 10.1108/DLP-05-2024-147.

BIBLIOTHÈQUE NATIONALE, 2019. Publications académiques. [en ligne]. 2019. Disponible à l'adresse : <https://www.nb.admin.ch/snli/fr/home/fachinformationen/e-helvetica/hochschulschriften.html> [consulté le 25 mars 2025].

BOERO, Alexandre, 2025a. L'ANSSI alerte sur l'explosion des cyberattaques qui touchent le Cloud, toujours plus menacé. *clubic.com* [en ligne]. 21 février 2025. Disponible à l'adresse : <https://www.clubic.com/actualite-554553-l-anssi-alerte-sur-l-explosion-des-cyberattaques-qui-touchent-le-cloud-toujours-plus-menace.html> [consulté le 7 mars 2025].

BOERO, Alexandre, 2025b. Cloudflare contre une nouvelle attaque DDoS record, brève mais d'une folle intensité. *clubic.com* [en ligne]. 19 juin 2025. Disponible à l'adresse : <https://www.clubic.com/actualite-569592-cloudflare-contre-une-nouvelle-attaque-ddos-record-breve-mais-d'une-folle-intensite.html> [consulté le 26 juin 2025].

BOULET, Patrick, 2008. *Plan de continuité d'activité : secours du système d'information*. Paris : Hermès Science. Management et informatique. ISBN 978-2-7462-2048-5.

BOURGIN, Yoann, 2024. Internet Archive victime d'une cyberattaque, les données de 31 millions d'internautes dans la nature. *Usine Digitale* [en ligne]. 10 octobre 2024. Disponible à l'adresse : <https://www.usine-digitale.fr/article/internet-archive-victime-d'une-cyberattaque-les donnees-de-31-millions-d-internautes-dans-la-nature.N2220284> [consulté le 31 mai 2025].

BOWIE, Simon, 2024. The British Library hack is a warning for all academic libraries - Impact of Social Sciences. *Impact of Social Sciences - Maximizing the impact of academic research* [en ligne]. 19 mars 2024. Disponible à l'adresse : <https://blogs.lse.ac.uk/impactofsocialsciences/2024/03/19/the-british-library-hack-is-a-warning-for-all-academic-libraries/> [consulté le 16 juin 2025].

BREEDING, Marshall, 2024. Libraries Under Cyberattack. *Computers in Libraries* [en ligne]. Vol. 44, no 02. Disponible à l'adresse : <https://librarytechnology.org/document/29866> [consulté le 4 décembre 2024].

BRITISH LIBRARY, 2024. *LEARNING LESSONS FROM THE CYBER-ATTACK*, *British Library Cyber Incident Review* [en ligne]. London, United Kingdom : British Library. Disponible à l'adresse : [https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf/](https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf) [consulté le 2 novembre 2024].

BROWNE, Ryan, 2024. How a software update from cyber firm CrowdStrike caused one of the world's biggest IT blackouts. *CNBC* [en ligne]. 19 juillet 2024. Disponible à l'adresse : <https://www.cnbc.com/2024/07/19/what-is-crowdstrike-crwd-and-how-did-it-cause-global-it-outages.html> [consulté le 8 juillet 2025].

BURGI, Pierre Yves et MAKHLOUF SHABOU, Basma, 2021. Le projet Data Life-Cycle Management (DLCM) en Suisse : une gestion des données de la recherche pensée pour ses utilisateurs. *I2D - Information, données & documents*. Vol. 2, no 2, pp. 87-95. DOI 10.3917/i2d.212.0087.

BURNEL, Florian, 2025. Web : Cloudflare bloque les robots d'exploration IA. [en ligne]. 3 juillet 2025. Disponible à l'adresse : <https://www.it-connect.fr/cloudflare-bloque-les-robots-exploration-ia-et-propose-un-modele-de-pay-per-crawl/> [consulté le 6 juillet 2025].

CAPDAREST-AREST, Nicole, TOMPSON, Sara et ZIPPERER, Lorri, 2022. Persistent service even in disruptive times: an introduction to resilience engineering. *Journal of the Medical Library Association*. Vol. 110, no 1, pp. 139-145. DOI 10.5195/jmla.2022.1359.

CARACO, Alain, 2019. Open access et bibliothèques. *Arabesques*. No 93, pp. 6-7. DOI 10.35562/arabesques.543.

CARAMANCION, Kevin Matthe et al., 2022. The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats. *Data*. Vol. 7, no 4, p. 49. DOI 10.3390/data7040049.

CAVALIER, François et POULAIN, Martine, 2015. *Bibliothèques universitaires : nouveaux horizons* [en ligne]. Paris : Éditions du Cercle de la Librairie. Bibliothèques. ISBN 978-2-7654-1469-8. Disponible à l'adresse : <https://www.cairn.info/bibliotheques-universitaires-nouveaux-horizons--9782765414698.htm>

CERN, 2025. Sécurité informatique : le coût de la compromission. *CERN* [en ligne]. 25 mars 2025. Disponible à l'adresse : <https://home.cern/fr/news/news/computing/computer-security-cost-compromise> [consulté le 27 mars 2025].

CERT-FR, 2025. *Rapport menaces et incidents - Cloud computing - État de la menace informatique* [en ligne]. France : Centre gouvernemental de veille, d'alerte et de réponse aux

attaques informatiques. Disponible à l'adresse : <https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-001/> [consulté le 6 mars 2025].

CHAVANNE, Yannick, 2022. Cyberattaque contre l'Université de Neuchâtel: des données volées publiées sur le darkweb (update). *ICT Journal* [en ligne]. 28 février 2022. Disponible à l'adresse : <https://www.ictjournal.ch/news/2022-02-28/cyberattaque-contre-luniversite-de-neuchatel-des-donnees-volees-publiees-sur-le> [consulté le 7 mars 2025].

CHEN, Jay, 2022. A Look Into Public Clouds From the Ransomware Actor's Perspective. *Unit 42* [en ligne]. 16 mai 2022. Disponible à l'adresse : <https://unit42.paloaltonetworks.com/ransomware-in-public-clouds/> [consulté le 8 juin 2025].

CHRISTIAN, Brian, GRIFFITHS, Tom et GRIFFITHS, Tom, 2023. *Penser en algorithmes: [comment de simples stratégies inspirées de l'informatique peuvent transformer votre vie]*. Version poche 2023. Lausanne : Quanto. ISBN 978-2-88915-255-1.

CIGREF, 2023. *Cigref - Réagir à une cyberattaque massive - Février 2023* [en ligne]. Paris. Réagir à une cyberattaque massive . Disponible à l'adresse : <https://www.cigref.fr/reagir-a-une-cyberattaque-massive> [consulté le 6 mars 2025].

CISA, 2023. *Understanding Ransomware Threat Actors: LockBit* [en ligne]. USA : Cybersecurity and Infrastructure Security Agency. Disponible à l'adresse : <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a> [consulté le 6 mars 2025].

CLAERR, Thierry et MOUFFLET, Jean-François, 2014. Gestion de la conservation des collections numériques. In : BARRON, Géraldine et LE GOFF-JANTON, Pauline (éd.), *Intégrer des ressources numériques dans les collections*. Villeurbanne : Presses de l'enssib. La Boîte à outils. ISBN 978-2-37546-057-3. DOI 10.4000/books.pressesenssib.11678. container-title: Intégrer des ressources numériques dans les collections

CLOCKSS, 2025. Swiss Archives of Neurology, Psychiatry and Psychotherapy. *CLOCKSS* [en ligne]. 2025. Disponible à l'adresse : <https://clockss.org/triggered-content/swiss-archives-of-neurology-psychiatry-and-psychotherapy/> [consulté le 16 juin 2025].

COAR, 2025. *Open repositories are being profoundly impacted by AI bots and other crawlers: Results of a COAR Survey* [en ligne]. Confederation of Open Access Repositories. Disponible à l'adresse : <https://coar-repositories.org/news-updates/open-repositories-are-being-profoundly-impacted-by-ai-bots-and-other-crawlers-results-of-a-coar-survey/> [consulté le 2 mai 2025].

COHEN, Joseph Paul et LO, Henry Z., 2014. Academic Torrents: A Community-Maintained Distributed Repository. In : *Proceedings of the 2014 Annual Conference on Extreme Science and Engineering Discovery Environment*, pp. 1-2. Atlanta GA USA : ACM. 13 juillet 2014. DOI 10.1145/2616498.2616528.

CONFEDERATION SUISSE, 2024. Nouvelle loi sur la protection des données (nLPD). [en ligne]. 2024. Disponible à l'adresse : <https://www.kmu.admin.ch/kmu/fr/home/fakten-und-trends/digitalisierung/datenschutz/neues-datenschutzgesetz-revdsg.html> [consulté le 17 juillet 2025].

CONSEIL FÉDÉRAL, 2020. *Loi fédérale sur le droit d'auteur et les ...* [en ligne]. RO 2020 1003. Disponible à l'adresse : <https://www.fedlex.admin.ch/eli/oc/2020/181/fr> [consulté le 2 juillet 2025].

CONSEIL FÉDÉRAL, 2024. *Loi fédérale sur la sécurité de l'information* [en ligne]. RO 2024 257. Disponible à l'adresse : <https://www.fedlex.admin.ch/eli/oc/2024/257/fr> [consulté le 2 juillet 2025].

CORDEL, Frédéric, 2019. Chapitre 5. L'identification et l'évaluation des risques. *Référence Management* [en ligne]. Vol. 3, pp. 121-145. Disponible à l'adresse : <https://shs.cairn.info/gestion-des-risques-et-controle-interne--9782311406030-page-121> [consulté le 26 juin 2025].

CORRADO, Edward M. et MOULaison, Heather Léa, 2014. *Digital preservation for libraries, archives, and museums*. Lanham : Rowman & Littlefield. ISBN 0-8108-8712-6.

DDPS, Département fédéral de la défense, de la protection de la population et des sports, 2023. *Cyberstratégie nationale CSN* [en ligne]. Berne : Office Fédéral de la Cyber Sécurité OFCS. Disponible à l'adresse : <https://www.ncsc.admin.ch/ncsc/fr/home/strategie/cyberstrategie-ncs.html> [consulté le 5 mars 2025].

DDPS, Département fédéral de la défense, de la protection de la population et des sports, 2024a. Rançongiciels - Office fédéral de la cybersécurité. [en ligne]. 19 novembre 2024. Disponible à l'adresse : <https://www.ncsc.admin.ch/ncsc/fr/home/cyberbedrohungen/ransomware.html> [consulté le 6 mars 2025].

DDPS, Département fédéral de la défense, de la protection de la population et des sports, 2024b. *Mesures contre les attaques par rançongiciel* [en ligne]. Berne : Office Fédéral de la Cyber Sécurité OFCS. Disponible à l'adresse : <https://www.ncsc.admin.ch/ncsc/fr/home/strategie/berichte-und-studien.html> [consulté le 5 mars 2025].

DELLAC, Sébastien, 2024. Démystifier la cyber-sécurité pour mieux la rationaliser : proposition d'une grille de lecture. *Defenso* [en ligne]. 1 février 2024. Disponible à l'adresse : <https://defenso.fr/articles/grille-de-lecture-cybersecurite-part-3> [consulté le 2 juillet 2025].

DÉON, Sébastien, 2023. *Cyber-résilience en entreprise : enjeux, référentiels et bonnes pratiques*. 2e édition. St Herblain : Editions ENI. Epsilon. ISBN 978-2-409-04144-0.

DIS, 2025. *Directive générale du Plan de sauvetage (PdS) des collections & des fonds de la Division de l'information scientifique (DIS)*. . DIS - Université de Genève. 2ème édition. Interne

DONALDSON, Devan Ray et BELL, Laura, 2018. Security, Archivists, and Digital Collections. *Journal of Archival Organization*. Vol. 15, no 1-2, pp. 1-19. DOI 10.1080/15332748.2019.1609311.

DPC, 2024a. *Digital Preservation Coalition Rapid Assessment Model*. Digital Preservation Coalition. version 3-March 2024. DOI 10.7207/dpcram24-03.

DPC, 2024b. *The Bit List 2024 The Global List of Endangered Digital Species* [en ligne]. Digital Preservation Coalition. Fourth Edition Interim Review. Disponible à l'adresse : <https://www.dpconline.org/doclink/bitlist2024/eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9eyJzdWIiOiJiaXRsaXN0MjAyNCIsImIhdCI6MTczMDczMzk2MywiZXhwIjoxNzMwODIwMzYzfQ.8oIwyDanRm6uNFDF6iq5ZONdeR8yreKOQKe9iGgwyA> [consulté le 1 avril 2025].

DULAUNOY, Alexandre et FAFNER, 2022.  RansomLook . *Ransomlook.io* [en ligne]. 2025 2022. Disponible à l'adresse : <https://www.ransomlook.io/> [consulté le 5 mai 2025].

ENISA, 2024. *ENISA threat landscape 2024* [en ligne]. LU : European Union Agency for Cybersecurity. Disponible à l'adresse : <https://data.europa.eu/doi/10.2824/0710888> [consulté le 4 juin 2025]. July 2023 to June 2024.

ESRI, 2024. *Sécurité des SI · saison 2 : La cybersécurité au cœur de la stratégie de l'ESRI*. . Paris : Etat de l'Enseignement Supérieur de la Recherche et de l'Innovation.

EVE, Martin Paul, 2024. Digital Scholarly Journals Are Poorly Preserved: A Study of 7 Million Articles. *Journal of Librarianship and Scholarly Communication*. Vol. 12, no 1. DOI 10.31274/jlsc.16288.

EX LIBRIS, 2024. Frankfurt Data Center Migration (DC06) FAQ. *Ex Libris Knowledge Center* [en ligne]. 11 décembre 2024. Disponible à l'adresse : [https://knowledge.exlibrisgroup.com/Cross-Product/Knowledge\\_Articles/Frankfurt\\_Data\\_Center\\_Migration\\_\(DC06\)\\_FAQ](https://knowledge.exlibrisgroup.com/Cross-Product/Knowledge_Articles/Frankfurt_Data_Center_Migration_(DC06)_FAQ) [consulté le 17 juillet 2025].

EXTANCE, Andy, 2016. How DNA could store all the world's data. *Nature*. Vol. 537, no 7618, pp. 22-24. DOI 10.1038/537022a.

FERRACCI, Elsa, 2016. *Archivage pérenne en bibliothèque universitaire : bilan et perspectives*. . Enssib.

GENEVOIS, Sylvain, 2025. Cartographie numérique: Quand l'Administration Trump fait disparaître des données sur les sites gouvernementaux. *Cartographie numérique* [en ligne]. 2025. Disponible à l'adresse : <https://cartonumerique.blogspot.com/2025/02/quand-ladministration-trump-fait.html> [consulté le 7 mars 2025].

GHERNAOUTI, Solange, 2022. *Cybersécurité - 7e éd.. Analyser les risques, mettre en oeuvre les solutions* [en ligne]. Dunod. Dunod. Disponible à l'adresse : <https://shs.cairn.info/cybersecurite--9782100841493> [consulté le 7 mars 2025].

GHERNAOUTI, Solange et AGHROUM, Christian, 2012. Cyber-résilience, risques et dépendances : pour une nouvelle approche de la cyber-sécurité. *Sécurité et stratégie*. Vol. 11, no 4, pp. 74-83. DOI 10.3917/sestr.011.0074.

GOUVERNEMENT DU QUÉBEC, 2016. *Guide de catégorisation de l'information*. Version 2.1. Québec (Québec) : Sous-secrétariat du dirigeant principal de l'information : Direction des communications du Secrétariat du Conseil du trésor. ISBN 978-2-550-71120-9.

GROVE, Jack, 2024. How the British Library cyberattack disrupted research. *Times Higher Education (THE)* [en ligne]. 21 novembre 2024. Disponible à l'adresse : <https://www.timeshighereducation.com/depth/how-british-library-cyberattack-disrupted-research> [consulté le 7 mars 2025].

GUIREL, Marielle, 2020. Guide décisionnel et vade-mecum pour la mise à disposition d'un dépôt de données de recherche ouvertes en Suisse. [en ligne]. Disponible à l'adresse : <https://sonar.ch/global/documents/315086> [consulté le 6 août 2024].

HARMSEN, J.H, 2024. Audit and certification – The Data Seal of Approval | DCC. *Digital Curation Centre* [en ligne]. 2024. Disponible à l'adresse : <https://www.dcc.ac.uk/resources/curation-reference-manual/chapters-production/audit-and-certification> [consulté le 2 juillet 2025].

HASTINGS, Robin M., 2017. *Planning Cloud-Based Disaster Recovery for Digital Assets: The Innovative Librarian's Guide*. ABC-CLIO, LLC. ISBN 978-1-4408-4238-2. Open Library ID: OL34612500M

HEDLEY, Esme, 2025. How to protect research data. *Nature*. pp. d41586-025-01034-x.  
DOI 10.1038/d41586-025-01034-x.

HEINTZ, Lauryn, 2024. Calgary Public Library says member, employee data safe after breach. *CityNews Calgary* [en ligne]. 29 octobre 2024. Disponible à l'adresse : <https://calgary.citynews.ca/2024/10/29/calgary-public-library-cybersecurity-breach/> [consulté le 2 novembre 2024].

HOUGHTON, Frank, WINTERBURN, Michael et OAKLEY, Ken, 2025. The 2023 Rhysida Ransomware Attack on the British Library Prioritisation, Expertise, and Funding Issues About the Authors. *Information Technology and Libraries*. Vol. 44. DOI 10.5860/ital.v44i1.17112.

HUG BUFFO, Anna, 2020. La gouvernance de l'information dans les hôpitaux universitaires suisses. [en ligne]. Disponible à l'adresse : <https://sonar.rero.ch/global/documents/315120> [consulté le 6 mars 2025].

HUGHES, Henry, 2024. Universities should test their cyber defences - before someone else does. *Jisc* [en ligne]. 6 mars 2024. Disponible à l'adresse : <https://beta.jisc.ac.uk/blog/universities-should-test-their-cyber-defences-before-someone-else-does> [consulté le 6 mars 2025].

IFLA, 2020. Awareness, Planning, Resilience: Thoughts on Libraries' Cyber Defense in 2020 | Library Policy and Advocacy Blog. [en ligne]. 27 mars 2020. Disponible à l'adresse : <https://blogs.ifla.org/lpa/2020/03/27/awareness-planning-resilience-thoughts-on-libraries-cyber-defense-in-2020/> [consulté le 5 mars 2025].

IFLA, 2022. IFLA Information Technology Section + IFLA Strategy: Statement on Cybersecurity. *IFLA* [en ligne]. février 2022. Disponible à l'adresse : <https://www.ifla.org/news/ifla-information-technology-section-ifla-strategy-cybersecurity-artificial-intelligence-future/> [consulté le 5 mars 2025].

IMPERVA, Thales Group, 2025. *Bad Bot 2025* [en ligne]. 12 ème rapport annuel d'Imperva. Disponible à l'adresse : [https://www.thalesgroup.com/fr/monde/defence-and-security/press\\_release/rapport-bad-bot-2025-dimperva-lia-favorise-lexplosion-des](https://www.thalesgroup.com/fr/monde/defence-and-security/press_release/rapport-bad-bot-2025-dimperva-lia-favorise-lexplosion-des) [consulté le 25 juin 2025].

INTERCERT. *Chiffrement ou Effacement en cours Qualification* [en ligne]. Disponible à l'adresse : <https://www.intercert-france.fr/fichesreflexes-remediation/files/FicheReflexe-Chiffrement-Qualification.pdf> [consulté le 13 mars 2025]. Cc-By-Nc-Sa

INTERCERT, 2024a. *Compromission système Qualification*. Disponible à l'adresse : <https://www.intercert-france.fr/fichesreflexes-remediation/files/FicheReflexe-Chiffrement-Qualification.pdf> [consulté le 13 mars 2025]. Cc-By-Nc-Sa.

INTERCERT, 2024b. *Chiffrement ou Effacement en cours Endiguement* [en ligne]. Disponible à l'adresse : <https://www.intercert-france.fr/fichesreflexes-remediation/files/FicheReflexe-Chiffrement-Endiguement.pdf> [consulté le 13 mars 2025].

IŞIK, Öykü, 2024. British Library Cyber Attack - 10 Lessons - Cyber Security - I by IMD. [en ligne]. 30 septembre 2024. Disponible à l'adresse : <https://www.imd.org/ibyimd/technology/full-transparency-10-lessons-from-the-cyber-attack-on-the-british-library/> [consulté le 26 mars 2025].

ISO, 2018. *ISO 27005:2018 - Information technology — Security techniques — Information security risk management*. ORGANISATION INTERNATIONALE DE NORMALISATION. Genève. ORGANISATION INTERNATIONALE DE NORMALISATION .

ISO, 2019. *ISO 22301:2019 - Security and resilience - Business continuity management systems. Requirements.* ORGANISATION INTERNATIONALE DE NORMALISATION. BSI British Standards. ORGANISATION INTERNATIONALE DE NORMALISATION . DOI 10.3403/30382483.

ISO, 2020. *SN EN ISO/IEC 27000:2020 - Information technology - Security techniques Information security management systems Overview and vocabulary* [en ligne]. ORGANISATION INTERNATIONALE DE NORMALISATION. Genève. ORGANISATION INTERNATIONALE DE NORMALISATION . Disponible à l'adresse : <https://viewer.snv.ch/product/271098?filePath=100820171.pdf&isPrint=1> [consulté le 15 mars 2025].

ISO, 2022a. *ISO 27001:2022 - Information security, cybersecurity and privacy protection Information security management systems — Requirements.* . ORGANISATION INTERNATIONALE DE NORMALISATION. Genève. ORGANISATION INTERNATIONALE DE NORMALISATION .

ISO, 2022b. *ISO 27002:2022 - Information security, cybersecurity and privacy protection Information security controls.* . ORGANISATION INTERNATIONALE DE NORMALISATION. Genève. ORGANISATION INTERNATIONALE DE NORMALISATION .

ISO, 2025a. *ISO 14721:2025 - Reference Model for an Open Archival Information System (OAIS).* . ORGANISATION INTERNATIONALE DE NORMALISATION. Genève. ORGANISATION INTERNATIONALE DE NORMALISATION .

ISO, 2025b. *ISO 16363 - Audit and Certification of Trustworthy Digital Repositories.* . ORGANISATION INTERNATIONALE DE NORMALISATION. Genève. ORGANISATION INTERNATIONALE DE NORMALISATION .

JABRAYILZADE, Elgun et al., 2022. Bus factor in practice. In : *Proceedings of the 44th International Conference on Software Engineering: Software Engineering in Practice*, pp. 97-106. New York, NY, USA : Association for Computing Machinery. 17 octobre 2022. ICSE-SEIP '22. ISBN 978-1-4503-9226-6. DOI 10.1145/3510457.3513082.

JAUN, René et SCHENNER, Maximilian, 2023. Cyberattaque contre l'Université de Zurich: des accès aux serveurs vendus sur le darkweb (update). *ICT Journal* [en ligne], 6 février 2023. Disponible à l'adresse : <https://www.ictjournal.ch/news/2023-02-06/cyberattaque-contre-luniversite-de-zurich-des-acces-aux-serveurs-vendus-sur-le> [consulté le 8 mars 2025].

JIANG, Yuning et al., 2025. *MITRE ATT&CK Applications in Cybersecurity and The Way Forward.* arXiv:2502.10825. arXiv. arXiv:2502.10825. DOI 10.48550/arXiv.2502.10825. arXiv:2502.10825 [cs]

JOELVING, Frederik, 2024. Swiss medical association accused of forcing publishing subsidiary into insolvency. *Retraction Watch* [en ligne]. 5 septembre 2024. Disponible à l'adresse : <https://retractionwatch.com/2024/09/05/swiss-medical-association-accused-of-forcing-publishing-subsidiary-into-insolvency/> [consulté le 13 mai 2025].

JOHNSON, Christopher S. et al., 2016. *Guide to Cyber Threat Information Sharing.* National Institute of Standards and Technology. NIST SP 800-150. DOI 10.6028/NIST.SP.800-150.

KAHN, Miriam, 2004. *Protecting your library's digital sources: the essential guide to planning and preservation.* Chicago : American Library Association. ISBN 978-0-8389-0873-0.

KAHN, Miriam, 2012. *Disaster response and planning for libraries.* 3rd ed. Chicago : American Library Association. ISBN 978-0-8389-1151-8.

KASTELLEC, Mike, 2012. Practical Limits to the Scope of Digital Preservation. [en ligne]. Vol. 31, no 2, pp. 63-71. Disponible à l'adresse : <https://www.proquest.com/docview/1022030090/abstract/B3C31D3BC6A04D51PQ/1> [consulté le 17 mars 2025].

KAUFMAN, Matthew, 2025. The 'Wayback Machine' is preserving the websites Trump's White House took down | CNN Business. CNN [en ligne]. 18 février 2025. Disponible à l'adresse : <https://www.cnn.com/2025/02/18/tech/internet-archives-deleted-websites-wayback-machine/index.html> [consulté le 7 mars 2025].

KEDERLHUÉ, Gaétan et IRIARTE, Pablo, 2023. *From digital sobriety to blackout - how to archive essential health knowledge and offer offline access in our libraries.* . Présentation . EAHIL Conference 2023, Trondheim, NORVÈGE. 15 juin 2023.

KHADGI, Nischal, 2023. Découverte du ransomware Rhysida et de ses activités. *Logpoint* [en ligne]. 27 décembre 2023. Disponible à l'adresse : <https://www.logpoint.com/fr/emerging-threat-fr/dcouverte-ransomware-rhysida-et-activites/> [consulté le 5 mars 2025].

KNIGHT, Sam, 2023. The Disturbing Impact of the Cyberattack at the British Library. *The New Yorker* [en ligne]. Disponible à l'adresse : <https://www.newyorker.com/news/letter-from-the-uk/the-disturbing-impact-of-the-cyberattack-at-the-british-library> [consulté le 31 mars 2025].

KONDRUSS, Bert, 2025. Cyberattacks on universities. *KonBriefing Research* [en ligne]. 2025. Disponible à l'adresse : <https://konbriefing.com/en-topics/cyber-attacks-universities.html> [consulté le 10 juillet 2025].

KONSTANTELOS, Leo et YAN, Emma, 2023. PRIORITIZING STORAGE MEDIA FOR DIGITAL ARCHIVING AND PRESERVATION [presentation]. *iPRES 2023* [en ligne]. Disponible à l'adresse : <https://hdl.handle.net/2142/121668> [consulté le 6 août 2024].

KORBEN, 2025. Développeurs, attention à l'empoisonnement de vos IA ! *Le site de Korben* [en ligne]. 22 avril 2025. Disponible à l'adresse : <https://korben.info/backdoors-invisibles-github-copilot-cursor-mcp-hack.html> [consulté le 30 juin 2025].

KUCHARAVY, Andrei et al. (éd.), 2024. *Large Language Models in Cybersecurity: Threats, Exposure and Mitigation.* Cham : Springer Nature Switzerland. ISBN 978-3-031-54826-0.

KWON, Diana, 2025. Web-scraping AI bots cause disruption for scientific databases and journals. *Nature*. pp. d41586-025-01661-4. DOI 10.1038/d41586-025-01661-4.

LAAKSO, Mikael, MATTHIAS, Lisa et JAHN, Najko, 2021. Open is not forever: a study of vanished open access journals. *Journal of the Association for Information Science and Technology*. Vol. 72, no 9, pp. 1099-1112. DOI 10.1002/ASI.24460. arXiv:2008.11933 [cs]

LALLIE, Harjinder Singh et al., 2023. *Understanding Cyber Threats Against the Universities, Colleges, and Schools.* arXiv:2307.07755. arXiv. arXiv:2307.07755. DOI 10.48550/arXiv.2307.07755. arXiv:2307.07755 [cs]

LANEY, Douglas B., 2018. *Infonomics: how to monetize, manage, and measure information as an asset for competitive advantage.* First edition. New York, NY, USA : Bibliomotion, Inc. ISBN 978-1-138-09038-5.

LANKES, David R, 2025. Don't Look Away – R. David Lankes. <https://davidlankes.org/> [en ligne]. 26 mars 2025. Disponible à l'adresse : <https://davidlankes.org/dont-look-away/> [consulté le 5 juillet 2025].

LANTZ, Mark, 2024. CERN Tape Archive Workshop : CTA 2024. *Indico* [en ligne]. 2024. Disponible à l'adresse : <https://indico.cern.ch/event/1353243/contributions/5846917/> [consulté le 12 août 2024].

LEMONNIER, Patrice, 2025. *Lancement d'une initiative européenne inédite : l'Indice de Résilience Numérique (IRN), outil de pilotage au service de la souveraineté technologique* [en ligne]. Disponible à l'adresse : <https://assets.rte-france.com/prod/public/2025-07/2025-07-04-cp-indice-resilience-numerique.pdf> [consulté le 5 juillet 2025].

LEPLAT, Jacques, 2007. Resilience engineering. Concepts and precepts de Hollnagel, Woods et Leveson. *Perspectives interdisciplinaires sur le travail et la santé*. No 9-2. DOI 10.4000/pistes.3770.

LÉVY, Pierre, 1997. *Cyberculture: Rapport au Conseil de l'Europe*. Paris : Odile Jacob. ISBN 978-2-7381-7380-5.

LINDSTRÖM, Emilie et SPIRKINA, Sasha, 2024. *British Library Unplugged : A Media Analysis of Institutional Pressures during a Cyber Attack on a National Library* [en ligne]. Disponible à l'adresse : <https://urn.kb.se/resolve?urn=urn:nbn:se:hb:diva-32074> [consulté le 5 mars 2025].

LIU, Guoying et ZOU, Qing, 2023. Cybersecurity and Libraries: Global trends, challenges, and best practices. [en ligne]. Disponible à l'adresse : <https://2023.ifla.org/poster-sessions/> [consulté le 5 mars 2025].

MALLAPATY, Smriti, 2025a. 'Omg, did PubMed go dark?' Blackout stokes fears about database's future. *Nature*. DOI 10.1038/d41586-025-00674-3. Bandiera\_abtest: aCg\_type: Newspublisher: Nature Publishing GroupSubject\_term: Databases, Peer review, Publishing

MALLAPATY, Smriti, 2025b. Scientists globally are racing to save vital health databases taken down amid Trump chaos. *Nature*. Vol. 638, no 8051, pp. 589-590. DOI 10.1038/d41586-025-00374-y. Bandiera\_abtest: aCg\_type: Newspublisher: Nature Publishing GroupSubject\_term: Databases, Politics, Public health

MARTEL, Marie D., 2025. Ce qui se passe au sud de la frontière : des attaques répétées contre les bibliothèques, la mémoire collective et la recherche. *bibliomancienne* [en ligne]. 24 mars 2025. Disponible à l'adresse : <https://bibliomancienne.ca/2025/03/24/ce-qui-se-passe-au-sud-de-la-frontiere-des-attaques-repetees-contre-les-bibliotheques-la-memoire-collective-et-la-recherche/> [consulté le 5 juillet 2025].

MARTINEZ, Claire, 2023. Ukraine : l'Unesco dénonce onze bibliothèques endommagées. *Archimag* [en ligne]. Disponible à l'adresse : <https://www.archimag.com/bibliotheque-edition/2023/01/26/ukraine-unesco-denonce-onze-bibliotheques-endommagees> [consulté le 6 mai 2025].

MESGUICH, Véronique et BERMÈS, Emmanuelle, 2023. *Les bibliothèques face au monde des données*. Villeurbanne : Presses de l'ENSSIB. Papiers. ISBN 978-2-37546-147-1.

MESSARRA, Luca, FREELAND, Chris et ZISKINA, Juliya, 2024. *Vanishing Culture: A Report on Our Fragile Cultural Record* [en ligne]. United States of America : Internet Archive. Disponible à l'adresse : <https://blog.archive.org/wp-content/uploads/2024/10/Vanishing-Culture-2024.pdf> [consulté le 2 novembre 2024].

METRAT, Lore et OURY, Clément, 2017. *L'archivage des revues scientifiques électroniques pour les bibliothèques universitaires en France*. Villeurbanne : Enssib.

MINET, Pascaline, 2025. « C'est une réelle menace pour les progrès de la science »: à la suite des coupes américaines, Les chercheurs suisses craignent pour leurs données - Le Temps.

[en ligne]. 29 juin 2025. Disponible à l'adresse : <https://www.letemps.ch/sciences/c-est-une-reelle-menace-pour-les-progres-de-la-science-a-la-suite-des-coupes-americaines-les-chercheurs-suisses-craignent-pour-leurs-donnees> [consulté le 30 juin 2025].

MITRE ATT&CK®, 2025 [en ligne]. Disponible à l'adresse : <https://attack.mitre.org/> [consulté le 1 avril 2025].

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2024. *The NIST Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD : National Institute of Standards and Technology. NIST CSWP 29. DOI 10.6028/NIST.CSWP.29.

NGWUM, Nnatubemugo et al., 2020. A Model for Security Evaluation of Digital Libraries: A Case Study on a Cybersecurity Curriculum Library. *Journal of The Colloquium for Information Systems Security Education* [en ligne]. Vol. 7, no 1, pp. 12-12. Disponible à l'adresse : <https://cisse.info/journal/index.php/cisse/article/view/115> [consulté le 6 mars 2025].

NIST, 2024. *The NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology - U.S. Department of Commerce. NIST CSWP 29. DOI 10.6028/NIST.CSWP.29.

Nomoreransom, 2021 *The No More Ransom Project* [en ligne]. Disponible à l'adresse : <https://www.nomoreransom.org/> [consulté le 15 juin 2025].

NRC, 1991. *Computers at risk : safe computing in the information age* [en ligne]. Washington, D.C. : National Academy Press. National Research Council (U.S.). Computer Science and Telecommunications Board. System Security Study Committee. ISBN 978-0-309-04388-5. Disponible à l'adresse : <http://archive.org/details/computersatrisks00nati> [consulté le 20 juillet 2025].

OES, 2025. *L'impact de l'ouverture des publications scientifiques sur les habitudes de lecture du lectorat scientifique en France* [en ligne]. Observatoire de l'édition Scientifique. Ministère chargé de l'enseignement supérieur et de la recherche et du Ministère de la Culture . Disponible à l'adresse : <https://www.enseignementsup-recherche.gouv.fr/sites/default/files/2025-07/l-impact-de-l-ouverture-des-publications-scientifiques-sur-les-habitudes-de-lecture-du-lectorat-scientifique-en-france-37514.pdf> [consulté le 12 juillet 2025].

OLGIATI, Mirta, 2005. *Politique de la mémoire nationale: la sélection du patrimoine documentaire en Suisse* [en ligne]. Institut de hautes études en administration publique. Suisse. Cahier de l'IDHEAP, 224 /2005. Disponible à l'adresse : [https://serval.unil.ch/resource/serval:BIB\\_38227.P001/REF.pdf](https://serval.unil.ch/resource/serval:BIB_38227.P001/REF.pdf) [consulté le 30 juin 2025]. Chaire Politiques publiques et durabilité

OURY, Antoine, 2024. Attaque de la British Library: 600 Go partis sur le dark web. *ActualLitté.com* [en ligne]. 26 mars 2024. Disponible à l'adresse : <https://actualitte.com/article/116407/bibliotheque/attaque-de-la-british-library-600-go-partis-sur-le-dark-web> [consulté le 6 mars 2025].

OWASP, 2021. OWASP Top Ten. *The Open Worldwide Application Security Project Foundation* [en ligne]. 2021. Disponible à l'adresse : <https://owasp.org/www-project-top-ten/> [consulté le 3 juillet 2025].

PASTEUR, Ceris-Institut, 2024. Une étude alerte sur le risque de perdre l'accès à des millions de publications en ligne. *Open science : évolutions, enjeux et pratiques* [en ligne]. 18 mars 2024. Disponible à l'adresse : <https://openscience.pasteur.fr/2024/03/18/une-etude-alerte-sur-le-risque-de-perdre-lacces-a-des-millions-de-publications-en-ligne/> [consulté le 3 avril 2025].

PEET, Lisa, 2025. Harvard Law School Library Innovation Lab Preserves Federal Data. *Library Journal* [en ligne]. 6 mars 2025. Disponible à l'adresse : <https://www.libraryjournal.com/story/harvard-law-school-library-innovation-lab-preserves-federal-data> [consulté le 18 juin 2025].

PENNOCK, Maureen, 2013. *Web-Archiving*. Digital Preservation Coalition. DOI 10.7207/twr13-01.

PEREZ, Kate, 2024. Seattle Public Library still reeling from May cyberattack. *The Seattle Times* [en ligne]. 6 août 2024. Disponible à l'adresse : <https://www.seattletimes.com/seattle-news/seattle-public-library-still-reeling-from-may-cyberattack/> [consulté le 2 novembre 2024].

PERROD, Maxime, 2023. L'utilisation des réseaux neuronaux pour la détection d'intrusions dans les réseaux informatiques. [en ligne]. Disponible à l'adresse : <https://sonar.rero.ch/global/documents/328186> [consulté le 6 mars 2025].

POLCHOW, Michelle, 2021. Exploring Perpetual Access. *The Serials Librarian*. Vol. 80, no 1-4, pp. 107-113. DOI 10.1080/0361526X.2021.1883206.

POLCHOW, Michelle et NASIG, 2020. *Exploring Perpetual Access* [en ligne]. 8 juin 2020. Disponible à l'adresse : <https://www.youtube.com/watch?v=jdiLxKK2Ols> [consulté le 19 mai 2025].

POUPARD, Guillaume, 2018. Sécurité numérique – sommes-nous condamnés à une lutte inégale entre le glaive et le bouclier ? | Collège de France [en ligne]. Paris, 17 juillet 2018. Disponible à l'adresse : <https://www.college-de-france.fr/fr/agenda/seminaire/ou-va-informatique/securite-numerique-sommes-nous-condamnes-une-lutte-inegale-entre-le-glaive-et-le-bouclier> [consulté le 13 mars 2025].

RIVERO, Athena Chapekis, Samuel Bestvater, Emma Remy and Gonzalo, 2024. When Online Content Disappears. *Pew Research Center* [en ligne]. 17 mai 2024. Disponible à l'adresse : <https://www.pewresearch.org/data-labs/2024/05/17/when-online-content-disappears/> [consulté le 24 mars 2025].

ROSENTHAL, David S. H. et al., 2005. Requirements for Digital Preservation Systems: A Bottom-Up Approach. *D-Lib Magazine*. Vol. 11, no 11. DOI 10.1045/november2005-rosenthal.

ROSS, Ron et al., 2021. *Developing cyber-resilient systems : a systems security engineering approach*. Gaithersburg, MD : National Institute of Standards and Technology (U.S.). NIST SP 800-160v2r1. DOI 10.6028/NIST.SP.800-160v2r1.

RS 231.1 - Loi fédérale du 9 octobre 1992 sur le droit d'..., *Fedlex* [en ligne]. Disponible à l'adresse : [https://www.fedlex.admin.ch/eli/cc/1993/1798\\_1798\\_1798/fr](https://www.fedlex.admin.ch/eli/cc/1993/1798_1798_1798/fr) [consulté le 20 mars 2025].

SAFE-PLN, 2024. About SAFE PLN. *SAFE PLN* [en ligne]. 2024. Disponible à l'adresse : <http://localhost:4000/about/> [consulté le 7 mars 2025].

SCHWARTZ, Natalie, 2023. Over half of higher ed institutions hit by ransomware paid to get data back, survey finds. *Higher Ed Dive* [en ligne]. 4 août 2023. Disponible à l'adresse : <https://www.highereddive.com/news/higher-education-ransomware-paid-ransom-college/689929/> [consulté le 7 mars 2025].

SERRIES, Guillaume, 2025. Pourquoi le Danemark vire Microsoft Office et Windows pour LibreOffice et Linux. *ZDNET* [en ligne]. 12 juin 2025. Disponible à l'adresse : <https://www.zdnet.fr/actualites/pourquoi-le-danemark-vire-microsoft-office-et-windows-pour-libreoffice-et-linux-477075.htm> [consulté le 16 juin 2025].

SEYDTAGHIA, Anouch, 2022. EXCLUSIF – Le piratage de l’Université de Neuchâtel est tentaculaire - Le Temps. [en ligne]. 9 mars 2022. Disponible à l’adresse : <https://www.letemps.ch/cyber/exclusif-piratage-luniversite-neuchatel-tentaculaire> [consulté le 7 avril 2025].

SMITHERS, Matt, 2025a. CERN: Library Science Talk Presentation Recording. CLOCKSS [en ligne]. 19 juin 2025. Disponible à l’adresse : <https://clockss.org/cern-library-science-talk-presentation/> [consulté le 30 juin 2025].

SMITHERS, Matt, 2025b. Understanding CLOCKSS: A Commitment to Preserving Content Safely and Securely. CLOCKSS [en ligne]. 8 mai 2025. Disponible à l’adresse : <https://clockss.org/understanding-clockss-security/> [consulté le 10 mai 2025].

SNIA, 2025. *SNIA-Data-Protection-Best-Practice* [en ligne]. SNIA, Storage Networking Industry Association. v2. Disponible à l’adresse : <https://www.snia.org/sites/default/files/2025-03/SNIA-Data-Protection-Best-Practice-2025-01-27-v2.pdf> [consulté le 18 avril 2025].

SOKOLOV, Daniel AJ, 2022. Unibibliothek Leipzig meldet Sicherheitslücke. *Heise, Security-Lage* [en ligne]. 27 avril 2022. Disponible à l’adresse : <https://www.heise.de/meinung/Unibibliothek-Leipzig-meldet-Sicherheitsluecke-7066305.html> [consulté le 5 mars 2025].

SOLOMON, Howard, 2025. Prolongé temporairement, le financement du programme CVE reste incertain. *Le Monde Informatique* [en ligne]. 18 avril 2025. Disponible à l’adresse : <https://www.lemondeinformatique.fr/actualites/lire-prolonge-temporairement-le-financement-du-programme-cve-reste-incertain-96642.html> [consulté le 21 juin 2025].

SOPHOS, 2023. *State of ransomware in education* [en ligne]. Disponible à l’adresse : <https://assets.sophos.com/X24WTUEQ/at/j74v496cfwh4qsvgqhs4pmw/sophos-state-of-ransomware-education-2023-wp.pdf> [consulté le 7 mai 2025].

STOKES, Alice M., 2022. Disruption of Library Services Due to Hospital Cyberattack: A Case Study. *Medical Reference Services Quarterly*. Vol. 41, no 2, pp. 204-212. DOI 10.1080/02763869.2022.2054198.

STRECKER, Dorothea et al., 2023. *Disappearing repositories -- taking an infrastructure perspective on the long-term availability of research data*. arXiv:2310.06712. arXiv. arXiv:2310.06712. DOI 10.48550/arXiv.2310.06712. arXiv:2310.06712 [cs]

SWISSINFO.CH, 2025. IA et droit d'auteur: un juge donne raison à Meta. *SWI swissinfo.ch* [en ligne]. 26 juin 2025. Disponible à l’adresse : <https://www.swissinfo.ch/fre/ia-et-droit-d-auteur-un-juge-donne-raison-a-meta/89589292> [consulté le 5 juillet 2025].

TAVERNIER, Willa, WESTERVELT, Ted et CARLSON, Amy J., 2021. Where Do We Keep That? The New Keepers Registry and the Digital Content in Your Collection. *The Serials Librarian*. Vol. 80, no 1-4, pp. 155-160. DOI 10.1080/0361526X.2021.1865020.

THE MITRE CORPORATION, 2025. CVE Record: CVE-2020-1472. *CVE* [en ligne]. 2025. Disponible à l’adresse : <https://www.cve.org/CVERecord?id=CVE-2020-1472> [consulté le 10 mai 2025].

TISTOUNET, Claire et FISCHER, Philipp, 2025. La nouvelle obligation d’annonce des cyberattaques. *swissprivacy.law* [en ligne]. 30 mars 2025. Disponible à l’adresse : <https://swissprivacy.law/345/> [consulté le 18 juin 2025].

UNIGE, 2017. *Guide de sécurisation des applications* [en ligne]. Genève : DISTIC - Université de Genève. SECU-071223-1551-24. Disponible à l’adresse :

<https://cybersecurite.unige.ch/application/files/4917/0204/1976/SECU-071223-1551-24.pdf> [consulté le 17 juin 2025].

UNIGE, 2018. Cybersécurité et Sécurité du numérique - Sécurité de l'information. *Université de Genève* [en ligne]. 23 octobre 2018. Disponible à l'adresse : <https://cybersecurite.unige.ch/> [consulté le 11 juillet 2025]. Last Modified: 2025-05-12T10:21:51Z

UNIGE, 2021a. *Standards minimaux - Sécurité de l'information / Cybersécurité - UNIGE* [en ligne]. DISTIC - Université de Genève. Disponible à l'adresse : <https://cybersecurite.unige.ch/pour-les-it-people/regles-minimales-de-securite> [consulté le 6 mars 2025]. Last Modified: 2021-12-20T07:20:48Z

UNIGE, 2021b. *Gestion de la continuité d'activité - Sécurité de l'information / Cybersécurité - UNIGE* [en ligne]. DISTIC - Université de Genève. Disponible à l'adresse : <https://cybersecurite.unige.ch/politiques/gestion-de-la-continuite-dactivite> [consulté le 6 mars 2025]. Last Modified: 2021-12-20T07:20:49Z

UNIGE, 2021c. Les services numériques par niveaux de sensibilité - Sécurité de l'information / Cybersécurité - UNIGE. [en ligne]. 17 août 2021. Disponible à l'adresse : <https://cybersecurite.unige.ch/je-gere-des-donnees/liste-des-services-numeriques-par-niveau-de-sensibilite> [consulté le 21 juillet 2025]. Last Modified: 2023-03-01T13:50:53Z

UNIGE, 2024. *Library's Strategy 2024-2027 - Bibliothèque - UNIGE* [en ligne]. DIS - Université de Genève. Disponible à l'adresse : <https://www.unige.ch/biblio/en/news/archive/2023-2/strategie-2024-2027/> [consulté le 26 février 2025]. Last Modified: 2025-01-23T10:11:43Z

UNIGE, 2025a. *Expenditure Per Reporting Code - Document Interne*. . Genève : Université de Genève.

UNIGE, 2025b. *Stratégie numérique 2025-2028* [en ligne]. Université de Genève. Disponible à l'adresse : <https://www.unige.ch/universite/politique-generale/strategie-numerique#toc4> [consulté le 18 juin 2025]. Last Modified: 2025-06-04T10:07:25Z

VILLE DE GENÈVE, 2025. *Proposition du Conseil administratif* [en ligne]. PR-1687 (182e). Disponible à l'adresse : <https://www.geneve.ch/autorites-administration/conseil-municipal/documents/PR-1687-182> [consulté le 20 mai 2025].

WAGNER, Steven, 2020. Les superordinateurs de l'EPFZ et du CSCS victimes d'une cyberattaque. [en ligne]. 18 mai 2020. Disponible à l'adresse : <https://www.ictjournal.ch/news/2020-05-18/les-superordinateurs-de-lepfz-et-du-cscs-victimes-dune-cyberattaque> [consulté le 8 avril 2025].

WANG, Shaopeng et al., 2024. Data Storage Using DNA. *Advanced Materials*. Vol. 36, no 6, p. 2307499. DOI 10.1002/adma.202307499.

WELCH, Don, 2019. Creating a Cybersecurity Strategy for Higher Education. .

WIENER, Norbert, 2019. *Cybernetics ; or, Control and communication in the animal and the machine*. [Second edition, 2019 reissue]. Cambridge : MIT Press. ISBN 978-0-262-35591-9.

WINTER, Susie, 2022. Guest Post – Cybersecurity and Academic Libraries: Findings from a Recent Survey. *The Scholarly Kitchen* [en ligne]. 21 mars 2022. Disponible à l'adresse : <https://scholarlykitchen.sspnet.org/2022/03/21/guest-post-cybersecurity-and-academic-libraries-findings-from-a-recent-survey/> [consulté le 5 mars 2025].

WRIGHT, Eric, 2024. *SNIA - Data Protection in the Ransomware Era: Strategies and Insights* [en ligne]. 23 octobre 2024. Disponible à l'adresse : <https://www.youtube.com/watch?v=VBZI8-Kg-yE> [consulté le 28 juin 2025].

WU, Daniel, 2024. The world's largest internet archive is under siege — and fighting back. *Washington Post* [en ligne]. 18 octobre 2024. Disponible à l'adresse : <https://www.washingtonpost.com/nation/2024/10/18/internet-archive-hack-wayback/> [consulté le 2 novembre 2024].

ZIMBA, Olena et al., 2025. Open infrastructures in conflict zones: a case study of DOAJ and Ukrainian journals. *Insights the UKSG journal*. Vol. 38. DOI 10.1629/uksg.689.

ЧИТОМО, 2022. The bombing of Kharkiv damaged one of Europe's largest libraries. [en ligne]. 14 mars 2022. Disponible à l'adresse : <https://chytomo.com/en/the-bombing-of-kharkiv-damaged-one-of-europe-s-largest-libraries/> [consulté le 7 mars 2025].

# Annexe 1 : Registre des normes applicables

Portée	Norme / Méthode	Date - Dernière version	Pays	Organisme	Type	Caractéristiques	Avantages	Possible application en bibliothèque	Note
Analyse et Gestion des Risques	<b>E BIOS RM</b> Expression des Besoins et Identification des Objectifs de Sécurité	2018 - version Risk Manager	France	ANSSI	Approche analytique	Identification précise des risques Évaluation contextuelle Traitement des vulnérabilités	5 phases méthodologiques Analyse approfondie des menaces Adaptation au contexte local	Évaluation des risques spécifiques liés à l'accès et à la sécurité des collections numériques. Identification précise des menaces (cyberattaques, indisponibilité des ressources documentaires). Analyse de vulnérabilités spécifiques (serveurs, accès à distance, gestion des identifiants).	Retenue
	<b>OCTAVE</b> Operationally Critical Threat, Asset, and Vulnerability Evaluation	2007 - version Allegro	International	Carnegie Mellon University	Approche opérationnelle	Évaluation comprehensive des risques Approche centrée sur l'organisation	Flexible et adaptable Forte implication organisationnelle	Identification et priorisation des actifs critiques documentaires et numériques (bases de données, systèmes intégrés de gestion de bibliothèque). Évaluation opérationnelle des risques liés aux infrastructures informatiques des bibliothèques. Clarification des dépendances critiques avec d'autres services institutionnels (informatiques, administratifs).	
	<b>ITIL</b> Information Technology Infrastructure Library	2019 - version ITIL 4	UK	AXELOS	Approche opérationnelle et processus	Bonnes pratiques de gestion IT, Gestion standardisée des incidents, problèmes et changements	Amélioration de la qualité des services informatiques Optimisation des ressources et réduction des risques opérationnels Approche centrée sur la continuité et la disponibilité des services	Gestion standardisée des incidents informatiques (pannes d'accès aux ressources documentaires numériques, interruptions réseau). Organisation efficace du support technique en bibliothèque. Amélioration de la disponibilité des services (accès aux ressources électroniques, catalogues en ligne, systèmes de prêt automatisés).	
	<b>FAIR</b> Factor Analysis of Information Risk	2014 - FAIR institute	International	FAIR Institute	Approche économique	Analyse économique des risques Méthode quantitative de gestion des risques Mesure financière de l'impact	Approche basée sur des données quantifiables Permet une prise de décision économique	Pertinent si l'approche économique des risques est requise (calcul des coûts liés à une indisponibilité prolongée des ressources électroniques critiques). Aide à déterminer finançièrement quelles ressources méritent une protection renforcée en raison de leur valeur stratégique (abonnements coûteux, bases de données spécialisées). Moins directement applicable pour l'évaluation quotidienne opérationnelle en bibliothèque, mais pertinent au niveau décisionnel et budgétaire.	
	<b>NIST 2.0</b> Cybersecurity Framework	2024 - NIST CSF 2.0	US International	NIST	Approche opérationnelle et gouvernance	Intégration de la fonction de gouvernance Gestion des risques à l'échelle de l'entreprise Guides de démarrage rapide pour différentes audiences Adaptation aux technologies émergentes (IA, quantique)	Structuré autour de six fonctions clés Renforcement de l'alignement avec la gestion des risques d'entreprise Guides de démarrage rapide pour différentes audiences Facilite la communication entre les équipes techniques et la direction	Offre un cadre structuré et adaptable pour la gestion des risques de cybersécurité, aligne la sécurité sur la gouvernance institutionnelle, et fournit des outils pratiques pour la mise en œuvre et la gestion des incidents. Inclusion de scénarios de gestion des incidents et de récupération après incident. Accent sur la responsabilité des dirigeants dans la gouvernance des risques cyber	Retenue
	<b>Cyber Assessment Framework</b> NCSC	2020 - V3.2	UK	National Cyber Security Centre (NCSC)	Approche orientée vers les services essentiels	Identification, analyse, gestion, et mitigation des risques pour les services essentiels	Cadre reconnu pour la conformité réglementaire, adaptable aux différents secteurs y compris critiques	Pas totalement pertinente en raison de sa complexité et des ressources qu'il requiert, ainsi que du niveau de risque qu'il vise à gérer. D'autres pourraient être plus adaptés pour les bibliothèques, offrant une meilleure flexibilité et une adaptation aux risques plus typiques de ces environnements.	
	<b>ISO 27005</b> Gestion des risques en sécurité de l'information	2022 - ISO/IEC 27005:2022	International	ISO/IEC	Approche exhaustive et analytique	Identification et analyse complète des risques et menaces Adaptable à tout type d'organisation	Norme internationale reconnue Approche structurée et exhaustive des risques Compatibilité avec d'autres normes ISO Standardisation de l'évaluation des risques	Analyse détaillée des risques liés aux collections numériques, à l'accès distant aux ressources documentaires. Identification complète des scénarios possibles de menaces documentaires et informatiques (cyberattaques, pertes de données, pannes de serveurs). Élaboration concrète d'un plan d'action pour sécuriser les actifs numériques des bibliothèques (bases documentaires, archives électroniques).	Retenue
Plan de continuité et reprise	<b>ISO 22301</b> Management de la continuité d'activité	2019	International	ISO	Norme de gestion de la continuité	Système de management de la continuité d'activité (BCMS), approche basée sur les risques	Standard international reconnu, intégration avec ISO 27001, amélioration continue	Applicable pour structurer un plan de continuité d'activité global, y compris en cas de cyberattaque	Retenue
	<b>ISO 27031</b> Continuité des TIC et DRP	2011	International	ISO	Norme sur la continuité des opérations IT	Approche spécifique aux technologies de l'information et à la résilience des infrastructures IT	Cadre détaillé pour la continuité IT, recommandations adaptées aux infrastructures numériques	Sécurisation des infrastructures IT, remplace ISO 24762	Retenue
	<b>NIST 800-34</b> Contingency planning guide	2010 (Rev. 1)	États-Unis	NIST	Guide pour la reprise des opérations IT	Guide détaillé pour la planification et la mise en œuvre des DRP	Orienté vers les systèmes informatiques et leur reprise après incident	Planification de la reprise des systèmes d'information en cas d'incident	Retenue
	<b>AFNOR SPEC 2208</b> Continuité d'activité	2020	France	AFNOR	Spécification française pour la résilience IT	Directives spécifiques pour la résilience et la continuité des systèmes IT français, reconstruction du SI et la gestion de la continuité des activités en cas de cyberattaque paralyssante	Aligné sur les besoins des organisations françaises, adapté aux environnements réglementés	Approprié pour les petites structures ayant des ressources limitées pour structurer un plan de continuité IT	
	<b>ANSSI - Guide d'élaboration d'un plan de continuité informatique</b>	2021	France	ANSSI	Guide opérationnel pour les SI critiques	Méthodologie pour l'élaboration d'un plan de continuité informatique en France	Spécifique aux besoins des infrastructures françaises, approche détaillée et pragmatique	Développement de procédures adaptées pour la continuité	Retenue

Management et contrôles de la sécurité du système d'information	<b>ISO/IEC 27001</b>	2022	International	ISO et IEC	Norme de management Certification	Management de la sécurité de l'information Amélioration continue	Système de management de la sécurité Approche processus Certification possible	Gestion globale de la sécurité informationnelle Protection des données de recherche Conformité et amélioration continue	Retenue
	<b>ISO/IEC 27002</b>	2022	International	ISO et IEC	Code de bonnes pratiques en sécurité de l'information Guide opérationnel	Catalogue de bonnes pratiques et contrôles détaillés Approche opérationnelle complémentaire à l'ISO 27001	Précision et complémentarité avec la norme ISO 27001 Application concrète des contrôles de sécurité Facilité d'implémentation des bonnes pratiques	Application pratique des contrôles de sécurité définis dans ISO 27001 Renforcement concret de la sécurité documentaire et numérique Bonnes pratiques spécifiques à l'accès, l'utilisation, et la gestion des ressources informationnelles	
	<b>NIST 800-53</b>	2020 - Revision 5	États-Unis	NIST National Institute of Standards	Référentiel de contrôles de sécurité IT Approche complète basée sur les contrôles	Catalogue détaillé des contrôles de sécurité Adaptation à divers contextes technologiques	Large éventail de contrôles classifiés par familles Approche adaptable à la sensibilité des données Développé initialement pour les systèmes fédéraux américains	Protection détaillée des actifs numériques et systèmes documentaires Contrôle précis de la sécurité des systèmes d'information bibliothéconomiques Mise en conformité des systèmes documentaires selon des standards nationaux ou académiques	Retenue
	<b>COBIT</b> Control Objectives for Information and Related Technologies	2018	États-Unis	ISACA	Référentiel de gouvernance Alignement stratégique	Gouvernance IT Alignement business	5 domaines de gouvernance Focus sur la valeur métier Gouvernance des systèmes d'information	Alignement des systèmes informatiques avec les objectifs académiques Gouvernance des ressources numériques Gestion de la valeur des systèmes d'information	
Préservation à long terme	<b>OAIS (ISO 14721)</b>	2025 - Revision 3	International	ISO	Modèle conceptuel	Cadre de référence pour la préservation numérique à long terme ; définit les rôles, responsabilités et processus	Reconnaissance internationale, souplesse d'application	Structure d'un dépôt numérique, définition des processus internes	Retenue
	<b>ISO 16363</b>	2025	International	ISO	Norme d'audit	Critères d'évaluation pour les dépôts numériques de confiance	Certification reconnue, amélioration continue des pratiques	Auto-évaluation des pratiques, certification d'un dépôt	Retenue
	<b>METS (Metadata Encoding and Transmission Standard)</b>	2018 (1.12.1)	États-Unis	Library of Congress	Standard de métadonnées	Encodage de métadonnées structurelles, administratives et descriptives associées à des objets numériques	Souplesse et interopérabilité, largement utilisé en bibliothèque	Structuration des métadonnées pour faciliter la gestion des objets numériques	
	<b>PREMIS (Preservation Metadata Implementation Strategies)</b>	2018 (version 3.0)	International	Library of Congress / PREMIS Editorial	Standard de métadonnées de préservation	Gestion des métadonnées nécessaires à la préservation sur le long terme	Très utilisé, complémentaire à METS, reconnu par la communauté archivistique	Gestion détaillée des informations de préservation, intégration aux systèmes existants	
	<b>PDF/A (ISO 19005)</b>	2020 (PDF/A-4)	International	ISO	Format de fichier normalisé	Version normalisée du PDF adaptée à l'archivage à long terme	Pérennité assurée des contenus, interopérabilité forte	Archivage des publications académiques, rapports, thèses et autres documents numériques	
	<b>Bagit</b>	2018 (RFC 8493)	États-Unis	Library of Congress / IETF	Standard technique	Méthode de stockage et transfert de contenus numériques avec leurs métadonnées	Facilité d'utilisation, validation intégrée, usage répandu	Transfert sécurisé et traçable des données entre institutions	Retenue
	<b>ISO/TR 18492</b>	2005	International	ISO	Rapport technique	Recommandations générales pour le stockage pérenne des documents électroniques	Orientations pratiques, facile d'accès	Définition de politiques de stockage et de gestion documentaire en bibliothèque	
	<b>ISO 15489</b>	2016	International	ISO	Norme de gestion documentaire	Fournit des orientations générales sur la gestion des documents et des archives	Applicable à divers contextes, complémentaire à la préservation numérique	Intégration de bonnes pratiques documentaires dans les politiques de gestion documentaire des bibliothèques	
	<b>AFNOR NF Z42-013</b>	2009	France	AFNOR	Norme	Composantes d'un système informatique pour l'archivage électronique – Conception et exploitation, Norme structurante pour la mise en œuvre d'un SAE sécurisé, souvent citée en contexte légal ou réglementaire.	Exigences relatives à la conception, à la mise en œuvre et à l'exploitation d'un SAE garantissant l'intégrité, la pérennité et la traçabilité des documents électroniques. Archivage interne sécurisé, preuve de conservation, conformité à la	Conception d'un SAE interne en bibliothèque pour les documents engageants (administratifs, contractuels, scientifiques).	
	<b>AFNOR NF Z42-026</b>	2020	France	AFNOR	Norme	Archivage électronique – Spécifications pour l'archivage numérique fidèle de documents. Définit les exigences pour garantir un archivage numérique fidèle, notamment dans des environnements en cloud.	Complémentaire à la NF Z42-013, spécifie les conditions de conservation fidèle dans des services cloud ou externalisés.	Adaptée aux bibliothèques utilisant des prestataires d'archivage numérique ou des services en ligne pour les documents sensibles.	

## Annexe 2 : Questionnaire d'entretien semi-dirigée

Grille d'entretien semi-dirigé - Résilience numérique et sauvegarde des actifs informationnels en bibliothèques académiques	
Introduction et cadre de l'entretien	
Bonjour et merci d'avoir accepté cet entretien. Je mène actuellement un projet de recherche dans le cadre de mon Bachelor, portant sur la résilience numérique et la sécurisation des ressources électroniques dans les bibliothèques académiques.	
De la préparation aux cyberattaques à la continuité des services - Stratégie de résilience numérique et sauvegarde des actifs informationnels en bibliothèques académiques	
Présentation du projet :	
L'objectif est de comprendre les stratégies de cybersécurité/les menaces mais surtout la continuité des services dans les bibliothèques académiques. Contexte des cyberattaques croissantes, dépendance aux infrastructures numériques, risques de coupures de services. Souvent considérée comme une solution pour la sauvegarde des documents physique le numérique ne dispose pas de plans d'urgences et nombreux sont, aujourd'hui les exemples qui nous font craindre pour la pérennité de ces ressources.	
Modalités de l'entretien :	
*Acceptez-vous être cité(e) dans mon étude avec votre nom et votre fonction ? Si oui, votre expertise pourra être référencée dans l'analyse des résultats.	
Format semi-dirigé : possibilité pour l'interviewé d'apporter des compléments libres.	
Durée estimée : 45 à 90 minutes.	
Consentement pour l'enregistrement et anonymisation des données.	
1. Préparation aux cyberattaques en bibliothèque académique	
1.1 Identification des vulnérabilités et menaces	
Selon vous, quelles sont les principales menaces (informatiques) qui pèsent sur les ressources numériques ?	
Avez-vous déjà été confronté à des exemples (cyberattaques) ? Si oui, pouvez-vous décrire la nature et l'impact de l'événement ?	
Quelles sont les autres vulnérabilités dans le cas des bibliothèques académiques (techniques, humaines, organisationnelles) ?	
1.2 Classification et protection des actifs informationnels	
Quels sont les documents et ressources numériques que l'on pourrait considérer comme critiques ? (BDD, Articles scientifiques, Références, ORD Depository)	
En quoi leur inaccessibilité pourrait constituer un risque ?	
Quels critères utilisez-vous pour prioriser la protection de certains actifs informationnels (valeur scientifique, rareté, usage, etc.) ?	
Comment sont gérés l'accès et la protection des bases de données et archives numériques de votre institution ?	
1.3 Plans d'urgence et gouvernance	
Existe-t-il un plan de gestion faisant référence des cyberattaques dans votre institution ?	
Avez-vous déjà entendu parler de plans d'urgences pour la sauvegarde des ressources numériques ? Si oui, dans quelle institutions ?	
Quels seraient selon vous les étapes ou les points importants pour la réalisation de ce type de politiques ?	
Quels sont les rôles et responsabilités des bibliothécaires, informaticiens et décideurs dans la gestion de ces incidents ?	
2. Continuité des services et accès aux collections numériques	
2.1 Maintien des services en cas d'incident	
Comment pourrais-t-on garantir la continuité des services et des ressources d'une bibliothèque en cas de cyberattaque ou de panne majeure ?	
Pensez-vous à des solutions techniques capables de préserver durablement et de maintenir un accès ?	
Quels services et accès considérez-vous comme prioritaires à maintenir en cas de crise ?	
2.2 Solutions d'accès en mode dégradé	
On peut ici questionner l'immuabilité d'internet...	
...Et on peu imaginer la mise en place en place des systèmes alternatifs, de consultation hors ligne ou des copies locales des catalogues et bases de données ? Quelles seraient les limites et les défis de ces solutions en pratique ?	
Selon vous peut-on imaginer une solution avec l'IA ? Ou au contraire cette technologie constitue un risque ?	
2.3 Relations avec les éditeurs et prestataires	
Avez-vous des accords spécifiques avec vos fournisseurs pour garantir l'accès aux ressources en cas d'incident majeur ?	
Quels sont les principaux obstacles qui peuvent freiner la résilience numérique des bibliothèques ?	
Que voyez-vous comme risques, sur le fait que la bibliothèque soit à la croisée de l'Université, de la faculté de médecine et des HUG ?	
3. Stratégie de résilience des systèmes d'information (IT only)	
3.1 Gouvernance et gestion des risques	
Existe-t-il un cadre de gestion des risques en cybersécurité dans votre institution (ISO 27001, NIST, ANSSI) ? Si oui lesquels ?	
Comment les risques sont-ils évalués et priorisés ?	
Disposez-vous d'un registre des actifs critiques et d'une cartographie des services ?	
3.2 Sécurisation techniques et infrastructures	
Quelles technologies ou solutions de résilience avez-vous mises en place (redondance des serveurs, chiffrement avancé, multi-cloud) ?	
Avez-vous mis en place des protocoles de surveillance et de détection des menaces ?	
Comment intégrez-vous les retours d'expérience des incidents passés dans l'amélioration continue ?	
Avez-vous adopté des solutions comme LOCKSS, CLOCKSS, Portico pour l'archivage à long terme ?	
Effectuez-vous des audits ou tests de cybersécurité (pentesting, simulation de cyberattaques) ?	
Avez-vous organisé des campagnes de sensibilisation aux menaces comme le phishing ou les ransomwares ?	
Disposez-vous de guides de bonnes pratiques accessibles aux usagers et au personnel ?	
4. Sauvegarde, archivage et préservation des ressources numériques	
4.1 Stratégies de sauvegarde et stockage	
Quelles solutions de sauvegarde utilisez-vous pour les ressources numériques et les ressources numérisées, à quelle fréquence sont réalisées les sauvegardes et comment sont-elles testées ?	
J'ai lu à plusieurs reprises dans ma recherche documentaire "Avoir des sauvegardes ne suffit pas..." que'est ce que cela vous évoque ?	
4.2 Gestion de l'obsolescence et des formats numériques	
Comment anticipiez-vous l'obsolescence des formats numériques ?	
Disposez-vous d'un plan de migration des formats pour assurer la pérennité des ressources numériques ?	
Quels formats et standards (d'archivage) et de métadonnées utilisez-vous (OAI, PREMIS, METS) ?	
5. Conclusion et perspectives	
Quelles améliorations pourraient être apportées aux stratégies actuelles de résilience numérique ?	
Y a-t-il des initiatives internationales ou interinstitutionnelles que vous recommanderiez d'explorer ?	
Auriez-vous des contacts ou des ressources supplémentaires à me conseiller pour approfondir cette recherche ?	
Finalisation de l'entretien	
Remerciements et rappel des prochaines étapes de la recherche. Proposition de partager les résultats de l'étude si l'interviewé est intéressé. Vérification de toute demande de clarification ou de compléments d'informations de la part de l'interviewé.	

## **Annexe 3 : Liste des personnes interrogées**

Lors de chaque entretien, une demande de consentement pour l'enregistrement vocal a été formulée. Ils ont été utilisés uniquement à des fins de traitements et de prise de note et détruit à l'issu du traitement. Une transcription unitaire a été réalisée et une synthèse de ces transcriptions rédigée dans les annexes 6 et 7.

### **Entretiens externes à l'UNIGE :**

- Alexandre Flament, Adjoint Scientifique, Infrastructure labo, HES-SO.
- Albert Rossier, Responsable du MAS cybersécurité, Spécialiste SSI, HES-SO.
- Patrick Ruch, Group leader, enseignant-chercheur en bio-informatique, HES-SO.
- Yannick Grandcolas, Responsable des collections numériques, Chef de produit SPAR Gallica, Co directeur de l'Open Preservation Foundation, BNF.
- Expert en cybersécurité, le participant n'a pas souhaité que son nom apparaisse.
- Nelly Cauliez, Francois Petit, Conseillère en conservation du patrimoine, Conseiller de direction chargé sécurité DSI, Ville de Genève.
- Geraldine Goeffroy, Spécialiste en ingénierie documentaire, Data Librarian, Smartbibl.IA Solutions.
- Raphael Rey, Senior Data and Systems Specialist, Swiss Library Service Platform.

### **Entretiens internes à l'UNIGE :**

- Pierre L'Hostis, Responsable de la Sécurité des Systèmes d'Information, DiSTIC.
- Frederic Ducret, Responsable infrastructure et cloud computing, DiSTIC.
- Hugues Cazeaux, Responsable Pôle e-research et DLCM, DiSTIC.
- Floriane Muller, Bibliothécaire spécialiste, appui à la recherche scientifique et à la publication en *Open Access*, DIS.
- Kieran Pavel, Elise Point, Coordination secteur Espaces, Logistique, Sécurité et Équipement, ELSE, responsables du groupe Plan de sauvetage des collections, DIS.
- Olivia Peila, Chief Data Office, Rectorat.

### **Meetings :**

- Records and Archives of International Organizations in Geneva (RAIOG).
- WAME, World Association of Medical Editors.
  - Alicia Wise - Executive Director CLOCKSS Archive
  - Mariya Maistrovskaya - Senior Publishing, Support Specialist -Public KnowledgeProject
  - Snowden Becker - LOCKSS Program, Community Manager Stanford University
- Library Science Talk - Preserving Knowledge in a Shifting World: The Role of Libraries in Geopolitical Uncertainty (10 juin 2025) · Indico CERN.

## Annexe 4 : Grille de traitement des résultats

Nom de l'institution	
Date - Durée	26.05.2025 –10h – 75 min
Contact	
Poste	Spécialiste en ingénierie documentaire
Type d'entretien	Entretien semi-structuré suivant une série de questions prédéfinies en thématiques, l'interviewé peut compléter et approfondir librement certains aspects – A distance.
Objectifs	Comprendre la démarche gestion des risques, comprendre les enjeux actuels, apprécier les menaces, les mesures, les réalités, recueillir une expérience professionnelle et un avis sur les perspectives et le périmètre du projet
Sujet	Notes
Identification et compréhension des menaces et des vulnérabilités	
Protection et classification des ressources numériques critiques	
Plans d'urgence, gouvernance et répartition des responsabilités	
Continuité opérationnelle et solutions alternatives d'accès	
Sauvegarde, archivage numérique et gestion de l'obsolescence	
Recommandations et perspectives évoquées	

## Annexe 5 : Grille de synthèse de lecture

Rubrique	Contenu							
Référence bibliographique	citation complète							
Type de document	article scientifique, rapport, livre, ...							
Auteur(s), personnes nommées et profils								
Source d'information	éditeur, la revue, l'organisme de publication							
Thèmes identifiés	Cybersécurité et menaces	Gestion des risques et gouvernance	Résilience des systèmes d'information	Sauvegarde, stockage, archivage des données	Bibliothèques académiques et ressources numériques	Protection et accès aux collections numériques	Tests et validation des stratégies de cybersécurité	Adaptation aux crises et contextes extrêmes
Résumé	objet de l'article, objectifs et conclusions principales.							
Principaux concepts et théories	Listez les notions abordées (ex. : résilience numérique, plan de continuité d'activité, cybersécurité, etc.).							
Méthodologie	Décrivez le type d'étude (étude de cas, enquête, analyse de données, etc.), les outils utilisés et l'échantillon étudié.							
Résultats et conclusions	Résumez les principaux résultats et les recommandations des auteurs.							
Liens avec le sujet de recherche	Comment cette source contribue-t-elle à la compréhension de votre sujet ? Apporte-t-elle une nouvelle perspective ou une confirmation de théories existantes ? En quoi se distingue-t-elle des autres sources analysées ?							
Points forts et limites	Identifiez les forces de l'étude (approche originale, données solides) et ses limites (échantillon restreint, cadre spécifique).							
Citations clés	Notez ici les passages pertinents (avec numéro de page).  définition, argument clé, contre-argument, exemple pertinent							

## Annexe 6 : Synthèse des entretiens sur les pratiques externes

Dans le cadre de cette recherche, une analyse comparative a été menée sur un panel d'institutions Suisses et internationales, issues de l'enseignement supérieur, de la recherche et de bibliothèques patrimoniales. L'objectif était de mettre en perspective les enjeux de sécurité et de préservation numérique à travers différents contextes organisationnels. L'analyse s'est appuyée sur les six axes critiques déterminés dans l'exploration du sujet. Ce document est la synthèse des entretiens des différents participants externes.

### Identification et compréhension des menaces et vulnérabilités

Les institutions interrogées reconnaissent diverses menaces critiques, avec une prédominance des cyberattaques telles que les *ransomwares*. Les environnements ouverts, typiques des instituts de recherche et des institutions académiques, exacerbent les risques liés à ces menaces. Plusieurs acteurs pointent également l'importance des attaques par déni de service (DDoS), particulièrement lors d'événements politiques ou institutionnels sensibles. Les risques liés à l'utilisation de l'intelligence artificielle à des fins malveillantes et à l'espionnage ciblant les données sensibles des secteurs de la recherche sont également mis en avant ainsi que l'importance de leur trafic à des fins de moissonnage sur les sites mettant à disposition des données ouvertes. Certaines institutions insistent sur une définition élargie de la cybersécurité intégrant la confidentialité, l'intégrité, la disponibilité et la traçabilité des données, ainsi que sur l'importance de stratégies de prévention proactive face aux interruptions non anticipées, pouvant conduire à des pertes irréversibles de savoir (épistémicide).

### Protection et classification des ressources numériques critiques

En matière de protection, des infrastructures solides telles que le stockage RAID, la redondance réseau et les sauvegardes immuables sont fréquentes. Cependant, des lacunes persistent concernant la haute disponibilité automatique et les mécanismes analytiques permettant d'anticiper précisément les besoins documentaires. Certaines institutions, comme la Bibliothèque Nationale de France (BNF), adoptent des standards (modèle OAIS) et des stratégies mixtes (disques pour accès rapide, bandes pour sécurité à long terme), mais rencontrent des limites budgétaires. La classification hiérarchisée des ressources selon leur criticité et leur usage est considérée comme essentielle, tout comme l'emploi des statistiques d'usage comme indicateurs indirects de cette criticité. Le recours à des outils tels que LOCKSS, Portico et CLOCKSS est recommandé, notamment pour les contenus éditoriaux critiques, avec une distinction claire entre sauvegarde et préservation à long terme.

### Gouvernance, plans d'urgence et répartition des responsabilités

Les approches de gouvernance varient fortement. Plusieurs institutions ne disposent pas d'un Plan de Continuité des Activités (PCA) ou de Plan de Reprise après Sinistre (PRA) formalisés, explicable par la taille et la supposé non-sensibilité des données produites ou gérées. À l'inverse, d'autres mettent en place des stratégies fondées sur le *framework* NIST CSF et la norme ISO 27001. Les acteurs soulignent l'importance des clauses contractuelles de service avec les prestataires externes. Certains, comme la Ville de Genève, démontrent une approche structurée avec une gouvernance sectorielle, intégrant des groupes dédiés à la gestion des

risques, à la continuité et à la préservation de l'information, tout en alignant leurs pratiques sur des normes reconnues.

#### Continuité opérationnelle et solutions alternatives d'accès

Plusieurs institutions ont mis en place des solutions opérationnelles pour garantir un accès continu ou alternatif aux ressources numériques. L'existence de miroirs (notamment de PubMed), la sauvegarde régulière sur bandes magnétiques et les procédures testées de restauration sont des pratiques courantes. Toutefois, l'accès reste souvent lent et complexe en cas de crise, et la sécurité doit être équilibrée avec la rapidité d'accès. Une cartographie des processus métiers et de leurs dépendances numériques est recommandée, tout comme la mise en place de solutions institutionnelles ou à défaut open source robustes. Certaines organisations arguent la nécessité d'une régulation proactive des accès destinés à l'entraînement des IA aux ressources culturelles et patrimoniales (moissonnées massivement), et l'importance d'intégrer la préservation dans les scénarios de crise et les exercices de formation des personnels.

#### Sauvegarde, archivage numérique et gestion de l'obsolescence

Les institutions adoptent majoritairement le principe de sauvegarde 3-2-1, avec, dans les meilleurs des cas, une utilisation de bandes magnétiques (LTO) et de solutions robustes comme LOCKSS. La migration régulière vers des technologies récentes doivent être effectuée et provisionnée dans les budgets. Des exemples précis soulèvent les risques concrets liés à l'obsolescence technologique, comme la perte de données à cause d'un support devenu illisible. Plusieurs institutions recommandent d'intégrer les enjeux de sécurité et de préservation dès la phase initiale de conception des projets informatiques (« Secure by design »).

## Annexe 7 : Synthèse des entretiens sur les pratiques internes

La synthèse des entretiens internes s'appuie sur une réflexion, menée à plusieurs niveaux. Il est rapidement apparu que la notion de « ressources électroniques » ne revêt pas la même signification selon l'interlocuteur : un responsable de la sécurité informatique, un développeur ou un gestionnaire de collection n'en auront pas la même perception ni les mêmes priorités. Cette approche permet de mieux comprendre les points de friction et de coordination nécessaires pour une gestion cohérente des ressources électroniques. Ce document est la synthèse des entretiens des différents participants internes à l'UNIGE.

### Identification et compréhension des menaces et des vulnérabilités

Les acteurs identifient des menaces internes importantes, notamment les erreurs humaines, les mauvaises manipulations, et les mauvaises configurations résultant souvent de l'inattention de la négligence ou parfois du multitâche. Certaines menaces proviennent d'un usage inapproprié des outils, sans intention malveillante. Des failles de développement peuvent être mal anticipées, et les dépendances critiques (stockage, annuaire) souvent sous-évaluées. Les outils internes disposent de certains contrôles mais leur gestion repose sur peu de personnes. Les menaces externes incluent principalement les *ransomwares*. Les attaques DDoS ou injections SQL sont présents mais bien gérés par les équipes sécurité. Les attaques par phishing, le partage illégal d'identifiants, ainsi que les risques émergents liés à l'intelligence artificielle sont également évoqués. L'absence de stratégie pour identifier et préserver les ressources numériques prioritaires augmente les risques de perte de données et un manque d'une cartographie des services numériques centralisée représente une lacune. Les vulnérabilités au niveau organisationnelle paraissent augmentées par la dispersion des responsabilités, la segmentation des services et des facultés. Des risques spécifiques sont également associés au *shadow IT* qui sort de la vision et donc de la surveillance des services de sécurité, et se trouvent accentués parfois par contrainte budgétaire de réalisation.

Un audit a pointé explicitement un manque critique de formalisation, une faible intégration entre classification et archivage, ainsi que des lacunes en Records Management. Il n'y a pas actuellement de réelle politique d'archivage numérique. Une politique de gestion des données institutionnelles est en cours de validation (2025) et un programme visant à développer le *data-stewardship* est en cours de réalisation, montrant la saisie de ce thème par l'institution.

### Protection et classification des ressources numériques critiques

La protection des services numériques essentielles (SNE) est diversement abordée. La politique de sécurité adopte une stratégie de fermeture systématique des accès aux ressources critiques, « tout ce qui n'est pas autorisé explicitement est interdit », notion de whitelisting et blacklisting. Les standards minimaux de la directive sur la continuité d'activité doivent être respectés. Il s'agit également de classer distinctement les données en fonction de la classification institutionnelle selon une grille de criticité basée sur la sensibilité des données (faible, moyenne, élevée, très élevée) et le niveau de risque associé. Cette classification détermine les exigences de protection en tenant compte des obligations légales, contractuelles et de l'impact potentiel sur la mission ou la réputation de l'institution. Le recours à *Microsoft Purview* est cité comme un outil pour contrôler les accès, mais des incertitudes persistent autour des fonctionnalités de sécurité et de sauvegarde des solutions comme *M365* et

*SharePoint*. Un backup des messageries priorisé en fonctions des profils d'usagers importants est envisagé via *SWITCHcloud*.

Pour les actifs sous la responsabilité de la DIS une proposition de création d'un registre, classés selon divers critères est mise en avant. Il est recommandé d'assurer un état des lieux pour pouvoir envisager une priorisation cohérente avec les moyens disponibles, ainsi qu'une meilleure hiérarchisation des ressources de gestion internes critiques en conformité avec les standards de l'institution. Concernant les collections électroniques de la Bibliothèque, l'important est d'identifier les ressources d'abord pour avoir une vision précise de la collection et être en mesure de constituer une évaluation puis pour déterminer les plus critiques. Ce travail permettra d'établir une *core collection* au niveau de la bibliothèque et de proposer une équivalence numérique du plan de sauvetage des collections physiques. L'absence d'équivalence numérique complète à l'archivage papier sécurisé reste à établir. Une annotation ou indexation spécifique des documents de cette *core collection* devrait être également étudiée.

#### Plans d'urgence, gouvernance et répartition des responsabilités

Une gouvernance naissante existe au sein du Data Office, intégrant des rôles clés liés au secrétariat général (CDO, DPO, RSSI). Cependant, cette gouvernance demeure partiellement fragmentée, et pour l'heure non reconnue en tant que véritable division. Sa légitimité reste à établir notamment en raison de la distinction entre les deux entités : administratives et académiques qui limite la maîtrise complète des processus internes, met en opposition le rectorat et les facultés, avec des objectifs distincts et peut contredire la liberté académique.

Depuis 2024 un projet de refonte du PRA est en cours par la DiSTIC appuyé par un cabinet de conseil externe. Le projet et les phases de tests sont lancées de manière unitaire dès que les responsables de chaque SNE se seront prononcés sur leurs exigences de criticité. Il est à noter que le manque de retours métiers pourtant essentiels pour la vision exhaustive et complète de la structure du SI constitue une contrainte. Cette synergie doit être renforcée pour assurer une vision et une couverture globale des systèmes de l'université. Bien que des analyses d'impact opérationnel (BIA) soient réalisées, leur application effective aux ressources numériques métiers reste inégale et manque clairement de mise à jour. Ceci révèle la segmentation des responsabilités entre service et le besoin en compétences transversales entre la DiSTIC et la DIS notamment. Des efforts sont à produire pour permettre une synergie plus fluide entre les services. Une meilleure intégration des spécificités métiers dans les plans de reprise après sinistre (PRA) est vivement recommandée.

Aucune démarche formalisée globale n'a été établie à ce jour concernant les collections électroniques de la Bibliothèque, bien que des réflexions soient initiées sur la clarification des relations contractuelles avec les éditeurs. Sur les ressources physiques en bibliothèque le plan de sauvetage des collections est établi et mis à jour mais n'est pas initié à partir d'une démarche normalisée d'étude de risques. Un désalignement financier et stratégique entre la DiSTIC et les services métiers/facultés est signalé comme une faiblesse. De même, les responsabilités et compétences dispersées peuvent entraîner des difficultés lors des situations de crise.

#### Continuité opérationnelle et solutions alternatives d'accès

Des infrastructures techniques robustes existent avec des réseaux redondants et une définition des objectifs de temps de récupération pour les dépendances techniques (RTO/RPO). La mise en œuvre de l'authentification multi-facteurs (MFA) et la formalisation des accords contractuels avec les prestataires renforcent cette résilience. Toutefois, des enjeux d'accès aux ressources électroniques nécessitent l'utilisation de solutions externe telles qu'OpenAthens pour faciliter les accès en dehors du réseau et réduire l'utilisation du VPN et de la bande passante. Deux datacenters sur deux sites différents en mode actif-actif avec sauvegarde de type snapshots garantissent une reprise rapide des données, mais l'absence de tests réguliers d'arrêt complet peut constituer une vulnérabilité. De plus la synchronisation de ces deux serveurs rend ces sauvegardes de reprise rapide potentiellement vulnérables aux *ransomwares*.

Certaines solutions d'accès dégradé existent (exports locaux des catalogues), mais restent marginales et insuffisamment formalisées dans le cadre d'un processus défini. Une approche pragmatique utilisant l'extraction régulière des métadonnées via OAI-PMH, indexées dans une base de données *elasticsearch* pour un accès minimal interne, est proposée comme point de départ d'une solution.

#### Sauvegarde, archivage numérique et gestion de l'obsolescence

La sauvegarde repose principalement sur un système de fichier sur NAS, un SAN est également utilisé et un système de sauvegardes immuables est possible. L'infrastructure permet également du stockage de données froides sur des bandes magnétiques. Une politique stricte de gestion de l'obsolescence est nécessaire. L'absence d'adhésion à des plateformes mutualisées comme CLOCKSS est reconnue comme problématique, bien que l'utilisation de SafePLN pour les thèses produites par l'UNIGE et des exports réguliers vers e-Diss de la Bibliothèque Nationale constitue une bonne pratique de couverture et de sécurisation. L'Archive Ouverte est le dépôt historique des publications produites par l'institution et représente un des services indispensables de la DIS. Reposant sur une version de *fedora* elle ne remplit cependant pas les critères d'un dépôt d'archivage à long terme. Le recours à SafePLN (technologie LOCKSS) pour l'archivage immuable (*dark archive*) est valorisé, même si des contraintes légales et techniques en limitent l'usage. Ces solutions présentent toutefois des contraintes techniques et juridiques, notamment en termes de droits d'auteur, de formats acceptés et de quotas de stockage (4 To répliqués sur le réseau de 12 partenaires).

Coté données de recherche, un service de pérennisation des données conforme au modèle OAIS est fonctionnel et maintenu, il a obtenu la certification Core Trust Seal en 2024. Yareta via la technologie DLCM peut être envisagée pour plusieurs développements à venir. Centella un projet d'archivage électronique pour le service des archives administratives et patrimoniales est mentionné. Un projet de numérisation a débuté en ce sens aux services des Archives mais aucune solution de stockage pérenne permet de sécuriser ce matériel. L'utilisation des produits Microsoft est très répandu et SharePoint tend à devenir la norme pour le stockage des fichiers mais reste peu utilisé par tous les services. L'archivage numérique constitue un enjeu critique encore insuffisamment adressé au sein des institutions universitaires. Si des pratiques techniques telles que l'utilisation de snapshots, ou de stockages off-line sont utilisés comme protections contre les *ransomwares*, elles demeurent non intégrées dans une politique globale d'archivage. Le recours à des sauvegardes synchronisées augmente quant à lui les

risques de propagation en cas d'attaque, soulignant la nécessité d'une stratégie de suppression rigoureuse et de désinstallation systématique des systèmes obsolètes.

Des réflexions sont en cours sur les plateformes cibles et un projet de migration depuis Fedora vers DLCM est envisagé pour améliorer l'interopérabilité avec les outils de préservation. Par ailleurs, bien que des sauvegardes techniques soient assurées par des entités telles que la DiSTIC, les modalités de restauration restent floues pour une partie des acteurs, et le risque d'initiatives autonomes au niveau des facultés compromet l'unité de la démarche.

Si l'idée de migrer l'Archive Ouverte vers une solution comme DLCM peut sembler pertinente, notamment dans une logique de préservation à long terme, elle doit être nuancée. Les caractéristiques évolutives des données (fichiers et métadonnées fréquemment modifiés) s'opposent à une intégration directe dans un système conçu pour l'archivage pérenne. Cette réticence marque la distinction entre diffusion et conservation, et pousse à envisager les publications davantage comme des données dynamiques à intégrer dans des cycles de gestion, plutôt que comme des reproductions numériques de documents papier figés. En parallèle, Fedora reste utilisé pour d'autres applications institutionnelles (photothèque, archives administratives), ce qui complexifie tout projet de transition sans coordination plus large.

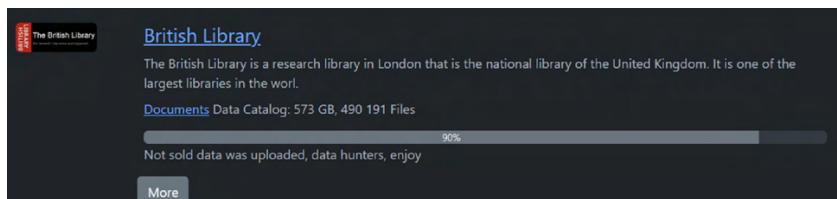
Enfin un déficit en compétences de Records Management est reconnu. Ce contexte nécessite une gouvernance documentaire unifiée, qui prenne en compte l'ensemble du cycle de vie de l'information, de sa création à sa préservation.

## Annexe 8 : Étude de cas concrets d'attaques

### La British Library

Le 28 octobre 2023, la British Library a subi une attaque par rançongiciel menée par le groupe criminel Rhysida, entraînant une paralysie majeure de ses services. Cette attaque a compromis 600 Go de données, incluant des informations personnelles. L'attaque menée reposait sur une stratégie de double extorsion ; chiffrement des données par un algorithme de cryptographie, exfiltration et menace de divulgation des données en cas de non-paiement assortie d'une rançon de 600'000 GBP en cryptoactif. Ce sont alors près de 490'000 fichiers volés finalement proposés à la vente sur le darknet.

Données de la British Library vendues aux enchères sur le darknet



(Khadgi 2023)

Les conséquences de l'attaque ont été profondes et durables. Plusieurs fonctions essentielles comme l'ingestion des dépôts légaux numériques, ou la recherche dans les catalogues, ont été gravement affectées. La bibliothèque a dû fonctionner temporairement dans un état pré-numérique (Knight 2023). Le rapport publié par la BL post-attaque, s'interroge d'abord sur les origines, le mode opératoire d'attaque ou les tactiques, techniques et procédures (TTP)(Johnson et al. 2016) utilisées et la stratégie de réponse mise en place (British Library 2024). L'enquête est rendue complexe par les moyens utilisés pour l'exfiltration, elle fait état d'une intrusion et de reconnaissances hostiles trois jours auparavant. Ce premier point de contact aurait été une manière de tester la solidité de l'infrastructure, avant l'attaque principale (British Library 2024). Le jour de l'attaque un mouvement anormal de 440 Go de données est détecté au niveau des serveurs. La vulnérabilité exploitée apparaît au niveau d'un serveur dédié au télétravail dont l'accès a été rendu possible par la compromission d'identifiants de comptes administrateurs, par le biais d'un phishing, d'une usurpation d'identité, ou d'une attaque par force brute. Ce serveur n'était pas protégé par l'authentification multi-facteurs (qui couple un mot de passe à d'autres méthodes d'identification) (British Library 2024). Rhysida exploite généralement ce type de lacunes sur des services critiques et l'usage d'identifiants compromis pour établir une présence persistante dans les systèmes (Khadgi 2023). La généralisation de l'authentification multi-facteur à l'ensemble de l'infrastructure avait été considérée trop lourde et coûteuse (Oury 2024).

Dès la détection et la qualification de l'attaque, la British Library a activé un dispositif de crise. En s'appuyant sur l'expertise d'acteurs externes. En parallèle la mise en place d'une cellule de communication a permis d'informer continuellement le personnel, les usagers et les parties prenantes, malgré la perte du site web et de l'intranet (British Library 2024).

L'environnement technologique, historiquement hétérogène en raison de la fusion progressive de collections, de services et de l'ajout de nouveaux programmes (dépôt légal numérique, partenariats de numérisation, etc.), reposait sur une superposition de systèmes hérités, et pour

certains, obsolètes. Cette architecture devenue complexe, les processus manuels de transfert de données et une segmentation réseau limitée, ont amplifiées les effets de l'attaque, facilitée les mouvements latéraux de l'intrus et retardées les opérations de reprise. (Işık 2024). Des rapports indiquent que le code du malware contient des fragments de cyrillique, et il semble qu'il n'ait pas frappé à l'intérieur de la Russie ou de ses proches alliés (Knight 2023).

L'attaque aurait débuté par une compromission du service VPN de la bibliothèque via des identifiants valides mais piratés, possiblement récupérés par hameçonnage ou via un mot de passe faible. L'absence de double authentification sur les serveurs internes a facilité cette intrusion. Une fois à l'intérieur du réseau, les attaquants auraient appliqué une stratégie dite de *living off the land*, utilisant des outils natifs du système (PowerShell, SSH, RDP, etc.) pour cartographier le réseau, identifier des serveurs vulnérables, puis exploiter des failles connues notamment Zerologon (CVE-2020-1472) (The MITRE Corporation 2025) sur un contrôleur de domaine Microsoft non mis à jour. Ce type d'attaque inclut souvent des outils de test d'intrusion comme Cobalt Strike pour le mouvement latéral et l'élévation de priviléges. Une fois les systèmes critiques atteints, les fichiers sont chiffrés à l'aide des algorithmes de cryptographie LibTomCrypt ou ChaCha20, et les données exfiltrées via le VPN (Houghton, Winterburn, Oakley 2025). Le modèle Cyber Kill Chain de Lockheed Martin, permet de visualiser l'ensemble des étapes de l'opération, allant de la reconnaissance initiale à l'exfiltration, au chiffrement et à l'extorsion finale :

Tableau 12 - *Cyber kill chain* de l'attaque sur la British Library

	Lockheed Martin 7-step Cyber Kill Chain framework						
	1. Reconnaissance >	2. Weaponisation >	3. Delivery >	4. Exploitation >	5. Installation >	6. Command & control >	7. Action on objectives
<b>Rhysida Attack</b>							
Hacking & system tools	Initial: Port scanning, Cobalt Strike, ohishing  After VPN access: cmd, ipconfig, whoami, nltest, net, secretsdump etc.	VPN access gained through compromised used account or brute force password attack	Phishing, RDP, SSH, PowerShell commands	Cobalt Strike (Beacon), Zerologon	Encryption of critical files (LibTomCrypt, ChaCha20), placing ransom note	Enabling remote access software e.g., AnyDesk > data exfiltration	Ransom demand, selling data on the dark web

(Houghton, Winterburn, Oakley 2025)

La British Library, membre du réseau des six bibliothèques de dépôt légal du Royaume-Uni et d'Irlande, avait développé une infrastructure sécurisée et résiliente dédiée à la conservation à long terme des contenus numériques, notamment des revues électroniques déposées sous le régime de dépôt légal numérique introduit en 2013 (Beagrie 2013). Cette infrastructure, qui comprend quatre nœuds de stockage répartis entre la British Library, la Bibliothèque nationale d'Écosse et celle du Pays de Galles, est complétée par des points d'accès supplémentaires à Trinity College Dublin ainsi qu'aux universités d'Oxford et Cambridge. Conçue principalement comme une « *dim archive* », cette plateforme garantit avant tout la préservation pérenne des ressources électroniques, (l'accès aux contenus commerciaux étant restreint aux salles de lecture des établissements concernés). Cette stratégie est soutenue par des collaborations techniques, notamment avec Portico (Beagrie 2013). Ce système comporte l'un des éléments salvateurs de la stratégie d'archivage des collections numériques et numérisées. Cette

redondance mutualisée et couplée à une réPLICATION des données dite « à froid » (air gapped ou hors ligne) sur bandes magnétiques a permis aux collections numériques d'être épargnées. Cette approche a ensuite permis d'envisager une restauration progressive, bien que lente, des contenus (Entretien Y.Grandcolas, 2025). Des sauvegardes sécurisées, épargnées par l'incident, permettent d'envisager la restauration des collections numériques et des métadonnées (British Library 2024).

Après une étude approfondie, les échanges entre la British Library (BL) et la Bibliothèque nationale de France (BNF) convergent sur l'aspect essentiel de la mise en place des mécanismes de redondance et d'un stockage hors ligne sécurisé au sein d'un dépôt numérique (ISO 2025a). Cette stratégie de préservation numérique est renforcée par l'application des certifications internationales telles que TRAC, TDR (ISO 2025b, p. 16) ou le modèle d'évaluation DPC RAM (DPC 2024a). Malgré leur caractère coûteux en ressources techniques et logistiques, les sauvegardes hors ligne sur bandes magnétiques sont désormais pleinement intégrées à la stratégie de conservation à long terme mais le sont aussi dans la sauvegarde des catalogues de la BNF (Entretien Y.Grandcolas, 2025).

La perte la plus lourde et la plus handicapante concerne les catalogues qui ont été rendus inaccessibles, et ont de fait, perturbée gravement la recherche documentaire et impactée le travail des chercheurs et des étudiants (Knight 2023). La mise hors service des catalogues, véritables points d'accès centraux aux ressources numériques, a entraîné une interruption majeure de la consultation des collections et l'accès aux contenus documentaires. Cet exemple est le pire scenario (Breeding 2024) et illustre un cas extrême. Une atteinte à la disponibilité, gravement compromise par le chiffrement des fichiers et l'inaccessibilité du catalogue. L'intégrité menacée par la suppression des sauvegardes actives et locales. La confidentialité mise en péril par l'exfiltration de données sensibles et l'authenticité affaiblie par l'usurpation d'identifiants privilégiés. L'attaque a révélé une vulnérabilité critique, plaçant l'institution dans une position difficile face à la loi sur la protection des données, la rendant à la fois victime et responsable de la non-conformité rendant possible la violation de données sensibles (Knight 2023).

Grâce au partage transparent de le BL des recommandations peuvent être déjà établies (British Library 2024) :

- La segmentation du réseau est un des fondamentaux de la défense informatique visant à compartimenter les environnements numériques afin de limiter les déplacements latéraux d'un attaquant au sein du système. Cette approche permet de circonscrire une intrusion à un périmètre restreint, et réduire son impact global.
- La généralisation de l'authentification multi-facteur (MFA) à l'ensemble des services critiques, couplée à la mise en œuvre de solutions de gestion des priviléges d'accès (PAM), doit permettre de mieux protéger les comptes à hauts niveaux d'autorité, souvent ciblés par les attaquants.
- La modernisation ou la mise à jour continue de l'infrastructure technique afin de prévenir les risques liés aux environnements hérités et non maintenus. Il est recommandé l'élimination rapide des systèmes obsolètes, ainsi qu'un basculement vers des architectures hybrides offrant plus de garanties en matière de sécurité, de supervision et de redondance.
- L'importance de l'observabilité est à développer pour la surveillance active et continue, permettant la détection rapide d'anomalies, la traçabilité des actions et une meilleure réactivité face aux signaux faibles ou aux activités et comportements suspectes.

- Enfin, une révision des stratégies de sauvegarde s'impose. Le modèle de sauvegarde recommandé s'inspire de la logique dite « 4/3/2/1 » (voir 3-2-1-1-0<sup>14</sup>), à savoir : quatre copies des données, sur trois supports distincts, dont deux hébergés dans des environnements différents et une hors ligne.
- Il est également conseillé de disposer de plans de continuité et de reprise d'activité (PCA, PRA) intégrant l'ensemble des systèmes critiques tels que les catalogues, les bases de données et les outils de consultation, de maintenir une cartographie à jour des dépendances applicatives, et d'adopter une approche transversale de la sécurité, impliquant la gouvernance, la DSI, bibliothécaires et les utilisateurs finaux (British Library 2024; Grove 2024).

Outre les perturbations à long terme, l'attaque a engendré des coûts de récupération estimée près de sept millions de livres sterling selon les projections (janvier 2024). Un plan de restructuration a été lancé à la suite de l'attaque et la bibliothèque profite de ce processus pour mettre en œuvre des améliorations de son infrastructure technologique et de ses pratiques de sécurité (Işık, 2024). En mars 2024, et encore aujourd'hui (Entretien Y.Grandcolas, 2025), les services n'étaient toujours pas entièrement restaurés. L'impact réputationnel sur l'institution est conséquent et proportionnel à la médiatisation de l'affaire, une étude de 2024 présente l'analyse de 123 articles parus dans les médias (Lindström, Spirkina 2024).

### **L'Université de Neuchâtel**

La cyberattaque ayant visé l'Université de Neuchâtel en février 2022 constitue un autre exemple d'attaque logique qui peut affecter les institutions académiques. Initialement perçue comme un vol limité de données internes, l'attaque s'est révélée plus grave, avec la publication progressive, sur le darknet, d'informations sensibles touchant la communauté universitaire et des entités externes telles que des entreprises privées, des instances cantonales et fédérales, voire des partenaires internationaux (Seydtaghia 2022). Contrairement aux objets physiques, les données numériques peuvent être exfiltrées sans laisser de traces visibles, car elles ne sont pas volées au sens classique du terme, mais dupliquées à l'insu de son propriétaire. Cette caractéristique rend la détection et la prévention d'autant plus complexes devant reposer sur des outils d'analyses comportementales (systèmes de détection et de prévention d'intrusion IDS/IPS) qui permettent d'identifier en temps réel les tentatives d'accès non autorisées au réseau ; les mouvements latéraux et les exfiltrations de données. Ces outils assurent la surveillance des comportements anormaux liés à la circulation interne ou à la fuite d'informations ; les solutions SIEM (Security Information and Event Management) centralisent, corrèlent et analysent les journaux d'événements afin de détecter des incidents complexes ; enfin, les solutions DLP (Data Loss Prevention) préviennent les fuites de données sensibles en surveillant et contrôlant leur transfert vers des destinations non autorisées). Dès la détection de l'incident, le service informatique à immédiatement mis hors réseau l'ensemble du système informatique pour contenir la menace. Bien que le mode opératoire rappelle celui d'un *ransomware*, aucune demande de rançon n'a été signalée (Chavanne 2022).

La diffusion non protégée de ces contenus, souvent dépourvus de chiffrement, pointe un défaut de sécurisation de l'information et de gouvernance des données. La classification de la

---

<sup>14</sup> La méthode 3-2-1-1-0 est une stratégie de sauvegarde avancée qui recommande de conserver trois copies des données sur deux supports différents, dont une hors site, une hors ligne et sans erreur c'est à dire testée, garantie, face aux pannes, erreurs humaines et cyberattaques.

sensibilité des données se révèle incontournable. Le traitement des mots de passe échangés en clair par courriel, l'absence généralisée de chiffrement concernant les données sensibles en transit et au repos et la centralisation insuffisante des protocoles de protection révèlent un manque de maturité en matière de politique de sécurité.

En explorant les sources disponibles sur le darknet, il a été possible de recueillir des informations sur le groupe à l'origine de l'attaque. Il s'agirait de *Conti* qui administre un *ransomware-as-a-service*. Au-delà des impacts réputationnels et juridiques, cette crise révèle l'urgence de renforcer leur politique de gouvernance conjointement à la cybersécurité, en adoptant des stratégies proactives. Le déploiement systématique du chiffrement, segmentation des réseaux, sensibilisation des usagers, et intégration de la sécurité dès la conception des systèmes «*secure by design*». À l'échelle nationale, cette affaire a d'ailleurs eu un effet catalyseur, poussant d'autres établissements comme l'Université de Genève et l'Université de Fribourg à réévaluer leurs dispositifs, dans un écosystème numérique universitaire de plus en plus interconnecté, la faiblesse d'un seul acteur peut exposer tout un réseau à des risques majeurs (Chavanne 2022).

### **L'Université de Zurich**

En février 2023, l'Université de Zurich (UZH) a été victime d'une cyberattaque impliquant plusieurs salves d'attaques par déni de service distribué (DDoS), impactant la disponibilité du système d'information. Cela permet d'infliger une pression à la cible au niveau de ses ressources. L'attaque a été facilitée par la mise en vente préalable de données d'accès aux serveurs institutionnels sur un forum clandestin. Cette situation montre une négligence initiale de la part de l'université, qui n'a pas eu la capacité d'identifier suffisamment tôt cette fuite d'identifiants. Bien qu'aucun accès effectif aux données personnelles ou à des comptes individuels n'ait été confirmé, l'incident a conduit à des mesures préventives telles que la modification généralisée des mots de passe et la réinstallation des accès VPN pour les membres de la communauté universitaire. Ce cas rappelle la nécessité d'une veille proactive sur les forums cybercriminels, sur le darknet et d'un renforcement constant des dispositifs de sécurité pour contrer les menaces qui augmentent elle-aussi en complexité et en technicité (Jaun, Schenner 2023).

L'Université de Zurich a lancé un appel urgent à l'ensemble de sa communauté universitaire afin de procéder à une modification immédiate de leurs mots de passe. Cette mesure vise à contrer les risques liés à l'utilisation de mots de passe compromis ou insuffisamment sécurisés, qui représentent une faille courante exploitée après une attaque informatique.

### **La Haute École Spécialisée de Lucerne**

En avril 2025, la Haute école spécialisée de Lucerne (HSLU) a été la cible d'une attaque par *ransomware* visant une partie spécifique de son infrastructure informatique, à savoir un environnement de laboratoire distinct des services IT centraux. Cette section, principalement utilisée par le département d'informatique, héberge plusieurs machines virtuelles, dont certaines ont été compromises. L'incident n'a toutefois eu aucune incidence sur les activités générales de l'établissement, et selon les premières analyses, aucune données sensibles concernant les étudiants ou le personnel n'a été affectée. La HSLU a immédiatement mobilisé ses spécialistes internes, en collaboration avec des entités externes telles que SWITCH CERT et l'Office Fédéral de la Cyber Sécurité (OFCS), afin d'évaluer l'ampleur de l'attaque et de

prendre les mesures nécessaires. Une plainte officielle a été déposée, et l'institution s'est engagée à communiquer toute nouvelle information pertinente. Cet incident montre la vulnérabilité des infrastructures de recherche et d'enseignement face aux cybermenaces notamment des risques liés au « *shadow IT* », ces environnements informatiques développés et maintenus en dehors du contrôle direct des services informatiques officiels, qui peuvent échapper aux politiques de sécurité institutionnelles et ainsi devenir des points d'entrée privilégiés pour les cyberattaques (ANSSI 2024a). Il exemplarise le recours aux appuis externes nationaux et sectoriel.

### **Bibliothèque de l'Université de Leipzig**

L'Université de Leipzig a révélé une vulnérabilité ayant permis, en avril 2023, l'accès non autorisé à environ 70 000 enregistrements d'utilisateurs de sa bibliothèque dont des anciens utilisateurs. Les données exposées étaient relatives à la confidentialité des informations personnelles, adresses e-mail, noms d'utilisateurs et les numéros des cartes de bibliothèque, mais excluaient explicitement les mots de passe. Prises seules on peut s'interroger sur la valeur de ces données, mais croisées avec d'autres informations elles peuvent révélées un intérêt financier non-négligeable (Entretien A. Rossier, 2025). L'exploitation effective de cette faille a été confirmée par l'accès d'au moins un acteur non identifié, et menace d'entraîner une augmentation des risques de *phishing*, *spear-phishing*, d'attaques ciblées basées sur ces informations. L'université a par ailleurs identifié que les données exposées comprenaient les utilisateurs actifs, mais aussi d'anciens inscrits, révélant ainsi des lacunes dans la gestion du cycle de vie des données. En réponse, la bibliothèque universitaire s'est engagée à réviser sa stratégie de suppression des données, à renforcer la qualité et la sécurité du développement logiciel, et à améliorer globalement ses pratiques de cybersécurité, notamment par la création d'une nouvelle direction dédiée à l'infrastructure informatique (Sokolov 2022). Cet exemple montre le risque de conversion d'une attaque opportuniste à une attaque ciblée, et la réaction post incident constructive, mais tardive de l'institution après avoir été victime d'une crise.

### **Établissements de l'enseignement et de la recherche**

Survenue entre 2022 et 2023, une crise d'ampleur à touché les établissements de l'enseignement supérieur et de la recherche françaises (ESR). Ce cas montre l'escalade des menaces informatiques sur plusieurs sites d'un même ensemble, notamment via la diffusion massive de malwares de type « *information stealer* » ayant permis l'exfiltration silencieuse de milliers de mots de passe étudiants à partir de dispositifs personnels non gérés par les établissements. Cela a rendu possible l'exploitation directe des identifiants compromis pour pénétrer les systèmes d'information de plusieurs universités et hautes écoles. Ces intrusions ont conduit, dans certains cas, à des attaques par rançongiciel ayant partiellement ou totalement détruit des infrastructures, de certains établissements, contraint à une reconstruction intégrale de leur SI. La réponse institutionnelle centralisée, orchestrée par la cellule opérationnelle de crise cyber, a nécessité la mobilisation coordonnée de plusieurs instances ministérielle de la sécurité du numérique (CERT-RENATER, COSSIM, FSSI), ainsi que la mise en œuvre d'un plan d'urgence comportant seize mesures techniques et organisationnelles prioritaires. L'analyse de cette crise montre la nécessité de disposer d'un RSSI identifié, disposant de moyens humains, techniques et financiers adaptés, ainsi que de renforcer la résilience des établissements par des politiques de sécurité robustes. La mesure concernée mentionnait le cloisonnement réseau, la supervision des accès distants, la gestion

des mots de passe, la fiabilité des sauvegardes et structuration d'une organisation locale de gestion de crise cyber. Les SI universitaires sont des cibles de choix pour des cybercriminels et qu'un pilotage stratégique de la cybersécurité, est désormais une exigence incontournable pour l'ensemble des institutions.(ESRI 2024)

En août 2024, l'Université Paris-Saclay a été la cible d'une cyberattaque par *ransomware*, provoquant l'inaccessibilité de son site internet pendant plusieurs jours. Dès la détection de l'incident, une cellule de crise a été activée et l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été mobilisée pour accompagner la gestion de l'incident. L'attaque s'inscrit dans un contexte de recrudescence des cyber incidents en France, exacerbées par la tenue des Jeux Olympiques de Paris. Ce type d'attaque, en plus d'entraver gravement les activités administratives et pédagogiques, soulève également la possibilité d'opérations de diversion destinées à détourner l'attention des services de sécurité et infiltrer des systèmes critiques plus discrets.

### **Bibliothèque du Centre Médical Universitaire du Vermont**

L'attaque par rançongiciel ayant frappé le University of Vermont Medical Center en octobre 2020, en pleine pandémie de COVID-19, constitue un cas de la manière dont une cyberattaque peut perturber la continuité opérationnelle, documentaire et financière des établissements hospitaliers ainsi que par effet de bord les services d'une bibliothèque de santé rattachée à une université (Stokes 2022). La bibliothèque bien que non directement ciblée, a vu son accès en ligne suspendu pour les employés hospitaliers durant près de trois mois, en raison de l'interruption du lien réseau entre le centre médical et le campus. Cette situation montre la vulnérabilité des bibliothèques médicales dépendantes d'infrastructures interconnectées, mais également leur capacité d'adaptation en période de crise. Cette rupture génère l'isolement des services documentaires, et empêche l'accès aux ressources électroniques pendant une période prolongée pour le personnel soignant. À cela s'ajoute une communication défaillante due à la perte totale de messagerie institutionnelle ce qui affecte la capacité à réagir rapidement face à la crise. Enfin, la coordination organisationnelle complexe entre les différentes entités (hôpital, université, bibliothèque) constitue une difficulté qui peut retarder la remise en route des services. L'équipe de la bibliothèque a mis en œuvre plusieurs stratégies : acceptation temporaire d'e-mails personnels pour les prêts entre bibliothèques, création de comptes utilisateurs individuels sur certaines bases de données, communication ciblée dès le rétablissement partiel des systèmes, et maintien d'un accès sur place pour les usagers pouvant se déplacer. Le bilan permet de statuer sur l'importance pour les bibliothèques de disposer d'un plan de continuité spécifique aux cyberattaques, incluant des scénarios d'accès alternatifs, des canaux de communication d'urgence, et une collaboration renforcée avec les départements informatiques hospitaliers et académiques. Enfin, il met en évidence la place des bibliothèques dans l'écosystème hospitalier qui est souvent reléguée au second plan lors de crises informatiques, alors même qu'elles jouent un rôle important dans le soutien à la pratique clinique. Ces risques, peuvent avoir des répercussions sur la continuité des soins, l'accès à l'information et la sécurité des données.

Dans ce cas, l'inaccessibilité aux outils de communication internes et la non-priorisation des services bibliothéconomiques dans le plan de reprise ont prolongé les délais de rétablissement et prouve la nécessité pour toutes les bibliothèques de se doter d'un plan de réponse aux cyberattaques incluant, la planification de scénarios de contournement, la mise en place de

protocoles de communication d'urgence hors ligne et une évaluation régulière des vulnérabilités numériques.

### **CERN, EPFZ et centres de calculs**

Un incident majeur de cybersécurité survenu en 2024 dans un site de calcul pour le Centre Européen de Recherche Nucléaire (CERN) illustre le coût réel d'une compromission informatique prolongée. Des attaquants ont pris le contrôle de dizaines de serveurs afin d'y exécuter des opérations de minage de cryptomonnaies, s'appropriant les ressources destinées aux calculs scientifiques. Cette infiltration, passée inaperçue pendant plusieurs mois, a entraîné une perte directe de puissance de calcul estimée à 5 % sur la durée de vie du matériel, et une consommation abusive d'électricité financée par le centre. Au-delà des pertes matérielles immédiates, les conséquences de l'incident ont été lourdes sur le plan organisationnel et humain. Pendant quatre mois, l'ensemble de l'équipe système a dû abandonner ses activités habituelles pour se consacrer entièrement à la gestion de la crise, ce qui équivaut à près de deux années complètes de travail technique paralysé. À cela s'ajoute le soutien du bureau de la sécurité informatique du CERN, mobilisé pour l'expertise et l'investigation. La mobilisation a entraîné un gel des projets en cours, des retards dans les développements, et un surcoût significatif en main-d'œuvre spécialisée. De plus, la réputation du site a été mise à mal, et des ressources supplémentaires devront encore être mobilisées pour reconstruire l'environnement informatique, rétablir les services, améliorer les défenses et former le personnel. Au total, le coût de cet incident est estimé à l'équivalent de trois à quatre années de travail cumulé ainsi qu'à 10 % de l'investissement total en capacité de calcul du site. Ce chiffre est d'autant plus frappant qu'un investissement initial de même ordre dans des dispositifs de cybersécurité aurait très probablement permis d'éviter l'incident. En matière de politique des systèmes d'information, l'insuffisance d'investissement dans des mesures de sécurité préventives peut engendrer des coûts opérationnels, humains et financiers bien supérieurs à ceux requis pour une protection anticipée de l'infrastructure (CERN 2025).

Un cas similaire est survenu en 2020 sur le supercalculateur de l'École Polytechnique Fédéral de Zurich (EPFZ). Victimes d'une cyberattaque ciblant des connexions SSH compromises (Secure Shell, protocole réseau qui permet une connexion distante sécurisée et un transfert de fichiers). L'incident a conduit à la suspension temporaire de l'accès aux nœuds de connexion, visait vraisemblablement à exploiter la puissance de calcul pour miner de la cryptomonnaie. Bien que les supercalculateurs eux-mêmes aient continué de fonctionner, les infrastructures de recherche sont vulnérables à ces détournement et l'importance de sécuriser les accès distants dans des environnements scientifiques sensibles (Wagner 2020).

Ce cas met en évidence deux problématiques majeures dans les environnements académiques, d'une part, l'absence fréquente de plans formels de continuité d'activité dans les laboratoires, justifiée par une tolérance aux interruptions ; d'autre part, une architecture réseau souvent fondée sur un modèle de « château fort » où le franchissement du périmètre de sécurité donne accès à de nombreuses ressources. À l'inverse, l'adoption d'un modèle de type *Zero Trust*, plus cloisonné, permettrait de limiter l'ampleur des intrusions. La menace des *ransomwares* reste un risque critique, contre lequel la stratégie de sauvegarde 3-2-1 combinant copies principales, sauvegardes isolées et stockées hors ligne s'impose comme une mesure de protection incontournable (Entretien A.Flament, 2025).

### **Bibliothèques de lectures publiques**

Des bibliothèques publiques sont aussi la cible de ce type de menace. La Toronto Public library (Breeding 2024) apporte en plus des études de cas d'autres problématiques et des gestions différenciées des incident majeurs (Perez 2024). Dans le cas des cyberattaques affectant les institutions documentaires, la Seattle Public Library a été victime d'une attaque par rançongiciel qui, pendant plusieurs semaines, a perturbé gravement ses services numériques. Elle a nécessité une interruption complète des services en ligne, des catalogues électroniques et des systèmes d'emprunt automatisés. Le rétablissement progressif des systèmes a été mené par une petite équipe interne d'informaticiens, soutenue par des firmes spécialisées dans la gestion des incidents de cybersécurité et d'investigation forensique. Malgré la gravité de la perturbation, les bibliothèques ont maintenu leur ouverture au public grâce à un retour aux processus manuels préexistants. Le coût financier de cette attaque s'élève à plusieurs centaines de milliers de dollars et inclut les frais liés à la remise en état des systèmes, au recours aux consultants externes et aux efforts supplémentaires des employés. En réponse, la bibliothèque met désormais l'accent sur le renforcement de son infrastructure technologique, la sécurisation des systèmes, et une gestion stricte des données sensibles, notamment celles du personnel affecté. Ce nouvel incident, démontre l'intérêt de disposer d'un plan de continuité opérationnelle solide, des correspondants externes, d'une politique rigoureuse de cybersécurité, ainsi que de procédures de sauvegarde et de récupération des données régulièrement testées (Heintz 2024).

### **Internet Archive**

En octobre 2024, l'Internet Archive, figure centrale de la préservation de l'histoire du Web, a subi une cyberattaque compromettant les données personnelles de plus de 31 millions d'utilisateurs et entraînant la mise hors ligne temporaire de certains services dont la *Wayback Machine*. Cet événement constitue une véritable onde de choc pour l'écosystème de la mémoire numérique mondiale (Messarra, Freeland, Ziskina 2024). Bien qu'aucune demande de rançon n'ait été formulée et que les archives historiques n'aient pas été altérées, l'attaque révèle des failles structurelles majeures dans la cybersécurité de cette institution patrimoniale, pourtant dotée de dispositifs qualifiés de « conformes aux standards industriels »(Wu 2024).

Des failles au sein d'une bibliothèque JavaScript ont permis à des cybercriminels d'injecter un message d'alerte sur l'interface web, révélant la compromission de la base de données. Le fichier de 6,4 Go, diffusé sous forme de dump SQL, contenait notamment des adresses e-mail, pseudonymes, des mots de passe hachés, ainsi que des métadonnées sur les changements de mot de passe. Cette compromission a été rapidement relayée sur la plateforme "Have I Been Pwned", spécialisée dans la traçabilité des fuites de données. En amont de cet alerte, Internet Archive avait essuyé plusieurs attaques par déni de service (DDoS) mettant hors service les adresses archive.org et openlibrary.org. Le lien entre ces deux incidents n'est pas établi mais la corrélation entre la défaillance d'un composant applicatif, la fuite d'informations sensibles, et les risques de perturbations en série, font valoir la nécessité de surveillances techniques proactives, de stratégies de défense en profondeur, et de plans de continuité d'activité prévoyant des incidents en cascade (Bourgin 2024). L'identité des cybercriminels derrière la fuite de données n'est pas connue. Le groupe de hackers SN\_BlaCKMeta, a toutefois revendiqué les différentes attaques DDoS. Le message ironique laissé par les hackers. « L'Internet Archive fonctionne sur des bouts de ficelle » révèle crûment le décalage entre la mission publique essentielle de cette organisation et ses moyens techniques et financiers limités (Wu 2024).

La symbolique de l'événement peut rappeler celle de l'incendie de la Bibliothèque d'Alexandrie, tant il marque la fragilité de notre mémoire numérique collective, pourtant au cœur des usages académiques, judiciaires, journalistiques et citoyens. Internet Archive joue un rôle dans la documentation de contenus éphémères ou censurés, et offre un accès libre à plus de 900 milliards de pages web archivées. Ces structures garantes de la transparence démocratique et de la continuité du savoir sont devenues des cibles, sans disposer des moyens suffisants pour se défendre efficacement. Au-delà des aspects techniques, cette crise soulève des questions sur le sous-financement chronique des infrastructures de mémoire numérique. Comme l'a précisé le chercheur en cybersécurité Scott Helme, un tel niveau de compromission aurait pu avoir des conséquences bien plus critiques. Une diffusion de contenus malveillants ou des publications de messages idéologiques aurait pu être tout à fait possible si les attaquant avait des motivations politiques (Wu 2024).

La mobilisation concertée des acteurs publics et privés pour renforcer la résilience de ces institutions stratégiques, par une politique active de sécurisation, de financement pérenne et de reconnaissance statutaire n'est plus une option. La pérennité de l'Internet Archive, et plus largement des archives numériques, ne peut être laissée au hasard dans une société où l'accès à l'information constitue un pilier de la démocratie contemporaine. Le risque n'est pas seulement technique : il est épistémologique, démocratique et mémoriel. Pour y répondre, une mobilisation conjointe des acteurs publics, institutionnels et associatifs s'impose pour garantir la résilience des infrastructures d'archivage numérique, de renforcer les moyens des institutions comme l'Internet Archive, et d'intégrer l'archivage dès la conception des politiques publiques numériques (Kaufman 2025).

Ces attaques ne se contentent plus de perturber le service : elles compromettent la disponibilité et l'intégrité des systèmes qui assurent la sauvegarde de la mémoire collective. (Messarra, Freeland, Ziskina 2024). L'importance stratégique de l'Internet Archive<sup>15</sup> s'inscrit dans un contexte de fragilisation des contenus numériques publics, illustrée notamment par la suppression massive de milliers de pages web gouvernementales aux Etats-Unis. Cette tendance accentue la dépendance vis-à-vis d'initiatives indépendantes de préservation œuvrant pour conserver la mémoire d'un Web de plus en plus instable.

Les bibliothèques nationales comme académiques occupent une position privilégiée dans la vie culturelle et intellectuelle nationale et ont pour mission de sauvegarder la mémoire de toute une société, ce qui les obligent à maintenir une infrastructure fiable pour la diffusion du savoir. Comme beaucoup de choses importantes que nous tenons pour acquises, nous ne connaissons pas leur vraie valeur jusqu'à ce qu'elles nous soient enlevées (Lindström, Spirkina 2024).

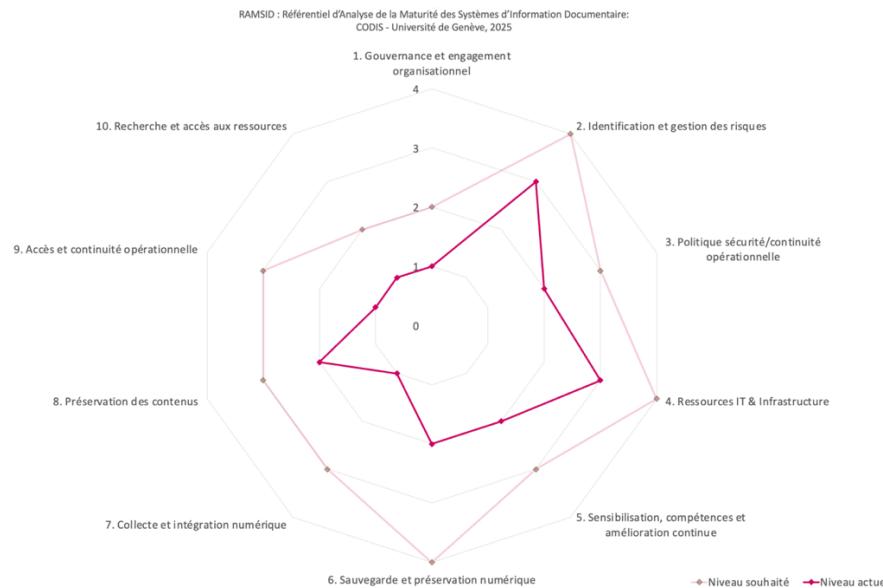
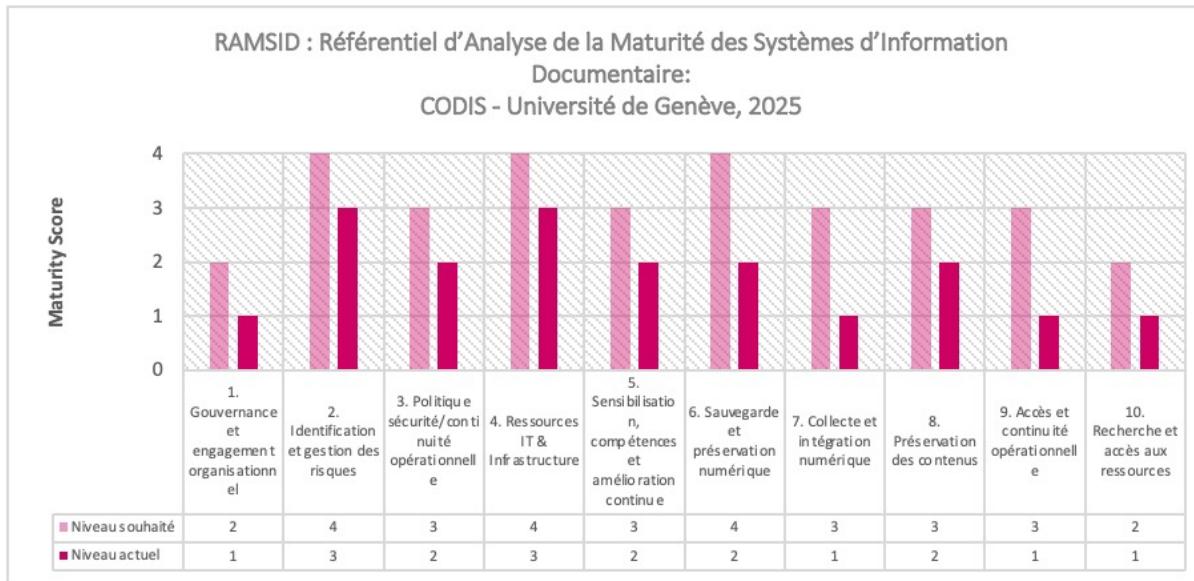
---

<sup>15</sup>Il participe à des projets comme l'End of Term Archive, qui sauvegarde systématiquement les données gouvernementales à chaque fin de mandat présidentiel depuis 2008. Cette démarche permet de contrer les suppressions arbitraires ou idéologiques de données publiques, et renforce ainsi la transparence démocratique et l'accès à l'information

## Annexe 9 : Matrice de maturité RAMSID

Niveau stratégique	Critères	Niveau actuel	Justification	Niveau souhaité	Mesures à mettre en place
<b>1. Gouvernance et engagement organisationnel</b>	Engagement de la direction, existence d'un Data Office. Clarté des responsabilités. Ressources financières et humaines allouées/allouables. Intégration de la conformité légale, classification des données, liés aux données personnelles. Capacité à démontrer la conformité en cas d'audit externe.	1 - Awareness	La mise en place d'un Data Office transversal regroupant CDO, DPO, RSSI et PDO montre un engagement clair du rectorat. Toutefois, la récence de la démarche, la reconnaissance du comité, la difficulté à arbitrer entre conformité légale et liberté académique empêchent l'atteinte d'un niveau supérieur. Une politique de protection et de gestion des données est en cours de validation, avec des efforts menés pour l'adoption globale de la classification. La formalisation est partielle, la classification des données sensibles et l'archivage doit encore être défini et devenir opérationnel.	2 - Basic	Reconnaissance du comité. Renforcement du lien entre classification et archivage. Utiliser les refontes de SI comme moyen d'intégration. Finaliser et diffuser la politique de gestion des données, et intégrer des déclinaisons sectorielles pour chaque domaine métier (recherche, RH, DIS...). Promouvoir une culture commune de la donnée, ateliers ou gt interservices et une gouvernance partagée entre les fonctions transversales et les utilisateurs métier.
<b>2. Identification et gestion des risques et vulnérabilités</b>	Niveau de formalisation des analyses de risques (BIA). Identification des menaces internes (erreurs humaines, shadow IT). Identification des menaces externes (cyberattaques, ransomwares). Surveillance proactive (SOC, cartographie CMDB).	3 - Managed	Les menaces internes et externes sont bien identifiées, un SOC est en place, des mesures proactives et réatives sont bien coordonées et la posture est managée et se trouve au delà de la moyenne pour le secteur de l'éducation. La politique institutionnelle est documentée, révisée, et disponible. Les analyses de risques et les remontées métiers restent hétérogènes, le manque d'un inventaire complet des actifs et l'adoption partielle d'une stratégie formalisée concernant les plateformes cloud constituent une vulnérabilité. La répartition budgetaire des services et des facultés peuvent augmenter la probabilité que des risques surviennent (shadow IT).	4 - Optimized	Généraliser l'usage de BIA sectoriels et consolider une vision centralisée des risques métier/DSI. Créer et maintenir une cartographie de l'ensemble des actifs numériques et leurs dépendances critiques. Formaliser une stratégie cloud complète incluant des clauses de réversibilité, des obligations de PCA/PRA, et un plan de reprise en autonomie. Renforcer les mécanismes de détection et d'encadrement du shadow IT, en intégrant une sensibilisation ciblée et une gouvernance budgétaire plus flexible entre les faculté et la DSI.
<b>3. Politique de sécurité et de continuité opérationnelle</b>	Existence et cohérence des plans de continuité (PCA/PRA). Formalisation des stratégies d'accès et classification des ressources numériques critiques. Politique documentée et régulièrement actualisée (archivage, sécurité des données, classification). Plans d'urgence des collections.	2 - Basic	Il existe des plans de continuité opérationnelle avec définition de RTO/RPO pour les parties critiques du SI, mais manque d'exhaustivité et de mise à jour pour les applications métiers, ils ne couvrent que partiellement les outils des SI métiers. Les implications métiers sont hétérogènes et insuffisamment intégrées aux processus. La présence des plans d'urgence révisés des collections et la constitution d'un groupe transversal en collaboration avec ELSE permet une assise organisationnelle, mais les plans ne font pas mention des outils métiers, des applications et des terminaux informatiques.	3 - Managed	Formaliser des PCA/PRA spécifiques pour les applications métiers documentaires (entre les PDs et le PCA) et les intégrer dans les SNE. Étendre les RTO/RPO aux applications documentation et en assurer la validation avec les responsables des processus. Mettre en place des tests en conditions simulées incluant des scénarios de rupture (ex. : perte d'accès réseau, panne SIGB). Consolider une documentation partagée entre la DSI et les services documentaires, inclure la procédure en cas d'indisponibilité des applications métier et des prestataires.
<b>4. Ressources informatiques et infrastructure</b>	Capacité des ressources informatiques à soutenir la continuité d'accès. Redondance et disponibilité des data centers et des infrastructures. Mise en œuvre de technologies spécifiques (snapshots, stockage à froid hors ligne).	3 - Managed	L'organisation dispose d'une infrastructure informatique avec des réseaux redondants et deux datacenters en mode actif-actif et un stockage sur bande, mais la mise en œuvre des tests d'arrêt formels est perfectible et les test unitaires sont réalisés au fil de l'eau. L'absence de solutions locales en cas d'interruption des services cloud empêche l'atteinte du niveau optimal. Les processus d'ingestion des backups sont formalisés mais pas remontés au niveau métier, les applications outils et ressources documentaires doivent être intégrées aux PCA.	4 - Optimized	Automatiser la bascule, tester l'arrêt complet. Étendre la documentation technique, intégrer les processus métiers critiques liés à la bibliothèques (portails, SIGB, Catalogue...). Développer des solutions de secours offline ou locales pour les services dépendants du cloud (Alma/Primo). Mettre en place une interface de dialogue entre DSI et DIS pour intégrer les ressources documentaires dans la chaîne de sauvegarde/restauration. Documenter les dépendances croisées entre infra et outils métiers pour améliorer la réactivité en cas de sinistre.
<b>5. Sensibilisation, compétences et amélioration continue</b>	Niveau de sensibilisation à la cybersécurité (formations régulières, sensibilisation, etc) Niveau de compétence et formations régulières en Records Management Communication centrale, transfert de connaissances, communication interservices Procédures régulières d'évaluation et de mise à jour des pratiques de sécurité et d'archivage. Existence d'indicateurs de performance et de suivi (score sécurité). Mécanisme d'amélioration continue fondé sur les retours d'expérience. Niveau d'implication des services dans la démarche de sécurité.	2 - Basic	Les besoins en compétences (Records Management, cybersécurité) sont clairement reconnus mais restent largement insatisfais. Les initiatives de formation sont identifiées, mais leur déploiement reste limité à certains secteurs seulement. Le projet d'organisation et de gouvernance des données est en cours de déploiement également. L'organisation a conscience de la nécessité d'une revue régulière des processus (cartographie, processus, services), les procédures d'évaluation régulières, les indicateurs de suivi, et l'amélioration continue formalisée ne sont pas encore en place de manière systématique. Le découpage et la taille de l'institution constitue un frein à la flexibilité. Les implications sont ponctuelles et non suivies.	3 - Managed	Déployer un plan de formation structuré par famille de métier. Intégrer des modules réguliers sur la cybersécurité, la gestion documentaire administrative, la préservation numérique et la conformité réglementaire. Renforcer les dispositifs de communication ascendante et transversale pour assurer une meilleure diffusion de l'information, notamment sur les risques identifiés, les incidents évités ou les évolutions de pratiques. Instaurer une revue des plans de continuité, politiques de sécurité, et processus de versement/archivage. Intégrer une logique d'amélioration continue dans les cycles de projet SI, avec des jalons dédiés à l'analyse des pratiques post-déploiement. Promouvoir une démarche qualité interservices soutenue par le Data Office, audits internes et échanges de bonnes pratiques.

Niveau opérationnel	Critères	Niveau actuel	Justification	Niveau souhaité	Mesures à mettre en place
<b>6. Sauvegarde et préservation numérique</b>	Gestion des exports et des archives courantes formalisé. Niveau de formalisation de la stratégie de sauvegarde (règles 3-2-1, etc). Archivage numérique hors ligne (réplication NAS, bandes). Gestion proactive de l'obsolescence technique (décommissionnement des systèmes obsolètes).	2 - Basic	Stratégie de stockage (NAS, bandes), la sauvegarde reste globalement mal formalisée et vulnérable aux attaques synchronisées. Une coexistence entre NAS et SP peut limiter l'uniformisation. L'usage de technologies comme DLCM est déployé comme appui à la recherche, mais non encore pleinement intégré dans une politique de préservation administrative et institutionnelle complète. La coexistence de plusieurs portails ou solutions d'archivages en fonctions des missions peuvent parasiter le message.	4 - Optimized	Intégrer les initiatives existentes de type DLCM dans une politique institutionnelle. Harmoniser les portails et outils de préservation selon les types de contenus. Formaliser une stratégie de sauvegarde claire (exports, règle 3-2-1, procédures de restauration).
<b>7. Collecte, transfert et intégration des ressources numériques</b>	Formalisation du processus de collecte et d'intégration. Documentation systématique et traçabilité du versement numérique. Automatisation des processus critiques (snapshots réguliers, intégration automatisée).	1 - Awareness	Certains processus opérationnels existent pour intégrer les ressources numériques, mais ces derniers sont encore très manuels et insuffisamment automatisés. Les politiques d'archivage et d'intégration des nouvelles applications commencent à se structurer, mais restent incomplètes et peu systématiques. L'utilisation partielle des systèmes existants et les pratiques très variables des métiers restent à formaliser.	3 - Managed	Formaliser les procédures d'intégration (logiciels métiers, messagerie, SI étudiants) et les documenter. Automatiser les processus critiques (versement, snapshots, traçabilité). Définir une politique unifiée d'ingestion des ressources numériques avec guides d'usage pour les métiers.
<b>8. Préservation de l'intégrité des contenus</b>	Mécanismes garantissant la sauvegarde, l'intégrité et la disponibilité des données. Contrôles d'intégrité réguliers, duplication et réplication géographique. Stratégies anti-ransomware avec copies immuables ou hors ligne.	2 - Basic	L'institution dispose de l'infra et des mécanismes (snapshots, bandes magnétiques), mais ceux-ci ne couvrent pas systématiquement toutes les données critiques (absence de solution de sauvegarde complète). Le risque d'attaques synchronisées sur les sauvegardes connectées reste élevé. Existence de technologies perennes mais adoption partielles.	3 - Managed	Étendre la couverture des sauvegardes à l'ensemble des données critiques. Mettre en œuvre des copies hors ligne immuables (air-gapped, WORM). Renforcer les contrôles d'intégrité périodiques avec alertes en cas d'anomalie. Procédures (multiniveau) de récupération formalisée et documentée.
<b>9. Accès et continuité opérationnelle des ressources</b>	Mise en œuvre de mécanismes alternatifs d'accès (solutions offline, copies locales). Déploiement effectif des accords contractuels (SLA avec prestataires externes, PCA et CA avec les éditeurs). Solutions distribuées et mutualisées de redondances des ressources électroniques Définition et tests réguliers des RTO/RPO. Documentation existante (mise à jour, connaissance, couverture)	1 - Awareness	Les accès d'urgence sont non garantis pour tous les systèmes essentiels, notamment en cas de coupure prolongée des services cloud. Des solutions ponctuelles sont ni formalisées ni testées régulièrement et dépendant des équipes locales. Des clauses contractuelles existent, mais leur portée et leur récolte n'est pas systématisée pour tous les fournisseurs, notamment pour les éditeurs de ressources électroniques. Pas d'inventaire exhaustif des SLA actifs ni de vérification régulière des engagements. L'absence d'adhésion à des solutions comme CLOCKSS, LOCKSS ou Portico mais Safe PLN et BN pour les thèses. Des plateformes comme Yareta sont utilisées pour certaines ressources, n'ont pas pour mission cette utilisation. Les RTO/RPO sont définis pour certains services (via le BIA mené par la DSI), mais elle n'est pas unifiée avec les métiers documentaires. Il manque une documentation partagée sur les procédures d'urgence, et les mesures de reprise propres aux ressources électroniques.	3 - Managed	Formaliser les procédures de continuité pour chaque plateforme documentaire critique (SIGB, résolveur de liens, accès à distance, portail d'accès). Créer un inventaire centralisé des SLA incluant : périmètre de responsabilité, modalités de reprise, durée d'indisponibilité tolérée, contre-parties en cas de non-respect. Élargir l'usage des solutions distribuées pour les ressources critiques (adhésion à CLOCKSS, Portico, PKP PN pour certains abonnements). Documenter et tester régulièrement les RTO/RPO en impliquant les équipes métiers.
<b>10. Recherche, récupération et accès aux ressources préservées</b>	Mécanismes d'accès et de recherche avancés (outils collaboratifs sécurisés). Respect des droits d'accès et gestion sécurisée des utilisateurs. Accès sécurisé et continu aux ressources sensibles en cas de crise majeure.	1 - Awareness	L'accès aux ressources préservées (en cas de sinistre majeur) est limité, peu documenté, et ne repose pas sur des solutions éprouvées et robustes. Il n'existe pas encore de mécanisme clair pour garantir un accès continu et sécurisé en situation d'urgence, particulièrement pour les ressources numériques critiques.	2 - Basic	Créer une interface miroir minimale en cas de sinistre (HTML statique, PDF, etc.). Définir une procédure d'accès d'urgence aux ressources critiques (offline, PDF statiques, etc.). Mettre en place des outils de recherche et consultation résilients (interfaces simplifiées, catalogue statique). Documenter les droits d'accès et garantir un accès sécurisé en situation de crise (protocoles de repli).



## Annexe 10 : Registre des groupes d'actifs

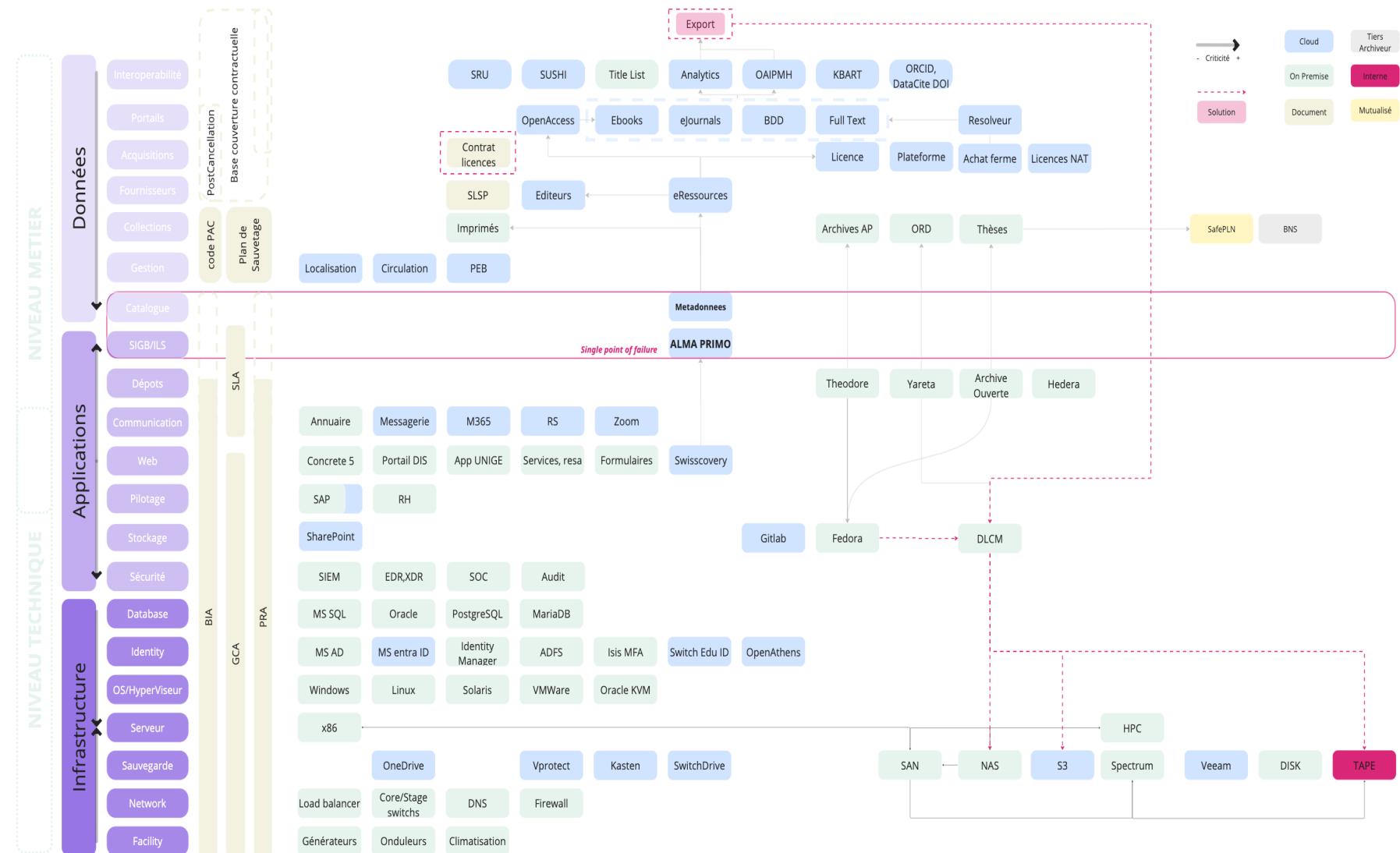
Catégorie d'actif	Description détaillée	Exemples concrets	Rôle dans la bibliothèque	Criticité	Priorité	Risques associés
Ressources électroniques	Revues électroniques, livres numériques, bases de données scientifiques, plateformes éditeurs	PubMed, ScienceDirect, UpToDate, e-books en médecine	Accès aux contenus scientifiques, support aux activités pédagogiques et de recherche.	3	1	Perte d'accès, altération des données, problème de licences, cyberattaques.
Système d'information	Infrastructures logicielles de gestion des ressources et des utilisateurs.	SIGB, portail documentaire, outil de découverte, résolveur de liens	Organisation, accès et diffusion des ressources, gestion des prêts.	4	1	Défaillance du système, perte de données, indisponibilité, intrusion.
Données utilisateurs	Informations personnelles et comportementales des usagers.	Historique de prêt, données de connexion, profils personnalisés	Adaptation des services, analyse des usages, sécurité d'accès.	4	2	Fuite de données, non-conformité LPD et RGPD, usurpation d'identité.
Données institutionnelles	Données internes liées au fonctionnement, à la stratégie et aux finances.	Statistiques d'usage, rapports d'activités, abonnements	Pilotage stratégique, prise de décision, justification budgétaire.	2	2	Manipulation des données, mauvaise gouvernance, perte d'information stratégique.
Équipements numériques	Matériel informatique et dispositifs numériques utilisés pour l'accès ou la gestion de l'information.	Serveurs, postes de travail, lecteurs RFID, bornes de prêt	Support physique à l'accès et à la gestion des services documentaires.	2	3	Défaillance matérielle, obsolescence, vol, attaque physique.
Capital humain / compétences	Ensemble des connaissances et expertises du personnel.	Bibliothécaires spécialisés, administrateurs système, formateurs	Exploitation, gestion et sécurisation des autres actifs.	3	1	Départs non anticipés, mauvaise transmission des savoirs, erreurs humaines.
Contenus internes	Documents produits localement pour l'accompagnement à l'utilisation des ressources.	Guides d'utilisation, tutoriels, notices bibliographiques	Valorisation et facilitation de l'usage des ressources.	2	3	Non sauvegarde, perte de valeur informative, obsolescence.
Dépôts institutionnels	Plateformes de dépôt, d'archivage et de diffusion des publications scientifiques et données de recherche.	Archive Ouverte, Fedora, dépôts institutionnels ou nationaux	Conservation, valorisation et accessibilité des productions scientifiques. Conformité aux exigences de la science ouverte.	3	2	Perte ou altération des données, non-conformité aux exigences de diffusion, indisponibilité, atteinte à l'intégrité scientifique.
Équipements numériques/stockage	Systèmes de stockage centralisé ou distribué pour héberger les données critiques de la bibliothèque.	NAS, SAN, Infra, voir Schéma Annexe	Stockage sécurisé et accessible des ressources numériques, dépôts, et données d'usage.	4	1	Perte de données, pannes critiques, ransomwares ciblant le stockage, mauvaise configuration, défaillance de redondance.

# Annexe 11 : Cartographie des processus

Inventaire des processus DIS																
Code	Processus métier	Sous-processus	Systemes impliqués *	Personnes / rôles responsables	Utilisateurs finaux	Criticité (UNIGE)	Justification	Impact DICA (ISO-27005)	Période critique	RTO (estimé)	RPO (estimé)	Coût estimé d'indispo/jour (CHF)*	Dépendances	Procédures de contournement	Ressources minimales requises	Responsable
P1	Acquisition des ressources électroniques	Identification Sélection Commandes, EDI, Facturation, Activation Import de notices	Authentification ALMA (module Acquisitions) : gestion des commandes, activation, réception SAP (système financier); traitement des factures Plateformes fournisseurs, portails éditeurs (EBSCO, Elsevier, Wiley,...) : commandes, téléchargement, licences, Outils de veille documentaire : repérage des besoins, nouveautés Formulaires (ebooks) EZProxy PRIMO	Responsable des acquisitions : supervision globale, lien avec les fournisseurs Responsable des collections : validation scientifique et budgétaire Bibliothécaires spécialisées : sélection et saisie des demandes Service comptabilité : vérification des factures et imputations SAP Gestionnaire de l'intégration ALMA x SAP : gestion des flux d'information	Bibliothécaires spécialisées (demandeurs) Enseignants-chercheurs prescripteurs Étudiants et chercheurs (usagers finaux indirects) Utilisateurs externes(HUG)	3	Processus essentiel au maintien de l'accès à la documentation scientifique. Un blocage impacte la disponibilité à moyen terme, un décalage temporaire est gérable grâce aux collections existantes.	C, I, D, A	Rentrée universitaire (septembre-octobre) et renouvellement budgétaire (décembre-janvier)	2-3 jours	1 jour	= 5000	Connexion ALMA/SAP stable (middleware, API) Portails fournisseurs accessibles (via proxy/authentification) Personnel formé disponible Statut de livraison et d'activation mis à jour Couverture budgétaire validée dans SAP	Enregistrement manuel des demandes via Excel Consultation des fournisseurs par email Saisie différée dans ALMA quand le système est de retour Accès provisoire via URLs directes si activation KO	1 personne de liaison ALMA-SAP 1 bibliothécaire acquisitions 1 accès proxy temporaire ou direct aux plateformes Excel de suivi mis à jour quotidiennement	Res. e-ressources (Nom, téléphone interne, email)
P2	Traitement documentaire	Indexation Catalogage Contrôles d'autorité Indexation MeSH	Authentification ALMA (Module gestion MD) Outils d'import Fichiers d'autorité Appels PRIMO	Resp. métadonnées Équipes en charge du catalogage	Bibliothécaire en charge du catalogage	2	Affecte la visibilité et l'accessibilité des documents dans les outils de recherche. Des retards prolongés peuvent freiner l'accès aux nouvelles ressources. Impacte que certaines ressources.	I, C, D	-	1 semaine	2 jours	3000	Connexion ALMA Fichiers autorités	Notices minimales Imports Excel	ALMA Personnel formé	Res. métadonnées
P3	Accès aux ressources électroniques	Authentification Consultation Resolution de liens Routage via proxy Consultation/téléchargement sur les plateformes éditeurs	Primo VE / Swisscovery Résolveur de liens Proxies Plateformes éditeurs idP (AAI/SWITCH edu-ID, OpenAthens) EZproxy Reverse-proxy Plateformes éditeurs (ScienceDirect, Wiley, PubMed Central...) - SaaS externes DNS interne (réseau)	Responsable ressources électroniques Data librarian IT Ingénieur IAM / IdP (DSI) Administrateur réseau (DSI) Support HelpDesk 1er niveau	Étudiants Chercheurs Médecins Personnel soignant	4	Interruption > 4 h bloque cours, recherche et support clinique pour potentiellement plus de 10 000 usagers. Toute la communauté est impactée, l'accès indisponible compromet directement l'activité pédagogique, la recherche et l'activité clinique.	C, I, D, A	Rentrée Examens Cours Recherche	4h	2h	12000, (productivité perdue + pénalités éditeurs + surcoût support)	Authentification AAI Fédération SWITCH Accès IP Internet & DNS Certificats TLS Contrats éditeurs valides	Guides imprimés URLs alternatives Diffuser URLs directes + VPN Guides PDF hors-ligne	VPN, URLs directes VM idP & EZproxy actives 1 admin réseau 1 bibliothécaire d'astreinte	Res. e-ressources
P4	Gestion des collections physiques	Equipement Recyclage, inventaire, adresseage Ranger Rangement Retour & retrait Numérisation PEB (aussi DBU) Mise en avant Désherbage Validation cotés ALMA	Authentification ALMA (Circulation) Stations RFID & portiques Systèmes de rangement Cotes et indexation Imprimantes étiquettes	Responsables collections Équipe catalogage & rangement	Bibliothécaires Auxiliaires Étudiants et chercheurs en salle de lecture	2	Le bon fonctionnement logistique reste nécessaire à une expérience usager fluide. Perturbation logistique mais impact limité sur l'enseignement et la recherche, les services numériques restent disponibles.	D, A	-	2 jours	1 jour	2000 (heures supplémentaires + pénalités retards + réputation)	Infrastructure RFID Dispo ALMA & réseau LAN Electricité portiques RFID Accès bâtiment & magasin Consommables étiquettes Licence 365 (Template Cotes)	Registre manuel papier d'emprunt / retour Bureaux manuels de réservation Chants tri par cote	Liste physique, accès locaux 2 bibliothécaires + 2 manipulateurs / jour Clés des magasins Listes imprimées des cotés prioritaires	Res. collections
P5	Accès aux collections physiques	Consultation (Libre accès et demandes) Orientation usagers Recherche documents patrimoniaux Surveillance des salles	Authentification ALMA (Circulation) Swisscovery RFID Accès locaux (Bâtiments)	Équipe accueil	Étudiants en salle de lecture Chercheurs spécialisés	2	Moins critique en contexte de numérisation avancée, mais nécessaire pour certains usages spécifiques (patrimoine, ouvrages non numérisés, chercheurs spécialisés).	D, T	Examens Période de révision (février, juin, octobre)	2 jours	1 jour	800 (gestion manuelle, désorganisation, surcharge d'accueil, limitation de l'accès aux documents uniques)	Accès bâtiment (contrôle UNIGE) Disponibilité du personnel Systèmes ALMA / RFID / badge accès Electricité dans les salles	Consultation restreinte sur demande Accès par liste imprimée des documents disponibles Surveillance manuelle renforcée	Catalogue imprimé 1 agent d'accueil + 1 magasinier Clef des magasins et bureaux sécurisés Plan de salle et guides usagers imprimés	Res. accueil
P6	Gestion des espaces physiques	Réservation de salles Accès salle de lecture et places de travail Contrôle accès	Authentification Système de réservation (Badge)	Accueil Logistique Sécurité (STEP & DIBAT)	Communauté	1	Impact logistique et confort, mais contournable à court terme. Le contrôle d'accès reste important pour des raisons de sécurité, accès autonome peu représenté pour la bibliothèque de l'UNIGE.	D	Examens Période de révision (février, juin, octobre)	2 jours	1 jour	500	Contrôle accès UNIGE	Ouverture manuelle	Planning local	Res. locaux
P7	Services aux usagers	Prêt PEB Retour Aide à la recherche	Authentification ALMA Circulation PRIMO / Swisscovery RFID PEB Navette SLSP (services RAPIDO) Application Unige	Équipe accueil Bibliothécaires de référence Responsable des services aux publics	Étudiants Enseignants Chercheurs Personnel HUG Extérieurs	4	Cœur du service de la bibliothèque. Toute interruption entraîne une désorganisation majeure des services aux publics et une insatisfaction immédiate des usagers (1000+ usagers potentiels / jour). Impact sur l'image de l'institution et sur les obligations de service . Forte sollicitation du personnel sans outil numérique en cas de panne.	I, D, A	Examens, rentrée universitaire, période de remises de travaux et de thèses	4h	2h	10000 (perte de productivité et personnel redéployé, traitement différé, surcharge de gestion manuelle, erreurs, litiges usagers, image de marque et plaintes remontées aux niveaux supérieurs)	SI usagers/annuaire, authentication AAI RFID Authentification Connexion entre ALMA et PRIMO / Swisscovery (résa, visibilité des documents) SLSP (navette + interopérabilité PEB)	Fiches manuelles papier Prêt provisoire Feuilles d'emargements pour réservations	Accueil, supports papier guichet actif avec personnel formé Poste informatique avec tableau / scan Fiches papier standardisées (prêt/retour) Accès téléphonique à la coordination de service	Res. services aux publics

P8	Formation et accompagnement	Cours Tutoriels Ateliers	Moodle / plateforme e-learning UNIGE ALMA, PRIMO "sandbox" Outils bibliographiques externes : Zotero, EndNote Visioconférence (Zoom) Salles PC & réseau Wi-Fi	Formateurs Coord. Formations	Étudiants Doctorants	3	La formation est importante mais peut être replanifiée, l'indisponibilité a un impact limité à court terme, sauf en période de rentrée ou de début de thèse impact possible sur la qualité des recherches.	I, C	Rentrée, début thèse	1 jour	1 jour	1000 (temps formateurs + pénalités replanification + perte productivité étudiants)	Planning formation AAI / LDAP pour connexion aux plateformes Internet & réseau Wi-Fi stable Accès aux ressources électroniques (démonstration) Disponibilité des salles & PC	Supports imprimés, vidéos Matériel pédagogiques Accès local Réplanification	1 formateur + 1 salle PC ou vidéoprojecteur Supports PDF / print Accès local à la sandbox ALMA	
P9	[Accès aux ressources électroniques + Services aux usagers] Services de recherche spécialisés et soutien à la recherche	Rédaction et validation DMP Suivi dépôts publications et données Suivi obligations bailleurs	idP (AAI / SWITCH edu-ID, OpenAthens) VPN ORCID Bases de données bibliographique et full text PRIMO / Swisscovery outils DMP	Data librarian Resp. soutien à la recherche Support E-research	Chercheurs Médecins Doctorants	4	Lié aux exigences des bailleurs (FNS, H2020). Tout retard dans la fourniture d'un DMP ou de preuves de dépôt peut compromettre un financement ou la validation d'un diplôme. Un retard ≥ 24 h peut bloquer un financement, retarder soutenance ou audit + impact financier & réputationnel majeur.	I, D, A	Fenêtres dépôt bailleurs Soutenances doctorales Clôture projets	8h	1 jour	6000 (risque de pénalité, blocage fonds, heures sup.)	Réseau & Internet stables SWITCH AAI pour auth. APIs bailleurs accessibles Validation juridique (contrats)	Modèles DMP Word hors-ligne Envoi PDF par e-mail aux bailleurs Stockage temporaire sur disque Dépôt différé dès rétablissement	1 data librarian Modèles DMP & check-lists hors-ligne	Data librarian
P10	Administration et pilotage	Élaboration du budget (prévisionnel & rectificatif) Exécution, suivi budgétaire mensuel Reporting KPI Préparation des bouclages et audits (fin d'exercice)	Authentification ALMA Analytics SAP Outils BI SSO AAI LDAP Serveur fichiers budgets (.xlsx sécurisés) Planification budgétaire	Équipe de direction DIS Responsables de sites, CODIR Adjoint finances / contrôleur de gestion Rectorat enseignement	Direction DIS Rectorat DIFIN Auditores externes	3	Les fonctions budgétaires et de pilotage sont stratégiques. Une interruption prolongée affecte la planification, le reporting, et la comité institutionnel décision stratégique (allocations, acquisitions); respect des deadlines légales (bouclage cantonal, audits); traçabilité vis-à-vis des bailleurs (fonds FNS, EU).	A, C	Clôture mensuelle (25-30) Clôture annuelle (déc.-janv.) Audit externes	1 semaine	2 jours	2000	Disponibilité SAP & DB Oracle VPN vers SAP Licence BI ALMA API coûts Workflow validation budget	Export manuel CSV quotidien sur NAS Saisie engagements Reporting KPI simplifié Injection différée dans SAP à rétablissement	1 PC chiffré + Excel macros Back-up CSV Token VPN + accès AAI Guide procédures hors-ligne	Direction de la DIS CODIR Responsables administratifs
P11	Communication et valorisation	Actualisation du site Web Diffusion réseaux sociaux (Twitter, LinkedIn, Insta) Alertes-usagers (e-mail, SMS) Campagnes événementielles (Open Access Week)	Authentification CMS Concrete 5 Réseaux sociaux, compte institutionnel Emails/listes de diffusions	Resp. communication Webmaster Bibliothécaires et étudiants contributeurs	Grand public, communauté, étudiants chercheurs et médias	2	Moins critique pour le fonctionnement immédiat, mais la communication est stratégique en période de crise pour informer les usagers (panne catalogue, sinistre) le site et les réseaux sont le canal officiel	C, A	Crise opérationnelles Événements grand public	2 jours	1 jour	1500	DNS & SSL SWITCH LDAP / AAI pour CMS Hébergeur APIs Twitter/Meta	Newsletter, site secours Page Web statique pré-hébergée Routage DNS d'urgence Liste-mail de crise Affichage physique & écrans halls	1 laptop avec copie locale du site statique + client FTP Template e-mail d'alerte Accès 4G / hotspot si réseau campus KO	Resp. communication
P12	Dépôts de données de recherche	Création entité institutionnelle Pré-ingest (données + métadonnées) Agent (SIP), Archive (AIP), Broadcast (DIP) Définition droits d'accès Dépôt Octroi DOI Contrôle FAIR	Yareta (DLCM) API ORCID, DataCite DOI idP (AAI / SWITCH edu-ID, OpenAthens) Scripts (checksum, BagIt) Import en masse	Resp. archives numérique Data librarian	Doctorants Chercheurs	4	Lié à la préservation à long terme, à la conformité réglementaire, et à la valorisation de la recherche. La perte ou l'altération de ces données peut être irréversible. Moins immédiat que les publications mais fondamental dans les exigences de la science ouverte et des bailleurs. Le non-dépôt peut bloquer la soumission ou la validation des projets.	I, C, A	Soutenances (Juin Juillet et Décembre)	1 semaine	1 jour	5000	ORCID serveurs UNIGE DLCM AAI SAN Back-ups immuables (S3, LTO)	Archivage manuel Publication différée	VM Yareta read-only Accès backup S3 Checklist dépôt manuel PDF	Resp. Pole E-research
P13	Dépôts de publications	Soumission Validation Validation MD Obtention des diplômes Diffusion Passerelle pre-archive (SPLN, BN)	Archive ouverte UNIGE (Fedora) ORCID / Crossref idP (AAI / SWITCH edu-ID, OpenAthens)	Resp. académique Support thèses Référent OA	Doctorants Auteurs UNIGE	4	Étroitement lié aux obligations académiques et réglementaires. Des interruptions compromettent la validation des parcours ou le respect des exigences Open Access.	I, A, D	Période de soutenance	1 semaine	1 jour	3000	ORCID Utilis validation	Soumission manuelle Upload sur NAS Validation provisoire	Soutien support thèses Accès backup Guide dépôt hors-ligne	Support Thèses
Results			1-Authentification (AAI/SO) : 10+ Elève 2-ALMA (tous modules) : 5+ Elève 3-PRIMO / Résolveur / Swisscovery: 6+ Elève 4-Plateformes éditeur (SaaS): 5+ Elève 5-SAP : 3+ Moyenne à élève				*Criticité dans le cas d'une impossibilité de mener la totalité du processus dans le cadre d'un fonctionnement normal. Voir Matrice feuille 2					*Coût indirects d'indisponibilité/jour estimé : Le montant indiqué représente une estimation globale du coût financier et opérationnel engendré par l'indisponibilité totale du processus pendant une journée ouverte en période critique. Il tente d'inclure les coûts humains directs et la valorisation du temps perdu par les personnes impliquées (ETP mobilisés, agents administratifs, chercheurs, enseignants, professionnels) Evalué par la criticité du processus. De prendre en compte les retards ou ruptures d'accès, les conséquences sur les consultations, les traitements, ou délais critiques. Les coûts de remédiation soit les charges post-incident (retraitement manuel, corrections, replanification, surcharge des équipés) et les coûts d'image et de réputation (bafaille) : Perte de confiance des partenaires, usagers ou tutelles... sont ajoutés. NB: Estimation à titre indicatif				

## Annexe 12 : Cartographie du SI de l'UNIGE



## Annexe 13 : La définition d'une collection essentielle

Les ressources numériques et numérisées forment ce que certains qualifient de « cyberpatrimoine », en raison de leur valeur historique et culturelle (Ferracci 2016). Dans cette optique, un projet d'archivage à long terme, proposé par le Conseil administratif de la Ville de Genève et désormais validé, vise à centraliser, sécuriser et pérenniser les ressources électroniques des institutions culturelles municipales (Ville de Genève 2025; 2025). Ce projet repose sur la reconnaissance que la valeur des facsimilés numériques peut, dans certains cas, surpasser celle des originaux en matière de lisibilité, de conservation et de traitement documentaire avancé (Entretien VdG, 2025). À la Bibliothèque nationale de France (BNF), le système Système de Préservation et d'Archivage Réparti (SPAR) assure l'archivage à long terme des documents numériques à travers un système OAIS, certifié TDR et distribuable en marque blanche aux autres institutions de tailles plus modestes (Entretien Y. Grandcolas, 2025). Du côté des Universités, le Centre Informatique National de l'Enseignement Supérieur (CINES) est certifié pour l'archivage pérenne des données de recherche, acceptant les données des Services Commun de la Documentation français (Ferracci 2016). La Plateforme d'Archivage du CINES (PAC) assure la conservation pérenne de divers corpus scientifiques et culturels, tout en reposant sur une gouvernance partagée entre producteurs, diffuseurs et archivistes (Metrat, Oury 2017). Les dépôts de publications de recherche dans l'archive institutionnelle HAL suit le même chemin car les contenus sont automatiquement archivés dans l'infrastructure de stockage du CINES. Elle offre un archivage pérenne gratuit par le CINES, tout en permettant aux établissements de disposer de portails personnalisés. HAL permet ainsi de s'affranchir des types de publications en proposant une organisation par instance de son dépôt.

Le projet *Data Vault* du Harvard Law School Library Innovation Lab propose une initiative en matière de résilience technique et de responsabilité archivistique. En réponse à la disparition de plus de 2'000 jeux de données sur *data.gov* lors du changement d'administration américaine, cette initiative vise à collecter, authentifier et préserver des copies fiables de données publiques essentielles authentifier et rendre accessibles des données publiques à fort enjeu sociétal, comme celles de Data.gov ou de PubMed (Peet 2025). En utilisant des standards tels que BagIt pour garantir l'intégrité et la provenance cryptographiquement vérifiable des contenus, ce projet tente d'amener une réponse à la fragilité du modèle fondé sur l'existence d'un unique point d'accès, inspirée des principes du web décentralisé. Philosophiquement c'est une forme de résistance documentaire : il s'agit de rétablir la mémoire civique face à l'amnésie numérique induite par la volatilité politique, technique ou économique des hébergeurs initiaux (Peet 2025).

À l'UNIGE, la stratégie de préservation et de pérennisation des données de recherche a donné lieu au développement de la technologie DLCM (Data Life-Cycle Management). Cette solution constitue aujourd'hui le socle technique des services de pérennisation des données recherche, tels que Yareta à l'échelle cantonale et OLOS au niveau national. En facilitant la gestion du cycle de vie des données, DLCM concrétise la préservation numérique à long terme. Récemment, cette infrastructure a d'ailleurs été auditée dans le cadre du CoreTrustSeal, garantissant sa conformité aux standards internationaux de confiance (Burgi, Makhlouf Shabou 2021). Un projet prometteur fondé sur la technologie DLCM est actuellement porté par les Archives Administratives et Patrimoniales (AAP) de l'UNIGE : le projet Centella. Ce

dernier vise la mise en place d'une infrastructure pérenne pour l'archivage numérique à long terme, en réponse aux besoins croissants liés à la numérisation des fonds. En l'absence actuelle d'un système conforme aux standards de conservation, l'intégration des archives numérisées dans DLCM pourrait répondre à ces exigences et ouvrir la voie à une plateforme interne de préservation des publications scientifiques agnostique aux typologies d'archives.

Ce modèle pourrait également être envisagé pour l'Archive Ouverte, qui, pour le moment, n'assurent pas la pérennisation à long terme, bien qu'elles intègrent une sauvegarde active et récupérable des données déposées en cas d'incident technique. Historiquement, la plateforme repose sur Fedora, à l'instar du catalogue des fonds des AAP, mais une migration vers le système d'archivage à long terme DLCM pourrait assurer une préservation et une conservation à long terme réelle des contenus déposés. La possibilité d'une migration stratégique de Fedora vers DLCM représenterait l'aboutissement d'une démarche réfléchie et permettrait également de bâtir un portail comparable à HAL, offrant la conservation des données à long terme et la possibilité de multiplier les portails pour différentes missions d'archivage, d'intégrer les publications répondant ainsi aux besoins de certaines collections spécifiques à valeur patrimoniale et historique. L'utilisation de ces technologies et outils reste néanmoins soumise aux ressources financières et humaines disponibles pour leur mise en œuvre, leur maintenance et leur évaluation. La priorisation devient alors nécessaire, et le dimensionnement doit être effectué de manière réfléchie et consensuelle, sous peine d'accroître de manière intenable le coût total de possession (*Total Cost of Ownership*).

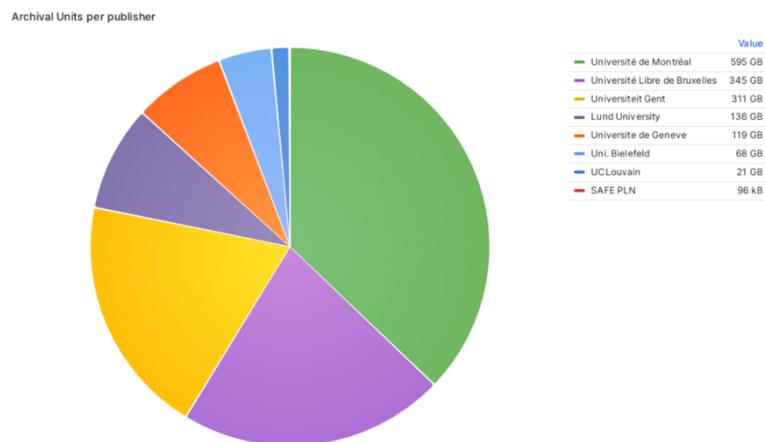
Le modèle conceptuel OAIS sert de référentiel pour mettre en œuvre des systèmes d'archivage qui peuvent conserver l'information et la rendre accessible sur de longues périodes. À la base, le fonctionnement de DLCM est structuré de manière modulaire. L'« archival storage » est responsable du stockage à long terme des données et constitue le point d'entrée vers les différentes infrastructures de stockage utilisées, tels que le système de fichiers, le stockage d'objets, ainsi qu'une troisième réPLICATION sur bandes magnétiques<sup>16</sup>. Ensuite, le module « data management » gère les métadonnées et les informations d'indexation, facilitant ainsi une recherche efficace dans les archives. Le module « administration » prend en charge la gestion des opérations et des politiques de l'archive, tandis que l'entité « preservation planning » est dédiée à la planification des actions nécessaires pour maintenir l'accessibilité et l'utilisabilité des informations stockées. Enfin, le module « access » offre aux utilisateurs les moyens de rechercher et d'exploiter les informations archivées. Le système DLCM intègre par défaut les fonctionnalités essentielles d'un "coffre-fort électronique" telles que définies dans la norme ISO 14641 sur l'archivage électronique. Le système garantit l'inviolabilité des documents en interdisant toute modification une fois validés et en maintenant les données figées. De plus, il empêche et peut tracer la destruction des documents, impose un contrôle strict des durées de conservation, et requiert une structure de classement rigoureuse gérée par l'administrateur.

---

<sup>16</sup> Les bandes magnétiques représentent une solution fiable et efficace (ANSSI 2023b) pour la sauvegarde et l'archivage à grande échelle, en particulier avec des systèmes comme le Linear Tape-Open (LTO). Ces bandes, souvent gérées par des bibliothèques automatisées, offrent une grande capacité et représentent une technologie mature, elle permet d'avoir une densité toujours plus importante comme le montre les derniers standards de LTO-9 pouvant stocker 18To (Lantz 2024). Son fonctionnement de types « near line » permet un stockage de données dites froides qui tolèrent plus de latence.

En complément en s'appuyant sur une infrastructure comme SafePLN, il est actuellement possible de mutualiser environ 4 To de capacité répartis sur 7 LOCKSS boxes, soit près de 600 Go disponibles par institution, dans les conditions techniques actuelles.

Figure 21 - Répartition du stockage du système Safe-PLN



(SAFE-PLN, 2025)

Car si l'idéal d'une conservation exhaustive des ressources électroniques peut sembler souhaitable d'un point de vue patrimonial, il se heurte rapidement à des contraintes structurelles, juridiques, économiques et techniques. En premier lieu, les limites de capacité de stockage et les coûts associés à l'archivage pérenne, notamment dans des environnements OAIS certifiés, imposent de hiérarchiser les contenus selon leur valeur d'usage, leur vulnérabilité et leur importance institutionnelle. À cela s'ajoute la complexité technique liée à la diversité des formats, des métadonnées, et des modalités d'accès : archiver des ressources numériques ne se réduit pas à leur simple duplication, mais implique des processus actifs de migration, documentation, contrôle d'intégrité et maintenance dans le temps. D'un point de vue juridique, les licences éditeurs comportent souvent des restrictions sur la copie ou la conservation locale, rendant illégal ou techniquement bloqué l'archivage de certains contenus. Par ailleurs, la volonté d'archiver sans distinction toutes les ressources pourrait paradoxalement diluer l'efficacité de la démarche en la rendant inexploitée ou inexploitable par manque de structuration et de moyens humains pour en assurer la gestion.

Le recours à des stratégies de préservation numérique apparaît indispensable. Développé par l'université de Stanford, le logiciel LOCKSS (*Lots of Copies Keep Stuff Safe*) constitue une solution open-source de préservation numérique conçue pour garantir la pérennité et l'intégrité des contenus académiques. À la différence des approches classiques de sauvegarde, LOCKSS repose sur un réseau distribué de nœuds autonomes et redondants, capable de détecter, réparer et prévenir toute altération des données via un mécanisme de comparaison continue entre copies. Cette technologie est au cœur du programme SAFE PLN. Le dispositif s'appuie sur un modèle de « dark archive », inaccessible en temps normal limitant ainsi les risques d'accès accidentels ou malveillants. Douze nœuds dispersés assurent la robustesse du stockage, complétés par des contrôles de sécurité avancés, authentification forte, chiffrement, audits réguliers, et diverses pratiques de sécurité propres à chaque site. Sa conformité aux exigences du référentiel TRAC, s'impose comme une infrastructure de confiance pour la préservation à long terme. en consolidant la souveraineté sur leurs actifs numériques (Smithers 2025b).

## Annexe 14 : Critères de priorisation des ressources électroniques

Critères	Catégorie	Description	Note (0-5)	Pondération (1-3)	Score
Techniques	Format des fichiers	Les fichiers sont-ils dans un format ouvert, lisible et documenté (ex : PDF/A, XML, MARC, Dublin Core) ? JHOVE?			
	Interopérabilité des métadonnées	Les métadonnées sont-elles récupérables via des standards ouverts (OAI-PMH, API, FTP) ?			
	Identifiant perenne	La ressource possède un identifiant perenne ISSN, DOI, ISBN, ARK, Handle, PMID..?			
	Accessibilité hors ligne	Peut-on recréer une version consultable sans dépendre d'un accès à la plateforme ?			
	Complexité d'extraction	Existe-t-il des outils ou scripts permettant d'automatiser l'extraction des données ?			
	Conditions d'exploitation	Le fournisseur accepte le text mining, le data-mining, et sous quelle condition ?			
	Taille estimée des données	Volume des données à sauvegarder (influence la capacité de stockage et la fréquence de sauvegarde).			
Quantitatifs	Fréquence d'utilisation	Nombre de consultations, téléchargements ou usages académiques par an.			
	Taux de citation ou de référence	Le contenu est-il souvent cité dans les publications ou cours de l'institution ? Utilisation du JCR Q1			
	Nombre de titres ou d'objets	Combien d'unités documentaires sont concernées (ebooks, articles, documents) ?			
	Nombre d'accès simultanés autorisés	Mesure l'importance du service pour les usages collectifs ou pédagogiques.			
	Durée d'accès post-résiliation (PCA)	Nombre d'années pendant lesquelles l'accès est garanti après résiliation du contrat.			
	Historique d'utilisation	La ressource est-elle utilisée de manière constante dans le temps ou de façon ponctuelle ? Taux d'usage par effectif facultaire			
	Nombre de départements concernés	Combien d'unités académiques utilisent ou dépendent de la ressource ?			
Qualitatifs	Durée de conservation souhaitée	Combien de temps la ressource doit-elle être conservée (court, moyen, long terme) ?			
	Valeur stratégique	Le contenu est-il essentiel à la mission de recherche, d'enseignement ou documentaire ?			
	Exclusivité du fournisseur	La ressource est-elle disponible uniquement via un fournisseur ou est-elle redondée ailleurs ?			
	Conditions d'accès en temps normal	La ressource est-elle en open-access, en freemium, protégée par DRM spécifique, nécessite une plateforme d'accès?			
	Présence dans les archives mutualisées	Le contenu est-il déjà conservé dans CLOCKSS, Portico, SafePLN ou similaire ? Voir DOAJ ? Voir Keepers Registry?			
	Clauses contractuelles explicites (PCA)	Existence de clauses précises autorisant l'archivage local ou via un tiers de confiance.			
	Stabilité du fournisseur	Le fournisseur est-il financièrement et structurellement stable ? Presence stable dans les bouquets, title list ?			
	Valeur patrimoniale ou légale	Le contenu doit-il être conservé pour des raisons juridiques, historiques ou institutionnelles ?			
	Disponibilité de copies exportables	Est-il possible d'obtenir des copies locales par export régulier (XML, MARC, fulltext) ?			
	Clarté des droits de conservation	Les droits de conservation sont-ils clairement définis dans les licences/contrats ?			
	Impact pédagogique	La ressource est-elle intégrée dans des cours, des modules de formation ou Moodle ?			
	Langue et accessibilité	La ressource est-elle disponible dans une langue et un format accessibles à la majorité ?			
	Criticité en cas de perte	Perdre cette ressource aurait-il un impact majeur sur l'enseignement ou la recherche ?			

# Annexe 15 : Analyse d'impacts métiers

## 1. Identification des Services Numériques Essentiels et activités

Lister les **Services Numériques** ainsi que les **principales activités** ou les **principaux processus clés** de l'entité concernée dépendants de ce Service Numérique.

#	Service Numérique* indispensable à la réalisation d'une activité	Activités (Prestation / sous-prestations / processus)	Activités / tâches clés (optionnel: permet de décrire plus en détail les activités analysées)
1	ALMA – Système intégré de gestion de bibliothèque	Gestion du prêt et du retour des ressources documentaires	Enregistrement des emprunts et des retours, prolongation des prêts, gestion des réservations, traitement des rappels automatisés, gestion des amendes, suivi des comptes usagers
2	PRIMO – Portail de découverte et accès public au catalogue	Mise à disposition des ressources documentaires aux usagers via une interface en ligne	Recherche documentaire, consultation et renouvellement des emprunts par les usagers, réservations en ligne, consultation du statut des ressources (disponible, emprunté, réservé), signalement des ressources électroniques ou physiques et accès aux ressources électroniques
3	ALMA – Gestion des acquisitions, traitement documentaire, catalogage et signalement des ressources	Traitements des nouvelles acquisitions, enrichissement du catalogue, signalement des ressources disponibles	Réception et traitement des commandes, création et mise à jour des notices bibliographiques et métadonnées, traitement des périodiques, importation/exportation de lots de notices, mise à disposition des ressources pour les usagers

\* faire référence si possible au nom du service dans le catalogue des Services de l'UNIGE.

<https://catalogue-si.unige.ch/>

## 2. Identification de la DIMA des activités clés et des impacts

Pour chaque activité (ou processus) clé :

- Identifier la DIMA : durée à partir de laquelle les conséquences de l'interruption des Services Numériques supports de ces activités deviennent intolérables
  - o Valeurs de DIMA (Durée d'Interruption Maximale Admissible : 1 h / 4 h / 1j / 3j / 1 s)
  - o La valeur de DIMA est à considérer en période normale (en dehors des périodes critiques qui seront précisées dans un paragraphe suivant)
- Déterminer les niveaux d'impact de l'interruption des activités au-delà de la DIMA
  - o Se baser sur la [grille d'impact de l'UNIGE](#)

Service Numérique	DIMA (1h / 3h / 1j / 3j / 1s / 1m)	Impact d'une interruption [1 à 4]
1	1j	3
2	4h	3
3	3j	2

La colonne DIMA doit obligatoirement être renseignée pour chaque activité identifiée.

Indiquer les niveaux des principaux impacts (il n'est pas obligatoire de remplir les valeurs de tous les types d'impact).

### 3. Précisions concernant les impacts de niveau 3 ou 4

Préciser quelles seraient les justifications des impacts de niveau 3 ou 4.

Ces précisions permettent de mieux appréhender les conséquences d'une indisponibilité d'un Service Numérique au-delà de la Durée d'Interruption Maximale Admissible

Service Numérique	Justification des impact(s) de niveau 3 ou 4
ALMA – gestion des prêts et retours	Une indisponibilité supérieure à 1 jour entraîne l'impossibilité complète d'enregistrer les prêts et les retours dans toutes les bibliothèques du réseau universitaire. Cela génère une interruption prolongée du service aux usagers, une impossibilité de gérer les comptes emprunteurs, une forte accumulation d'ouvrages en attente de traitement manuel et de potentielles pertes ou erreurs administratives. Cette situation altère significativement la qualité du service et impacte directement l'image institutionnelle ainsi que la satisfaction de la communauté à desservir.
Primo – accès public aux ressources documentaires	Une interruption dépassant 4 heures prive l'ensemble des utilisateurs (étudiants, enseignants, chercheurs) d'accès aux ressources documentaires, y compris les bases de données et les ressources électroniques essentielles pour les activités académiques et de recherche. Cela crée une situation critique en période de forte affluence (périodes d'exams, périodes de rédaction de travaux académiques, début des semestres), perturbant fortement l'activité académique.

### 4. Périodes critiques

Existe-t-il une ou des périodes critiques au cours de l'année ?

Si oui, préciser la DIMA (Durée d'Interruption Maximale Admissible) en période critique

Service Numérique	Période(s) critique(s)	DIMA en période critique Durée d'Interruption Max Admissible
ALMA/Primo	- Rentrée universitaire (septembre/octobre) - Périodes d'exams (janvier/février et mai/juin) - Renouvellement des contrats éditeurs	4 h

### 5. Perte de Données Maximale Admissible (ou fraîcheur des données)

En cas d'incident majeur entraînant l'indisponibilité d'un Service Numérique, la restauration des données dépend de la fréquence des sauvegardes. Il s'agit de définir les Pertes de Données Maximale Admissible (PDMA).

Préciser à quel moment dans le passé (à partir du moment de l'incident) faut-il être en mesure de récupérer les données ou informations clés, nécessaires pour un redémarrage adéquat des activités critiques ?

- Valeurs de PDMA à considérer : 1 h / 4 h / 1j / 3j / 1 s

Service Numérique	Pertes de Données Maximale Admissible (PDMA)	Commentaires si nécessaire
ALMA/Primo	1 j	Bien que la bibliothèque ne maîtrise pas la politique de sauvegarde, une perte de plus de 4 h de données critiques (prêts/retours, acquisitions, modifications de notices, réservations) entraînerait un besoin de reconstitution manuelle complexe et un risque accru d'erreurs. Cette valeur exprime le <b>niveau de tolérance de l'organisation, et doit être indiqué</b> même si le prestataire n'offre pas de garantie stricte de RPO. Cela peut servir de <b>base de négociation ou d'alerte</b> dans les échanges avec Ex Libris même si le prestataire ne garantit pas explicitement un RPO (Recovery Point Objective) aussi précis.
Note		<p>Dans le cadre de l'utilisation du système intégré de gestion bibliothécaire (SIGB) Alma, fourni en mode SaaS par Ex Libris, la définition de la Perte de Données Maximale Admissible (PDMA) soulève un questionnement lié à la nature externalisée du service. La gestion des sauvegardes et la résilience des données se doivent d'être entièrement assurées par le fournisseur, et ne relèvent donc pas du contrôle direct de l'Université de Genève.</p> <p>L'utilisateur final, en l'occurrence la Bibliothèque, ne peut ni configurer la fréquence des sauvegardes ni intervenir dans les procédures de restauration. Toutefois, selon la documentation officielle d'Ex Libris, Alma bénéficie d'une architecture à haute disponibilité, appuyée par une stratégie robuste de sauvegardes :</p> <ul style="list-style-type: none"> <li>- au moins quatre instantanés par jour</li> <li>- une sauvegarde complète quotidienne</li> <li>- une rétention des données de 10 semaines</li> <li>- un stockage sécurisé</li> <li>- tests mensuels de restauration.</li> </ul> <p>Malgré ces garanties techniques, la PDMA doit être définie en fonction des besoins opérationnels propres à l'institution. Dans le contexte de la Bibliothèque de l'UNIGE, une perte de données excédant quatre heures, concernant notamment les prêts, retours, acquisitions ou modifications de notices, serait susceptible d'engendrer des reconstitutions manuelles fastidieuses, source d'erreurs et de désorganisation. Cette valeur de PDMA constitue donc une référence interne permettant d'évaluer la tolérance acceptable à la perte d'information, même si le contrat de service ne prévoit pas explicitement un RPO (Recovery Point Objective) aussi précis. Il est par conséquent recommandé de documenter cette PDMA dans le cadre du BIA, de dialoguer avec le fournisseur pour obtenir des précisions sur les délais réels de restauration, et de mettre en place des procédures internes d'alerte et de suivi afin d'assurer une reprise d'activité aussi fluide que possible en cas d'incident.</p>

## Annexe 16 : Cartographie des risques

### Risques Cyber : liés aux intrusions, attaques, malwares, et compromissions du SI.

	Risque (Événement)	Causes	Conséquences	Risque brut						Risque net						Vitesse	Priorité	Traitement	Mesures	Coût	Délai	Responsable du risque					
				Probabilité	Impact			Contrôles effectués ou à effectuer	Probabilité	Impact			Criticité														
					F	H	R			F	H	R	P														
DIS-R1	Ransomware et cryptolocker	Phishing réussi Vulnérabilités non corrigées Formation insuffisante du personnel Clics sur liens malveillants	Inaccessibilité des catalogues et ressources numériques Perte de données de recherche Interruption des services essentiels Coûts de récupération élevés Atteinte à la réputation	4	4	3	4	4	16	Sauvegardes régulières hors ligne (stratégie 3-2-1) Segmentation des réseaux Formation du personnel Plans de continuité documentés Solutions EDR avancées	3	4	2	3	3	12	Haute	1	Réduire			RSSI					
DIS-R2	DDoS, DoS	Absence de protection DDoS Bande passante limitée Configuration réseau inadaptée Motivations idéologiques ou vengeance	Indisponibilité des plateformes pédagogiques Impossibilité d'accéder aux ressources pendant les périodes critiques (examens) Perte de confiance des usagers Perturbation des activités académiques	4	2	1	3	4	16	Services de filtrage DDoS Architecture redondante CDN (Content Delivery Network) Capacité d'absorption temporaire Détection comportementale	4	2	1	2	3	12	Instantanée	2	Eviter			RSSI					
DIS-R3	Exfiltration et publication de données	Contrôles d'accès insuffisants Absence de chiffrement Utilisateurs compromis Atttaques ciblées (APT)	Violation de la confidentialité des recherches Exposition de données personnelles Violation des accords de licence avec les éditeurs Poursuites légales Sanctions LPD /RGPD Responsabilité engagée	3	4	3	4	3	12	Chiffrement des données sensibles DLP (Data Loss Prevention) Classification des données Contrôles d'accès stricts Détection d'anomalies	2	4	3	3	2	8	Basse	3	Eviter			RSSI					
DIS-R4	Intrusion et phishing	Manque de sensibilisation Absence d'authentification forte Ingénierie sociale Partage d'identifiants	Accès non autorisé aux systèmes internes Compromission d'autres comptes Installation de backdoors persistantes Élevation de priviléges Détournement et utilisation des ressources de calculs	4	3	2	4	3	16	Authentification multi-facteurs (MFA) Formation anti-phishing récurrente Détection des comportements d'authentification anormaux Politiques de mots de passe robustes	3	3	2	4	3	12	Basse	4	Réduire			RSSI					
DIS-R5	Exploitation des API	Documentation publique excessive Absence de rate limiting Validation insuffisante des entrées Authentification faible	Extraction massive non autorisée de métadonnées Manipulation des requêtes Contournement des limitations d'accès Exposition de fonctionnalités internes	3	2	1	3	3	9	Authentification API robuste Rate limiting Validation stricte des entrées Journalisation des accès API Tokens à durée limitée	2	2	1	3	2	6	Haute	5	Eviter			RSSI					
DIS-R6	Robots et scrapping IA	Développement de l'IA générative Protection insuffisante des ressources Motivations économiques (reproduction) Contournement adaptatif	Surcharge des systèmes OPAC Extraction massive de contenus protégés Contournement adaptatif des protections Vol de propriété intellectuelle	4	1	1	2	2	8	CAPTCHAs évolutifs Détection comportementale Politiques d'accès définies par l'empreinte digitale du navigateur Limites de téléchargement	3	1	1	2	2	6	Instantanée	6	Réduire			RSSI					

## Risques technologiques, d'infrastructure : défaillances matérielles, logicielles, réseau.

DIS-R7	Obsolescence technologique	Évolution technologique rapide Absence de migration préventive Documentation insuffisante Propriété des formats	Perte d'accès aux collections numériques patrimoniales Impossibilité de migrer certaines données Coûts élevés de conversion Archives devenues inexploitables	4	4	2	3	4	<b>16</b>	Veille technologique active Migration préventive vers formats ouverts Documentation des formats Emulation des environnements obsolètes	3	3	1	3	3	<b>9</b>	Basse	7	Partager			DSI
DIS-R8	Infrastructure vieillissante	Budgets insuffisants Complexité de migration Dépendances techniques Incompatibilité entre systèmes	Vulnérabilités non corrigables Performance dégradée Incompatibilité avec les nouveaux services Maintenance coûteuse	4	3	2	3	3	<b>12</b>	Plan de renouvellement régulier Inventaire technique à jour Tests de vulnérabilité réguliers Segmentation des réseaux	3	3	2	2	3	<b>9</b>	Basse	8	Réduire			DSI
DIS-R9	Insuffisance des sauvegardes	Stratégie incomplète Absence de tests réguliers Sauvegardes en ligne vulnérables Processus manuels négligés	Impossibilité de restaurer après incident Perte définitive de données patrimoniales Prolongation des interruptions de service Coûts de reconstruction élevés	4	4	3	4	4	<b>16</b>	Sauvegardes immuables Tests de restauration réguliers Stockage géographiquement distribué Documentation des procédures Automatisation des sauvegardes	2	3	2	3	4	<b>8</b>	Haute	9	Réduire			DSI
DIS-R10	Problèmes d'alimentation électrique	Infrastructure vieillissante Pics de consommation Événements climatiques Maintenance insuffisante	Corruption des données Indisponibilité des services Dommages matériels Arrêts non contrôlés	3	3	3	3	3	<b>9</b>	Systèmes redondants Générateurs de secours Procédures d'arrêt progressif Systèmes de surveillance électrique	2	2	2	2	3	<b>6</b>	Haute	10	Accepter			DSI
DIS-R11	Défaillances réseau	Liaisons réseau uniques Absence de redondance Configuration DNS vulnérable Saturation non anticipée	Inaccessibilité des ressources externes Interruption des services cloud Impossibilité d'authentification fédérée Services web indisponibles	3	3	2	3	4	<b>12</b>	Liens réseau redondants FAI alternatif DNS secondaires Cache local des ressources critiques Plan de communication alternatif Supervision réseau proactive	2	2	2	3	3	<b>6</b>	Haute	11	Accepter			DSI
DIS-R12	Catastrophes physiques et climatiques	Bâtiments anciens Proximité installations hydrauliques Absence de détection précoce Stockage inapproprié Événements climatiques Réchauffement global	Destruction des collections physiques et du matériel Dommages aux infrastructures numériques Perturbation prolongée des services Perte définitive d'unicats	2	4	4	4	4	<b>8</b>	Systèmes anti-incendie adaptés Détection d'eau Redondance géographique Plans d'évacuation spécifiques BCP, DRP établis	2	3	3	3	3	<b>6</b>	Haute	12	Partager			DSI

## Risques de dépendance : concentration, externalisation ou services critiques tiers.

<b>DIS-R13</b>	Faillite d'éditeurs ou agrégateurs	Modèles économiques fragiles Concentration du marché Crise sectorielle Changements stratégiques	Perte soudaine de collections numériques Interruption d'accès aux abonnements Disparition de métadonnées d'accès Lacunes dans les collections	3	3	1	3	4	<b>12</b>	Clauses contractuelles de sauvegarde Solutions LOCKSS/CLOCKSS Participation à des consortiums Diversification des fournisseurs	2	2	1	2	3	<b>6</b>	Haute	13	Partager				<b>DIS</b>
<b>DIS-R14</b>	Dépendance SaaS/IaaS	Centralisation des solutions Économies d'échelle Compétences internes limitées Dépendance contractuelle	Interruption des services critiques Perte de contrôle sur les données Changements unilateral des conditions Augmentations tarifaires imprévues	4	4	1	3	4	<b>16</b>	Plans de continuité hybrides Export régulier des données Solutions locales de secours Négociation SLA robustes Documentation des API	3	3	1	2	4	<b>12</b>	Haute	14	Réduire				<b>DIS</b>
<b>DIS-R15</b>	Défaillance chaîne d'approvisionnement logicielle	Composants tiers non vérifiés Mise à jour automatique Confiance excessive Manque d'audit code	Vulnérabilités injectées dans les systèmes Accès non autorisés via backdoors Difficulté de détection Compromission silencieuse	3	3	1	4	3	<b>12</b>	Analyse des dépendances Containeurs isolés Monitoring des comportements anormaux Mise à jour rapide Signature de code	2	2	1	3	2	<b>6</b>	Instantanée	15	Réduire				<b>DIS</b>
<b>DIS-R16</b>	Défaillance des fournisseurs d'identité	Points uniques de défaillance Complexité des fédérations Absence d'alternatives Dépendance inter-institutionnelle	Impossibilité d'accès aux ressources numériques Blocage des services internes Perturbation des accès distants Augmentation support utilisateurs	3	3	1	3	4	<b>12</b>	Mécanismes d'authentification secondaires Cache local des droits d'accès Procédures dégradées documentées Supervision des services externes	2	2	1	2	3	<b>6</b>	Instantanée	16	Partager				<b>DSI</b>

## Risques politiques et géopolitiques : instabilité réglementaire, sanctions, conflits internationaux.

DIS-R17	Décisions politiques et censure	Changements idéologiques Pressions politiques Restrictions budgétaires Censure gouvernementale	Perte d'accès à des corpus documentaires Épistémicide (destruction sélective du savoir) Autorisations révoquées Auto-censure préventive	2 3 1 4 4 8	Archives locales des ressources critiques Participation à des initiatives de préservation Veille sur les enjeux de liberté académique Implication associations professionnelles	2 2 1 3 3 6	Basse 17	Partager			Rectorat
DIS-R18	Restrictions budgétaires	Crises économiques Priorisation autres secteurs Perception utilité réduite Métriques d'impact limitées	Infrastructure fragilisée Réduction des abonnements Baisse des investissements sécuritaires Perte de compétences (départs) Obsolescence accélérée	3 4 2 3 4 12	Diversification des sources de financement Mutualisation des ressources Priorisation stratégique Automatisation de processus coûteux Démonstration valeur ajoutée	3 3 2 2 4 12	Basse 18	Accepter			Rectorat
DIS-R19	Sanctions internationales	Tensions géopolitiques Mesures de rétorsion Embargo technologique Sanctions économiques	Impossibilité d'accéder à certaines bases de données Blocage des paiements internationaux Restrictions de collaboration Fragmentation des accès	2 3 1 4 4 8	Solutions d'accès alternatives légales Anticipation des changements géopolitiques Documentation des procédures exceptionnelles Mécanismes légaux de contournement	2 2 1 3 3 6	Haute 19	Accepter			Rectorat
DIS-R20	Conflits de propriété intellectuelle	Renforcement droits d'auteur Lobbying éditeurs Décisions jurisprudentielles Fragmentation juridictions	Restrictions nouvelles sur le TDM Augmentation des coûts d'accès Limitations des services aux usagers Complexité légale accrue	2 3 1 4 3 8	Veille juridique active Participation aux consultations publiques Relations avec des spécialistes du droit Politiques d'usage responsable	2 2 1 3 2 6	Instantanée 20	Réduire			Rectorat
DIS-R21	Cyber-conflits et attaques sponsorisées	Recherches sensibles Espionnage industriel Motivations géopolitiques Faible protection relative	Espionnage scientifique Compromission durable des systèmes Perturbations ciblées lors d'événements clés Vol propriété intellectuelle	2 4 2 4 4 8	Collaboration avec les services nationaux SNCS Partage d'informations inter-établissements Surveillance des menaces spécifiques Sensibilisation chercheurs domaines sensibles	1 3 2 3 3 3	Basse 21	Eviter			Rectorat

## Risques internes : erreurs humaines, malveillance interne ou insuffisance des procédures.

DIS-R22	Erreurs humaines	Formation insuffisante Procédures complexes Pression temporelle Interfaces complexes peu intuitives	Perte de données Configurations erronées Expositions accidentelles Interruptions de service Indisponibilité de ressources	4	2	3	2	4	16	Formation continue Procédures avec validations Environnements de test séparés Restauration facile (snapshots) Interfaces utilisateur intuitives	2	2	2	2	3	6	Basse	22	Réduire			Management
DIS-R23	Négligences et Shadow IT	Procédures perçues comme lentes Besoins spécifiques non couverts Méconnaissance des risques Culture organisationnelle	Fuite de données via canaux non surveillés Vulnérabilités non gérées Silos d'information inaccessibles Dépenses cachées	4	3	2	3	4	16	Formation aux risques Solutions flexibles approuvées Processus de validation accélérés Découverte automatisée d'actifs Communication sur les dangers	3	2	2	3	3	9	Basse	23	Eviter			Chef de projet
DIS-R24	Revente, transfert de credentials	Manque de sensibilisation à la sécurité Absence de surveillance des accès Inadéquation des sanctions Faible protection des identifiants	Accès non autorisé aux données Compromission des systèmes Usurpation d'identité Perte de confiance institutionnelle Avertissements des éditeurs Menaces de poursuites	3	3	2	4	4	12	MFA obligatoire (authentification multifactor) Surveillance des accès anormaux Politiques strictes d'usage des comptes Campagnes de sensibilisation régulières Rotation et révocation rapide des credentials	3	2	1	3	3	9	Basse	24	Réduire			Utilisateurs
DIS-R25	Fraudes et sabotage académique	Motivations personnelles (vengeances, notes, ...) Accès privilégiés Contrôles insuffisants Absence traçabilité	Perte d'intégrité des données Perturbation des services bibliothécaires Atteinte à la réputation Perte confiance utilisateurs	2	3	2	4	3	8	Séparation des priviléges Audit des activités sensibles Procédures de signalement protégées Validation multi-niveau Principe du moindre privilège	2	2	1	3	2	6	Haute	25	Réduire			Utilisateurs
DIS-R26	Départs de personnel clé	Veillissement personnel Attraktivité limitée secteur Non-reconnaissance expertise Burnout personnel	Perte de savoir-faire technique Incapacité à maintenir certains systèmes Ralentissement des résolutions d'incidents Perte expertise collections	3	3	2	2	4	12	Documentation systématique Transfert de compétences planifié Formations croisées Recrutements anticipés Valorisation de l'expertise	2	2	2	2	3	6	Haute	26	Réduire			Management
DIS-R27	Conflits internes	Réorganisations mal conduites Communication déficiente Culture en silo Compétition ressources	Blocages décisionnels Rétention d'information Fragmentation des responsabilités Détérioration climat social	3	2	3	4	3	12	Processus de médiation Documentation claire des rôles Canaux de communication transparents Gouvernance formalisée Gestion proactive conflits	3	2	3	2	3	9	Instantanée	27	Accepter			Management

## Risques informationnels : la qualité, la confidentialité, l'intégrité ou la disponibilité des données.

DIS-R28	Vulnérabilité des catalogues	Systèmes uniques centralisés Absence redondance Complexité technique Maintenance insuffisante	Impossibilité de localiser les ressources Perte des liens entre documents Recherche académique entravée Visibilité collections réduite	3 3 2 3 4	12	RéPLICATION DES INDEX Sauvegardes fréquentes des métadonnées Solutions de recherche alternatives APIs de secours Exports réguliers	2 2 1 3 3	6	Instantanée	28	Réduire					DIS
DIS-R29	Altération de l'intégrité des données	Absence vérification intégrité Multiples intervenants Systèmes distribués Migration données défectueuse	Perte de fiabilité des dépôts Citations devenues invalides Problèmes de reproductibilité scientifique Contenus altérés ou perdus	3 4 2 4 3	12	Signatures numériques Journalisation des modifications Checksums réguliers Systèmes WORM (Write Once Read Many) Audits périodiques	2 3 1 3 3	6	Basse	29	Eviter					DIS
DIS-R30	Problèmes de préservation numérique	Absence stratégie pérenne Focus court terme Évolution technologique rapide Sous-estimation risques	Perte irréversible de patrimoine Dégénération progressive invisible Investissements perdus Collections numériques inutilisables	4 4 2 4 4	16	Stratégie OAIS Migrations préventives Diversité des supports Vérifications périodiques d'intégrité Métadonnées de préservation	3 3 2 3 3	9	Basse	30	Réduire					DIS
DIS-R31	Problèmes de droits et licences	Contrats complexes mal négociés Législations changeantes Œuvres orphelines Licences restrictives Dépôts des droits dans un système centralisé (R14)	Risques légaux d'utilisation Conservation compromise Restrictions d'accès imprévues Impossibilité réutilisation	3 3 1 3 2	9	Audit des accords de licence Documentation des droits Participation à RightsStatements.org Clauses de perpétuité négociées Gestion droits numériques	2 2 1 2 2	4	Haute	31	Eviter					DIS
DIS-R32	Dépendance aux identifiants persistants	Modèles financiers instables Architecture centralisée Évolution standards	Liens brisés dans les citations Collections devenues inaccessibles Métadonnées orphelines Travaux de recherche non traçables	2 2 1 3 2	6	Diversification des systèmes d'identifiants Maintenance locale des correspondances Participation aux organismes de gouvernance Tables de correspondance	2 1 1 2 2	4	Basse	32	Accepter					DIS

## Risques opérationnels, logistiques : les processus, l'approvisionnement ou la continuité.

<b>DIS-R33</b>	Chaîne d'approvisionnement	Concentration fournisseurs Crises sectorielles Événements mondiaux disruptifs Faillites distributeurs	Interruption des acquisitions Lacunes dans les collections Retards d'accès aux nouvelles publications Budget inutilisé temporairement	3 3 2 2 3 <b>9</b>	Diversification des fournisseurs Relations directes avec éditeurs Participation à des consortiums Contrats avec clauses de force majeure	2 2 1 2 3 <b>6</b>	Basse 33	Accepter	-
<b>DIS-R34</b>	PCA/PRA insuffisants	Perception risque faible Manque de ressources dédiées Absence exercices réguliers Documentation obsolète	Récupération impossible post-incident Délais de restauration étendus Pertes définitives de services Réactions improvisées inefficaces	4 4 3 4 4 <b>16</b>	Exercices réguliers Documentation à jour Responsabilités clairement attribuées Tests de restauration réels Cellule de crise formée	4 3 2 3 3 <b>12</b>	Instantanée 34	Eviter	Métiers / DSI
<b>DIS-R35</b>	Communication de crise défaillante	Centralisation communication Canaux uniques dépendants SI Absence formation porte-parole Non-implication direction	Information erronée des usagers Panique ou confusion Dégradation de l'image institutionnelle Gestion de crise chaotique	3 2 3 4 3 <b>12</b>	Canaux multiples (SMS, médias sociaux) non-déterminé Porte-paroles formés Messages pré-approvés Contacts presse établis Plan de communication de crise	2 2 2 2 3 <b>6</b>	Haute 35	Réduire	Rectorat
<b>DIS-R36</b>	Problèmes logistiques internes	Locaux inadaptés Processus non optimisés Équipement insuffisant Organisation spatiale déficiente	Retards d'accès aux collections Services dégradés Ressources inaccessibles Frustration utilisateurs	2 2 2 2 3 <b>6</b>	Planification détaillée Communication préventive Alternatives temporaires Implication des usagers Cartographie des processus	2 1 1 2 2 <b>4</b>	Basse 36	Accepter	DIBAT/STEP
<b>DIS-R37</b>	Gestion des accès physiques	Systèmes de contrôle obsolètes Procédures laxistes Multiples accès Absence traçabilité Systèmes antivol défaillant ou centralisé	Vol de ressources Sabotage d'infrastructure Accès non autorisé aux systèmes Vandalisme	3 3 3 3 3 <b>9</b>	Contrôle d'accès par zones Surveillance vidéo Traçabilité des accès Audits de sécurité physique Formation personnel vigilance	2 2 2 2 2 <b>4</b>	Basse 37	Réduire	DIBAT/STEP

## Risques de gouvernance : absence de pilotage stratégique, de cadre normatif, de supervision.

<b>DIS-R38</b>	Perte de contexte et d'intelligibilité	Métadonnées insuffisantes Documentation incomplète Turnover personnel Discontinuité projets	Collections inutilisables Recherche impossible Patrimoine conservé mais inexploitable Perte valeur scientifique	3 3 2 4 3	<b>12</b>	Métadonnées enrichies systématiques Documentation des processus Standards ouverts Préservation des environnements Équipe dédiée qualité métadonnées	3 2 2 4 3	<b>12</b>	Basse	38	Réduire			Rectorat
<b>DIS-R39</b>	Fragmentation des responsabilités	Structures organisationnelles floues Évolutions organisationnelles Réorganisations, silos fonctionnels	Actions contradictoires Zones de non-responsabilité Retards décisionnels en crise Décisions incohérentes, zones grises de responsabilité, inefficacité	3 2 2 2 3	<b>9</b>	Gouvernance partielle, matrices de responsabilité incomplètes /Mise en place d'une matrice RACI, documentation des processus, gouvernance comités transversaux Exercices multiservices	2 2 1 2 2	<b>4</b>	Basse	39	Réduire			Rectorat
<b>DIS-R40</b>	Non-conformité et interopérabilité	Systèmes propriétaires, absence de mapping entre formats	Données piégées dans des systèmes Coûts élevés de migration Perte partielle lors des transferts	3 3 2 3 3	<b>9</b>	Adoption de standards ouverts Tests d'interopérabilité API documentées Métadonnées normalisées	2 2 2 2 2	<b>4</b>	Haute	40	Accepter			Rectorat
<b>DIS-R41</b>	Financement pérenne	Coupes budgétaires, arrêt de projets	Abandon de collections numériques Dégradation progressive non détectée Perte de compétences spécialisées	4 4 2 3 4	<b>16</b>	Modèles économiques diversifiés Mutualisation des coûts Démonstration de la valeur Institutionnalisation des services	4 3 2 3 2	<b>12</b>	Basse	41	Eviter			Rectorat
<b>DIS-R42</b>	Non-conformité réglementaire	Données non anonymisées, absence d'audit Absence de politique de gestion des données	Sanctions financières Atteinte à la réputation Restrictions d'usage imposées retrait de financements, perte de réputation	3 3 2 4 3	<b>12</b>	Veille juridique Audits réguliers DPO impliqué Formation continue	2 2 2 3 2	<b>6</b>	Haute	42	Réduire			Rectorat /Facultés / Metiers
<b>DIS-R43</b>	Qualité des données	Saisies erronées, absence de validation	Ressources introuvables Décisions basées sur données erronées Perte de confiance des usagers Décisions biaisées, perte de confiance usagers, erreurs dans les publications	3 2 2 3 3	<b>9</b>	Contrôles qualité automatisés Enrichissement collaboratif Corrections par lot Outils de détection d'anomalies	2 2 2 2 2	<b>4</b>	Basse	43	Eviter			Rectorat

## Risques émergents : évolutions technologiques, sociétales, environnementales peu maîtrisées.

<b>DIS-R44</b>	Désinformation et manipulations IA	Documents falsifiés, hypertrucage, citations fictives	Remise en cause des sources fiables Difficulté de validation Contamination des corpus, Perte de confiance, désinformation académique	3	3	2	4	3	<b>12</b>	Vigilance humaine, filtrage de base Outils de détection IA Certification des sources Éducation aux médias Préservation des originaux traçabilité des sources	2	2	2	3	2	<b>6</b>	Basse	44	Réduire
<b>DIS-R45</b>	Hyperconnectivité et dépendance IoT	Systèmes RFID, capteurs environnementaux, compteurs	Nouvelles surfaces d'attaque Fuites de données d'usage Perturbations des systèmes automatisés	3	3	2	3	4	<b>12</b>	Segmentation des réseaux IoT Mises à jour automatiques Chiffrement des communications Monitoring comportemental	2	2	1	3	2	<b>6</b>	Haute	45	Accepter
<b>DIS-R46</b>	Quantité massive de données de recherche	Big Data scientifique, simulations haute performance	Stockage insuffisant Préparation impossible Coûts explosifs	3	4	2	3	4	<b>12</b>	Politiques de rétention Infrastructures évolutives Critères de sélection Compression intelligente Politiques de rétention, stockage scalable	2	3	2	3	2	<b>6</b>	Haute	46	Réduire
<b>DIS-R47</b>	Défis des publications numériques dynamiques	Applications web, bases de données vivantes	Impossibilité de citation stable Préparation complexe Versionnage inadéquat	3	3	2	3	3	<b>9</b>	Archivage , Captures instantanées régulières Identifiants pour versions Métadonnées temporelles Documentation des changements	2	2	2	2	2	<b>4</b>	Instantanée	47	Accepter
<b>DIS-R48</b>	Fracture numérique et accessibilité	Publics éloignés, handicaps, fracture socio-économique	Discrimination d'accès Sous-utilisation des services Tensions communautaires	2	2	3	3	2	<b>6</b>	Interfaces multi-modales Services hybrides Formation des publics Conception universelle	2	1	2	2	2	<b>4</b>	Basse	48	Réduire

# Cartographie des risques

Université de Genève

Département : Division de l'information scientifique

Service : Pôle informatique documentaire, Coordination de la division de l'

Date

Validation

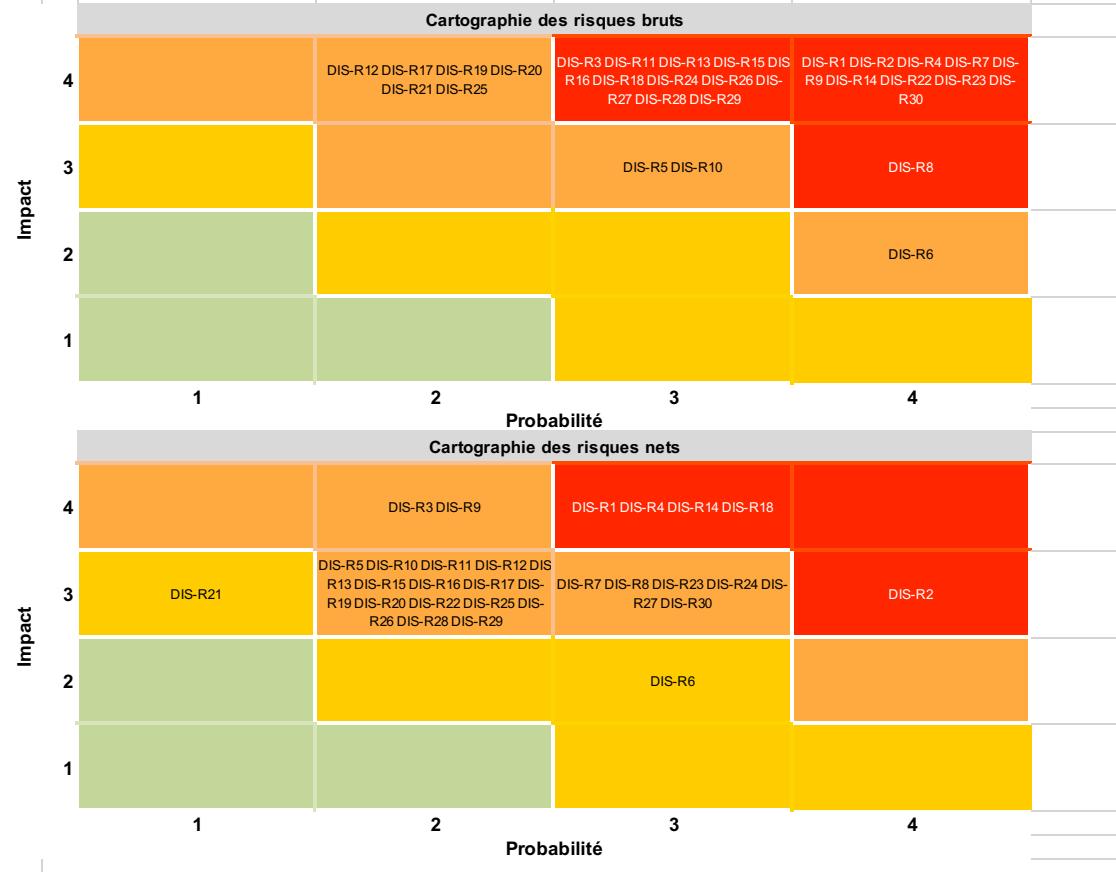
28/04/2025

0

## Mission / objectifs clés du service

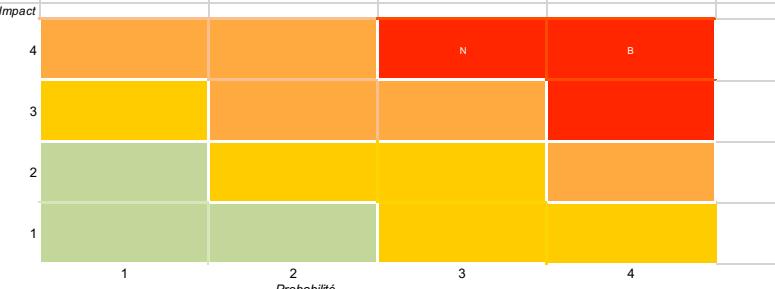
La Bibliothèque de l'Université fournit des ressources physiques et numériques alignées sur les domaines d'enseignement, de recherche et d'excellence de l'institution. Structurée par une politique documentaire validée par le Rectorat, elle combine services sur site et à distance, conserve et diffuse la production scientifique via une Archive ouverte, forme en continu son personnel aux sciences de l'information, gère ses ressources avec efficience et développe des partenariats pour optimiser l'acquisition documentaire.

## A USAGE INTERNE UNIQUEMENT



## Fiche de suivi de risque

**DIS-R1**

<b>Université de Genève</b>				
Département :	Division de l'information scientifique	Date	28/04/2025	
Service :	Pôle informatique documentaire, Coordination de la division	Validé par	0	
Mission / objectifs clés du service				
La Bibliothèque de l'Université fournit des ressources physiques et numériques alignées sur les domaines d'enseignement, de recherche et d'excellence de l'institution. Structurée par une politique documentaire validée par le Rectorat, elle combine services sur site et à distance, conserve et diffuse la production scientifique via une Archive ouverte, forme en continu son personnel aux sciences de l'information, gère ses ressources avec efficience et développe des partenariats pour optimiser l'acquisition documentaire.				
<b>A USAGE INTERNE UNIQUEMENT</b>				
Risque	Ransomware et cryptolocker			
Cause(s)	Phishing réussi Vulnérabilités non corrigées Formation insuffisante du personnel			
Conséquence(s)	Inaccessibilité des catalogues et ressources numériques Perte de données de recherche Interruption des services essentiels			
<b>Cartographie</b>	 <p>Impact</p> <p>Probabilité</p> <p>B = risque brut; N = Risque Net</p>			
Contrôle en place	Sauvegardes régulières hors ligne (stratégie 3-2-1)			
Traitemet du risque	Réduire			
Mesure d'amélioration				
Coût				
Délai				
Responsable du risque	RSSI			
Statut	.....			
<b>Détails</b>				
N° de l'action	Mesure détaillée	Effet escompté	Qui	Quand
<b>Remarques</b>				

## Annexe 17 : Synthèse des risques prioritaires

Scénario	Détail du Risque	Exemples concrets, étude de cas, littérature, entretiens	Lien OWASP Top 10 (2021)	CVSS (indicatif)	Responsable du risque
Ransomware et cryptolocker	Logiciels malveillants qui chiffrent les données et exigent une rançon pour leur déchiffrement	British Library (2023), Paris-Saclay (2024), CERN (attaques déjouées), EPFZ (tentatives) Attaque Xplain, répercussion sur l'administration fédéral	A02: Cryptographic Failures A08: Software & Data Integrity Failures	CVSS 9.8	RSSI
DDoS, DoS	Attaques visant à saturer les serveurs et rendre indisponibles les services en ligne	Université de Zurich (2023), CERN (attaques récurrentes), UNIGE (perturbations périodiques), Internet Archives (2023), Sites de la confédération (NoName)	A05: Security Misconfiguration	CVSS 7.5	RSSI
Intrusion et phishing	Compromission des comptes par vol d'identifiants, souvent via emails frauduleux	British Library (vecteur d'entrée), Université de Zurich (2022), EPFZ et CSCS(2020)	A07: Identification and Authentication Failures A01: Broken Access Control	CVSS 8.8	RSSI
Robots et scrapping IA	Utilisation d'intelligence artificielle pour générer des attaques sophistiquées ou scraper des contenus	British Library (2023), UNIGE (tentatives détectées)	A05: Security Misconfiguration A09: Security Logging & Monitoring Failures	CVSS 5.3	RSSI
Obsolescence technologique	Formats de fichiers, supports ou logiciels devenus inutilisables avec les technologies actuelles	British Library (médias obsolètes), Internet Archive	A06: Vulnerable and Outdated Components	-	DSI
Insuffisance des sauvegardes	Dispositifs de sauvegarde inadéquats ou désactivés lors d'attaques	British Library (sauvegardes compromises), Bibliothèques municipales Seattle, Toronto public library	A08: Software & Data Integrity Failures	CVSS 6.8	DSI
Failite d'éditeurs ou agrégateurs	Disparition de fournisseurs de contenu numérique avec perte d'accès immédiate	EMH (Editeur médecine), Dawsonera	A08: Software & Data Integrity Failures	-	DIS
Dépendance SaaS/IaaS	Services essentiels externalisés soumis aux aléas des prestataires	Ex Libris (Alma/Primo), Maintenance Juillet 2025 (1 jour), Microsoft et Crowdstrike(2024)	A05: Security Misconfiguration A01: Broken Access Control	-	DIS
Erreurs humaines	Manipulations accidentielles pouvant endommager ou compromettre les systèmes	Université de Neuchâtel (2022) – suppression accidentelle de données sensibles non chiffrées ; Leipzig (2021) – mauvaise configuration accès usagers	A01: Broken Access Control A09: Security Logging & Monitoring Failures	-	Management
Négligences et Shadow IT	Utilisation de solutions non approuvées ou contournement des mesures de sécurité	Cas TORTILLA (ESR français) : bases administratives piratées via outils non déclarés, stockage parallèle mal sécurisé Zero-day vulnérabilité	A02: Cryptographic Failures A07: Identification and Authentication Failures	CVSS 6.5	Facultés, Chefs de projets
PCA/PRA insuffisants	Plans de continuité et de reprise d'activité inadéquats ou non testés	Vermont Medical Center (2020) (ransomware, perte d'accès partielle 3 mois)	A04: Insecure Design A09: Security Logging & Monitoring Failures	-	Métiers / DS1
Perte de contexte et d'intelligibilité	Données devenues incompréhensibles par manque de documentation ou de métadonnées	British Library (2023) : perte temporaire de la cartographie des ressources numériques suite à corruption des bases Digital Dark Age, NASA	A08: Software & Data Integrity Failures A05: Security Misconfiguration	-	Rectorat
Financement pérenne	Interruption des dispositifs de préservation numérique par manque de ressources et arrêts des financements des sponsors	Pressions budgétaires continues sur archives nationales numériques ; avertissements sectoriels (Bellini, 2024), BL(2023), Dawsonera Fin de financements Swissuniversities (Lockss)	A04: Insecure Design A06: Vulnerable Components	-	Rectorat

## Annexe 18 : Schéma de données du réplica

Métadonnées bibliographiques issues d'ALMA via OAI-PMH

### Métadonnées descriptives

- Titre (dc:title)
- Auteur / Créeur (dc:creator)
- Contributeurs (dc:contributor)
- Date de publication (dc:date)
- Éditeur (dc:publisher)
- Sujet / Mots-clés (dc:subject)
- Langue (dc:language)
- Description / Résumé (dc:description)
- Type de ressource (dc:type)
- Format (dc:format)
- Identifiants (ISBN, ISSN, DOI, etc.) (dc:identifier)
- Relations avec d'autres ressources (dc:relation)
- Droits / Licence d'accès (dc:rights)
- Source (ex. : catalogue, dépôt institutionnel) (dc:source)

Données issues d'Alma Analytics

#### Licences (ressources électroniques) :

- Licence ID
- Titre de la ressource
- Fournisseur / Éditeur
- Type de licence (abonnement, achat perpétuel, etc.)
- Dates de début et de fin de la licence
- Clauses d'usage (text and data mining, accès distant, archivage, etc.)
- Statut de la licence (active, expirée)
- Périmètre d'accès (utilisateurs autorisés, campus)
- Lien vers le contrat/licence

#### Collections électroniques :

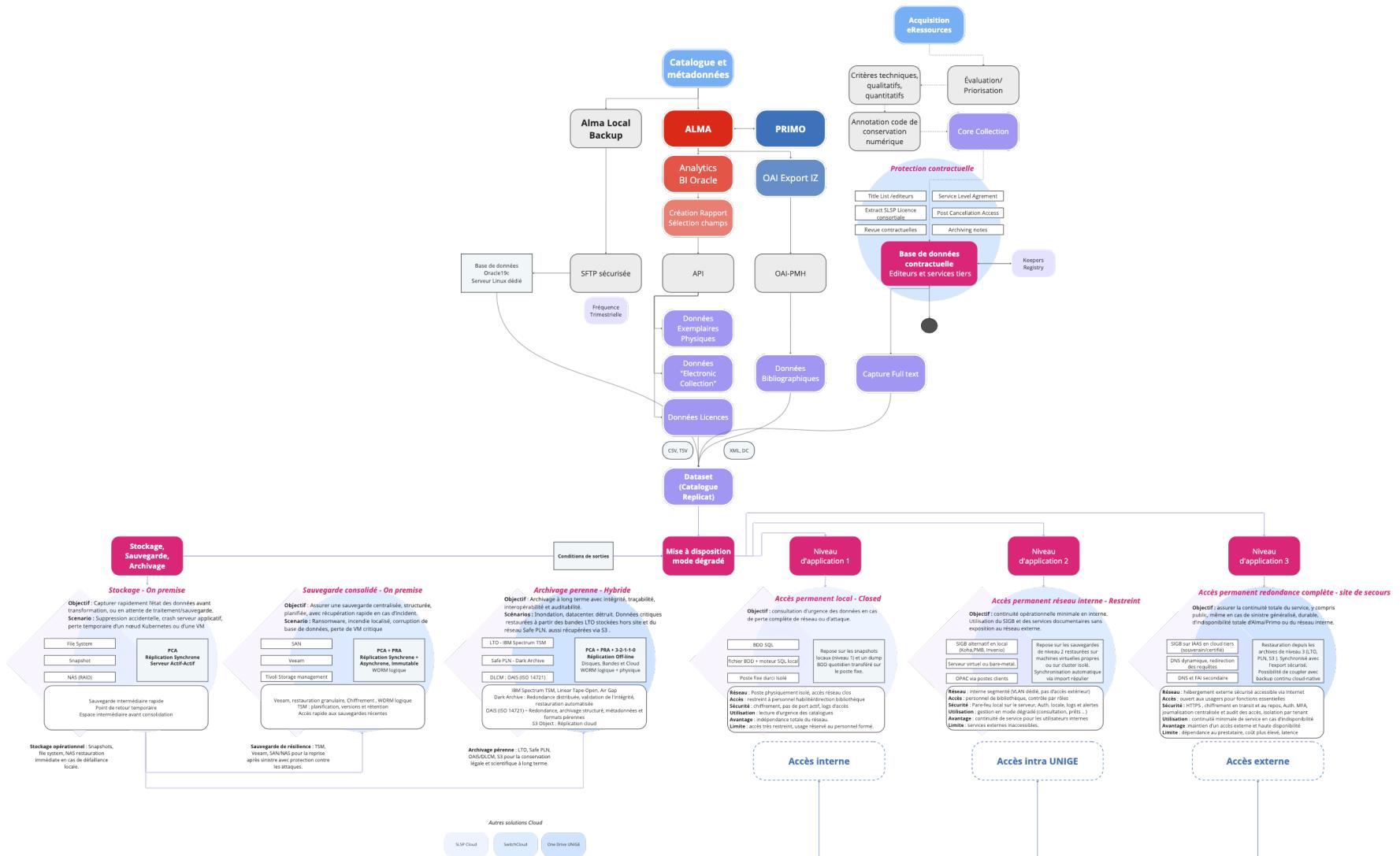
- MMS ID
- ISBN/ISSN
- Nom de la collection
- Fournisseur / Plateforme
- Type de collection (base de données, bouquets, titres isolés)
- Portée disciplinaire

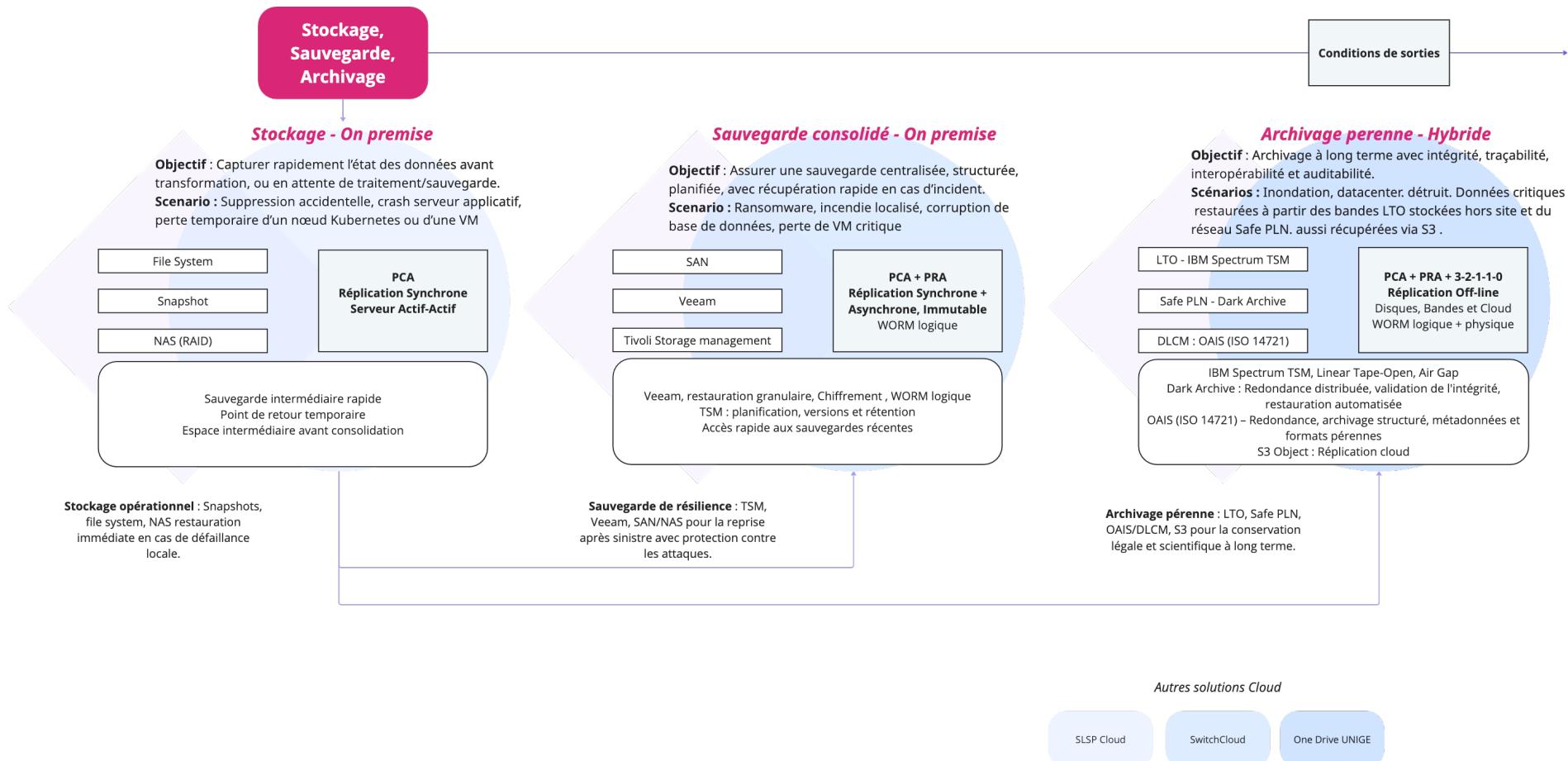
- Nombre de titres
- Mode d'acquisition (abonnement, open access, etc.)
- Statut de disponibilité (actif, supprimé)
- URL d'accès LEVEL
- Niveau de couverture temporelle

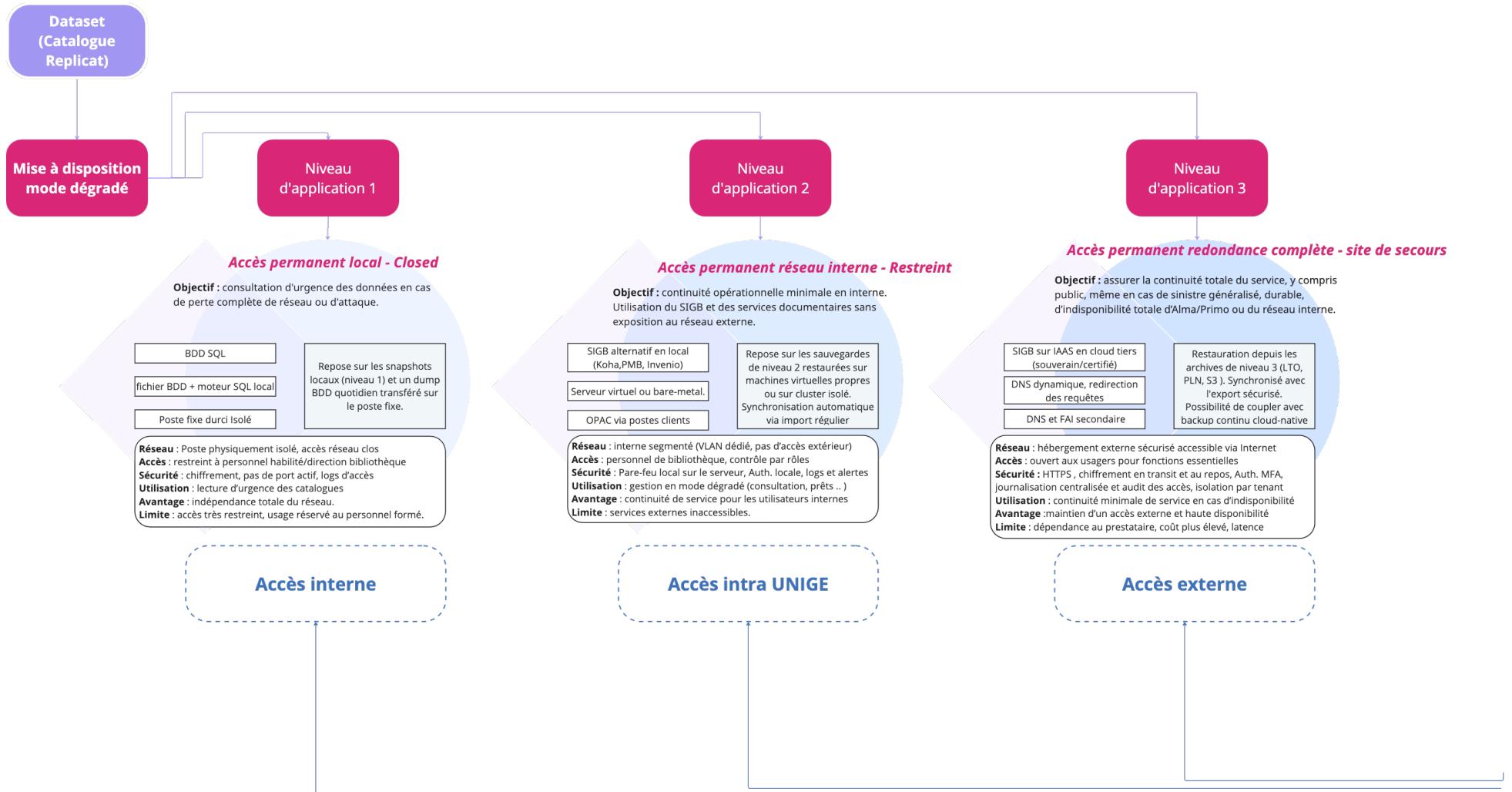
#### **Exemplaires physiques :**

- MMS ID
- Titre
- Localisation (bibliothèque, magasin, site)
- Cote
- Statut de prêt (en rayon, prêté, en traitement)
- Type de document (monographie, périodique, thèse...)
- Nombre d'exemplaires disponibles
- Statut de conservation (ex. : exemplaire de réserve)
- Code-barres / Identifiants internes

# Annexe 19 : Modélisation complète

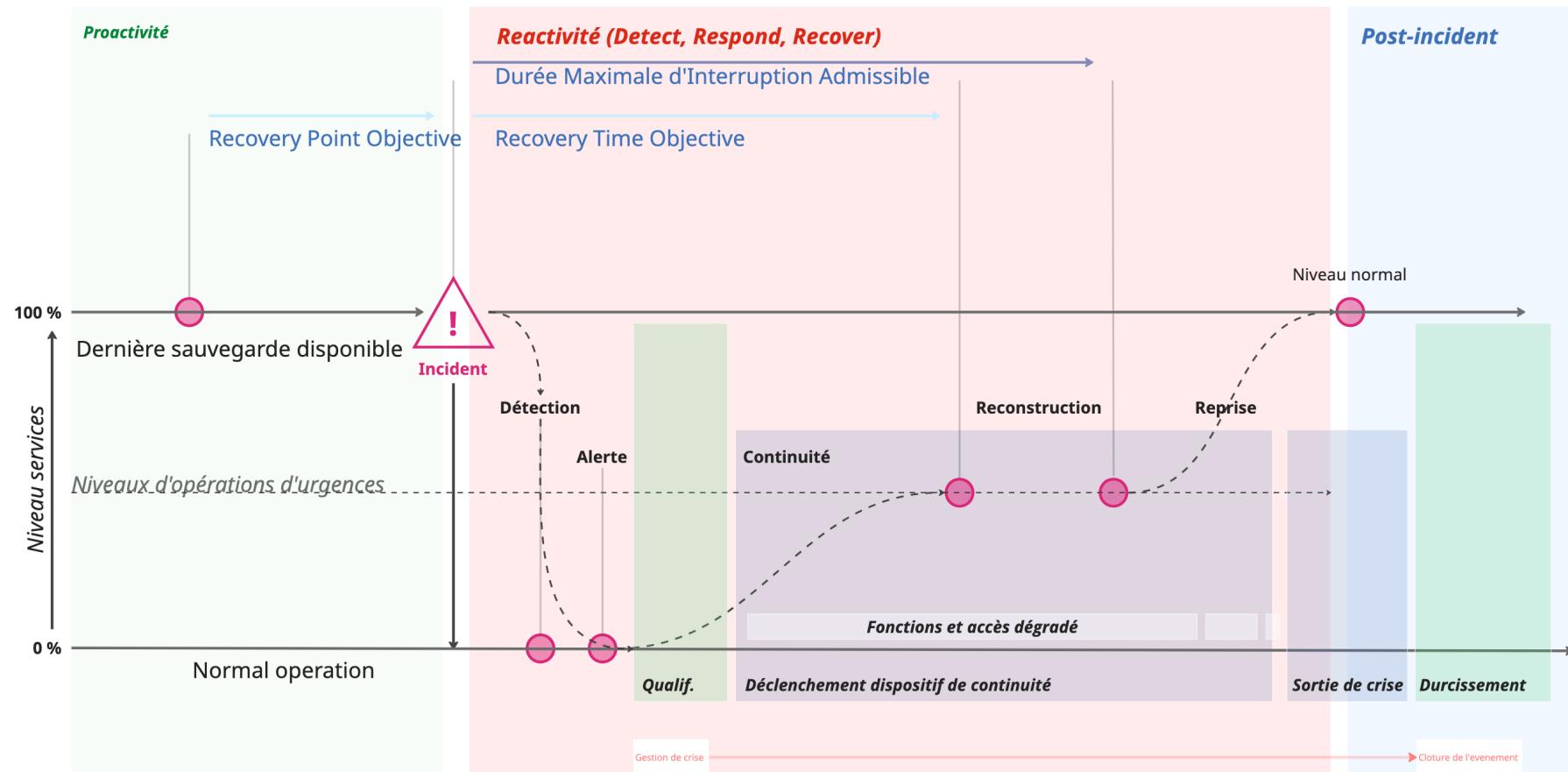






## Annexe 20 : Gestion de crise cyber

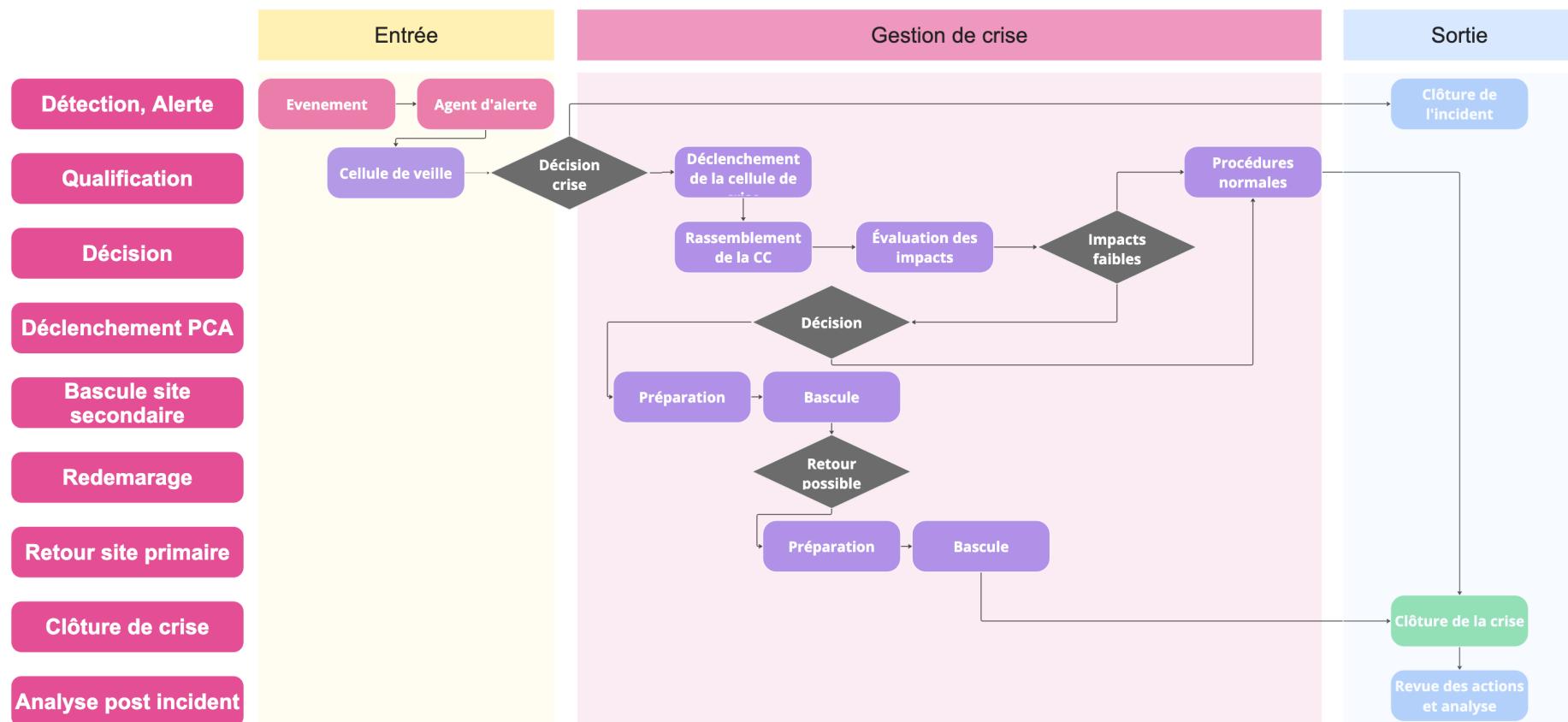
Chronologie, dispositifs de continuité et jalons d'un incident critique



## Niveau de mobilisation et évaluation d'impacts en cas de crise

Niveau d'incident	Description	Communication	Impacts	Exemple
1	Crise cyber critique – attaque majeure paralysant des services essentiels, nécessitant le déclenchement immédiat du PCA/PRA.	Communication officielle vers les usagers, partenaires, autorités et médias. Coordination avec les cellules de crise institutionnelles. Activation d'un canal unique d'information.	Paralysie de plusieurs services critiques ; perte potentielle de données ; atteinte à la réputation ; interruption d'activités pédagogiques ou de recherche. Impact CRITIQUE, combinaison de plusieurs scénarios à effets dominos avec atteinte massive à la continuité	(ex : ransomware à propagation rapide, compromission massive de données, attaque sur les systèmes de sauvegarde)
2	Incident cyber majeur nécessitant la mobilisation d'équipes pluridisciplinaires .	Information ciblée vers les services impactés, la direction, et les parties prenantes internes. Communication structurée pour éviter la panique.	Dysfonctionnement important d'un ou plusieurs systèmes ; risque de perte ou de fuite de données ; mise en œuvre de mesures correctives urgentes. Impact ÉLEVÉ à CRITIQUE, scénario composé ou amplification mutuelle	(ex : compromission d'un serveur stratégique, atteinte à l'intégrité des données, compromission d'identifiants à grande échelle)
3	Incident cyber significatif impliquant des ressources transverses .	Notification interne aux équipes concernées, documentation de l'incident et briefing post-incident. Rapport au RSSI.	Perturbation ponctuelle ou localisée ; impact limité à certains utilisateurs ou services ; menace maîtrisée. Impact ÉLEVÉ, affecte des services critiques de manière circonscrite	(ex : compromission d'un compte administrateur, tentative d'exfiltration de données, malware localisé)
4	Incident cyber modéré géré par une équipe restreinte .	Signalement au RSSI, documentation technique, gestion via les procédures standards.	Impact limité, sans atteinte grave aux données ; gestion en interne par les responsables techniques. Scénario isolé, impact limité, ne déclenche pas de scénario secondaire	(ex : phishing ciblé, détection d'activités suspectes, scan réseau anormal)
5	Situation normale – veille active et gestion quotidienne des alertes de sécurité	Pas de communication externe ; incidents enregistrés dans les outils de gestion et suivis par le SOC interne ou le prestataire MSSP.	Aucun impact ou impact négligeable sur les activités ; maintien des services avec surveillance continue. Activité de surveillance préventive – détection précoce, incidents sans impact significatif	(ex : tentatives de connexion échouées, mises à jour de sécurité, analyse de journaux, Tentatives de scan, phishing isolé, mises à jour critiques).

## Gestion de crise et chaîne de décisions



# Annexe 21 : Fiche d'urgence, attaque par Ransomware



UNIVERSITÉ  
DE GENÈVE

DIVISION DE L'INFORMATION  
SCIENTIFIQUE (DIS)

## Avant l'attaque - Mesures préventives

### 1. Sauvegarde des données

**Objectif :** garantir la disponibilité des données critiques même en cas de chiffrement par un rançongiciel.

- Mettre en place des procédures de sauvegarde régulière des postes utilisateurs, serveurs, applications métier, bases de données.
- Utiliser des supports hors-ligne (bande, disque dur externe débranché) ou du stockage cloud avec versioning.
- Tester régulièrement les procédures de restauration (exercice de restauration intégrale simulée).
- Séparer physiquement ou logiquement les sauvegardes de l'environnement de production.
- Identifier les données critiques à sauvegarder prioritairement.
- Conserver plusieurs versions des sauvegardes (réttention).

### 2. Mise à jour des systèmes et des logiciels

**Objectif :** corriger les vulnérabilités connues avant leur exploitation.

- Maintenir à jour tous les systèmes d'exploitation et logiciels (navigateurs, clients mail, Java, PDF, etc.).
- Suivre un calendrier de mise à jour formalisé (patch management).
- Identifier et isoler les équipements ne pouvant pas être mis à jour (par exemple pour raisons de compatibilité).
- Documenter les versions logicielles installées dans un inventaire à jour.
- Surveiller les alertes de sécurité via des sources officielles (OFCS, éditeurs, Switch, RSSI).

### 3. Sécurisation des postes et serveurs

**Objectif :** réduire la surface d'attaque.

- Installer un antivirus/antimalware sur tous les équipements (et vérifier son fonctionnement).
- Utiliser des outils de détection comportementale (EDR).
- Restreindre les droits d'exécution de programmes (stratégie AppLocker, SRP).
- Supprimer les comptes inutilisés ou sur-privilégiés.
- Appliquer les principes de sécurité par défaut (tout ce qui n'est pas explicitement autorisé est interdit).

### 4. Cloisonnement du système d'information

**Objectif :** limiter la propagation d'un rançongiciel.

- Segmenter le réseau par zone fonctionnelle ou niveau de sensibilité.
- Mettre en place des règles de filtrage interzones (via pare-feu, ACL...).
- Empêcher la communication latérale entre postes utilisateurs.
- Créer des VLAN séparés pour l'administration, les utilisateurs, les serveurs critiques.

## 5. Maîtrise des accès Internet

Objectif : empêcher les communications entre le rançongiciel et les serveurs de commande.

- Utiliser un proxy avec filtrage d'URL.
- Activer la surveillance DNS pour détecter les résolutions suspectes.
- Limiter les postes autorisés à se connecter à Internet.
- Bloquer les connexions sortantes non nécessaires.

## 6. Journalisation et supervision

Objectif : détecter précocement une compromission.

- Activer la journalisation des événements critiques (authentifications, accès aux fichiers, modifications système).
- Centraliser les logs dans un SIEM ou une solution équivalente.
- Mettre en place des alertes sur les comportements anormaux.
- Analyser régulièrement les logs à des fins de détection proactive.

## 7. Sensibilisation et formation

Objectif : faire du facteur humain une ligne de défense.

- Former tous les collaborateurs à la détection des e-mails de phishing, aux règles d'hygiène numérique.
- Distribuer des supports pratiques (guides, affichettes).
- Organiser des campagnes internes de sensibilisation.
- Former les administrateurs aux bonnes pratiques avancées.

## 8. Planification et gouvernance

Objectif : être prêt à agir efficacement.

- Définir une stratégie de communication interne/externe en cas d'incident.
- Constituer une cellule de crise avec rôles et responsabilités clairs.
- Prévoir des moyens de communication de secours/alternatifs hors SI (téléphones, radio, documents papier, outils autonomes).
- Évaluer les offres d'assurance cyber selon les besoins.
- Tous les documents critiques doivent être imprimés, consultables sans SI, stockés en lieu sûr. Les schémas d'architecture du SI, la cartographie des flux réseau, l'inventaire des actifs, avec indication du propriétaire, du métier associé, et du niveau de sensibilité.

# Pendant l'attaque – Réaction immédiate

## 1. Isolement et confinement

Objectif : stopper la propagation.

- Déconnecter immédiatement les postes suspects du réseau (filaire et sans-fil).
- Couper l'accès Internet de l'organisation (routeur, pare-feu).
- Interdire l'usage des supports USB, disques durs externes.
- Isoler les systèmes encore intacts pour éviter une contamination secondaire.
- Éteindre les équipements non utilisés.

## **2. Journalisation des actions (main courante)**

Objectif : conserver un historique précis.

- Ouvrir une main courante dès détection de l'incident.
- Renseigner pour chaque événement : date/heure, auteur, action ou constat.
- Utiliser ce document pour les comptes rendus, les démarches judiciaires, l'assurance et le RETEX.

## **3. Préservation des preuves**

Objectif : permettre l'investigation.

- Ne pas formater les machines infectées.
- Conserver les fichiers chiffrés et les messages de rançon.
- Envisager une image disque des postes critiques.
- Si possible, activer la mise en veille prolongée pour préserver la mémoire.

## **4. Pilotage de crise**

Objectif : coordonner efficacement les actions.

- Activer la cellule de crise avec l'ensemble des parties prenantes.
- Définir un plan d'action immédiat : cloisonnement, communication, sauvegarde des preuves, reprise partielle.
- Identifier les priorités métier à restaurer.

## **5. Communication maîtrisée**

Objectif : gérer l'information et rassurer.

- Appliquer la stratégie de communication définie.
- Informer en interne les utilisateurs sur les consignes à suivre.
- Centraliser toute sollicitation extérieure (médias, clients, autorités) vers le service communication.
- Prévoir un message public clair, sans divulgation sensible.

## **6. Recherche d'assistance**

Objectif : mobiliser des experts externes si nécessaire.

- Contacter les prestataires spécialisés (forensic, restauration, juristes).
- Contacter l'OFCS, Switch CERT, Task force VdG
- Informer l'assureur en cas de contrat cyber.

## **7. Dépôt de plainte**

Objectif : enclencher la procédure judiciaire.

- Rassembler les éléments techniques : fichiers chiffrés, adresse de rançon, logs, détails de la compromission.

- Préparer une délégation de pouvoir signée si la plainte est portée par un représentant autre que le dirigeant.
- Déposer plainte auprès de la police cantonale

## 8. Ne pas payer la rançon

Objectif : ne pas encourager le modèle économique des cybercriminels.

- Aucune garantie de récupération des données.
- Risque d'arnaque secondaire ou de réattaques.
- Position de principe des autorités (OFCS) contre le paiement.

# Après l'attaque – Restauration et reconstruction

## 1. Restauration du système

Objectif : repartir sur des bases saines.

- Réinstaller les machines depuis des sources fiables (ISO vérifié, image de référence).
- Restaurer uniquement les sauvegardes antérieures à l'infection, après vérification.
- Éviter toute réutilisation de système potentiellement contaminé.
- Supprimer les fichiers suspects, entrées de registre ou backdoors identifiés.

## 2. Sécurisation post-crise

Objectif : empêcher une nouvelle compromission.

- Appliquer les correctifs de sécurité sur tous les systèmes restaurés.
- Changer tous les mots de passe (comptes locaux, AD, outils SaaS).
- Révoquer les accès non utilisés ou suspects.
- Mettre en place un durcissement des configurations restaurées.

## 3. Analyse post-mortem (RETEX)

Objectif : tirer les enseignements de la crise.

- Organiser une réunion de retour d'expérience multidisciplinaire.
- Analyser l'origine de l'attaque, les délais de réaction, les défaillances.
- Mettre à jour le plan de réponse aux incidents et la documentation de crise.
- Planifier une campagne de sensibilisation à la suite de l'incident.

### Références :

ANSSI, 2020. *Atttaques par rançongiciels, tous concernés. | Comment les anticiper et réagir en cas d'incidents ?* [en ligne]. Agence nationale de la sécurité des systèmes d'information. Disponible à l'adresse : <https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concerne> [consulté le 6 mars 2025].

ANSSI, AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, 2021. Crise cyber, les clés d'une gestion opérationnelle et stratégique | ANSSI. [en ligne]. 6 décembre 2021. Disponible à l'adresse : <https://cyber.gouv.fr/publications/crise-cyber-les-cles-dune-gestion-operationnelle-et-strategique> [consulté le 6 mars 2025].

CIGREF, 2023. *Cigref - Réagir à une cyberattaque massive - Février 2023* [en ligne]. Paris. Réagir à une cyberattaque massive . Disponible à l'adresse : <https://www.cigref.fr/reagir-a-une-cyberattaque-massive> [consulté le 6 mars 2025].

DDPS, Département fédéral de la défense, de la protection de la population et des sports, 2024. *Mesures contre les attaques par rançongiciel* [en ligne]. Berne : Office Fédéral de la Cyber Sécurité OFCS. Disponible à l'adresse : <https://www.ncsc.admin.ch/ncsc/fr/home/strategie/berichte-und-studien.html> [consulté le 5 mars 2025].

## Annexe 22 : Scénarios de crise

ID	Nom du scénario	Type (Catégorie)	Actif métier impacté	Dépendance (Intra, Appli, Data)	Processus métiers DIS	Scénarios d'attaque détaillés				Conséquences détaillées	TTP MITRE ATT&CK	Mitigation MITRE DEFEND	Correspondances R-DIS	Risque ENISA	Mesures de sécurité renforcées	Réponse par niveau de sauvegarde	Mode d'accès en degrée possible	
						Scénario 1	Scénario 2	Scénario 3	Scénario 4									
						Défaillance contractuelle :	Défaillance contractuelle :	Défaillance contractuelle :	-									
S1	Rupture de contrat ou défaillance Alma / SLA / RISQS dépendances	SaaS / Contractuel (Risques dépendances)	Catalogue, accès lecteur, gestion documentaire	API Alma (cloud), Réseau (DNS, pare feu), Identity Manager	Accès aux ressources électroniques, Services aux usagers, Services de recherche spécialisées et soutien à la recherche	- Panne détectrice Cubitus (incendie, inondation) - Corruption base de données centrale - Attaque DDoS massive sur infrastructure - Erreur de mise à jour critique	- Panne détectrice Cubitus (incendie, inondation) - Corruption base de données centrale - Attaque DDoS massive sur infrastructure - Erreur de mise à jour critique	- Panne détectrice Cubitus (incendie, inondation) - Corruption base de données centrale - Attaque DDoS massive sur infrastructure - Erreur de mise à jour critique	- Conflit juridique bloquant l'accès	Perte d'accès immédiate aux notices, impossibilité de circulation (prélevement), Perte stratégie des transactions, Impact sur usagers actifs, Coût et complexité de migration	T1199- Trusted Relationship T1584- Compromise Infrastructure	D3-DA- Data Backup D3-SP- Software Process and Device Rules D3-U- DNS Denylisting	Faillite d'éditeur ou agresseurs, Dépendance SaaS/ISaaS, Problème de droits et licences, Restrictions budgétaires, Décisions politiques et censure	Third-party dependency risk Service availability/risk Vendor lock-in	E-export automatisé - Clauses de pertinabilité contractuelle - SIA avec pénalités (>95%) - PCA/méier avec solution dégradée - Surveillance continue des performances - Solution de secours (Koha/PBS)	Niveau 3 (archives, redondance PUN, solutions failback)	Z Réseau interne (mode secours) ou Z, auxCloud	
S2	Corruption des métadonnées dans Alma	SaaS / Intégrité (Risques informationnels)	Notices, préf, recherche	API Alma (cloud), Réseau (DNS, pare feu), Identity Manager	Accès aux ressources électroniques, Services aux usagers, Services de recherche spécialisées et soutien à la recherche	- Attaque interne maintenance : - Emploi mécontent avec droits administrateurs - Modification massive via API automatisée - Suppression sélective de collections sensibles - Insertion de contenus inappropriés/malveillants	- Attaque interne maintenance : - Import de fichier corrupt (CSV mal formaté) - Script de mise à jour défaillant - Fusion erreure de notices doublons - Mauvaise manipulation interface d'admin	- Attaque externe ciblée : - Import de fichier corrupt (CSV mal formaté) - Script de mise à jour défaillant - Fusion erreure de notices doublons - Mauvaise manipulation interface d'admin	- Attaque par déni d'intégrité (data poisoning)	Altération de notices bibliographiques, Erreurs de localisation physique, Faute disponibilité/ridicibilité, Impact recherche et discoverability, Temps de correction	T1555-001- Data Manipulation T1485- Data Destruction T1138- Create Account	D3-BA- Backup and Recovery D3-CP- Credential Stuffing Prevention D3-U- User Account Lifecycle	Altération de l'intégrité des données, Intrusion et phising, Erreurs humaines, Négligences et Shadow IT, Problèmes de préservation numérique	Data integrity threats Software vulnerabilities Privilege escalation	E-export avec vérification d'intégrité - Sandbox pour tests et mise à jour - Gestion des droits de profil (principe moindre privilège) - Versionnages des modifications massives - Contrôles de cohérence automatisés - Formation utilisateurs sur bonnes pratiques	Niveau 2 (sauvegarde immuable) + Niveau 3 (corruption massive)	Z Réseau interne	
S3	Indépendance de Primo / Neo/Swisscovery	SaaS / Disponibilité (Risques technologiques et infrastructure)	Catalogue public, accès distant	Primo VE (cloud), Réseau, Réseau (DNS, pare-feu), Identity Manager	Accès aux ressources électroniques, Services aux usagers, Accès aux ressources électroniques+ Services aux usagers	- Attaque DDoS coordonnée : - Burnet colant spécifiquement les serveurs Primo - Saturation bande passante (> 100 Gbps) - Attaque applicative (HTTP flood)	- Attaque DDoS coordonnée : - Burnet colant spécifiquement les serveurs Primo - Saturation bande passante (> 100 Gbps) - Attaque applicative (HTTP flood)	- Incident technique majeur : - Panne détectrice fournisseur cloud - Corruption base d'index Solr/Elasticsearch - Bug critique lors mise à jour Primo	-	Couper recherche pour usagers distants, impact sur recherches (web), Perte de visibilité collections, Frustration usagers et perte de trafic, Impact pédagogique	T1498- Network Denial of Service T1499- Endpoint DoS T1595-002- Transmitted Data Manipulation	D3-NTF- Network Traffic Filtering D3-ATR- Relay Pattern Recognition D3-U- User Account Monitoring	DoS, DDoS, Défaillances réseau, Dépendance SaaS/ISaaS, Décisions politiques et censure, Cyber-conflits et attaques sponsorisées, Robot et scraping/IA	Availability attacks DDoSattacks Service disruption	- Portail minor avec catalogue statique - Communication de crise multi-canal - Monitoring 24/7 avec alertes - Page de statut publique - Solution de recherche dégradée (OPAC simple) - Cache local des recherches fréquentes	Niveau 3 (failback, archives, OPAC simple)	Z Réseau interne, 3, auxCloud	
S4	Compromission de comptes	Cybersecurité / Authentification (Risques cyber)	Comptes admin, données usagers	Identity Manager, Switch EdUD, API Alma, SEMV / SOC	Accès aux ressources électroniques, Services aux usagers, Dépôts de données de recherche, Dépôts de publications	- Attaque à force brute sophisticated : - Credential stuffing avec bases de données compromises - Attaque dictionnaire adaptée (AL穷举) - Rotation IP via botnet pour éviter détection - Exploitation absence de RPA/CAPTCHA	- Attaque à force brute sophisticated : - Credential stuffing avec bases de données compromises - Attaque dictionnaire adaptée (AL穷举) - Rotation IP via botnet pour éviter détection - Exploitation absence de RPA/CAPTCHA	- Ingérence sociale ciblée : - Spam-phishing par personnel - Man-in-the-middle sur connexion WiFi	- Attaque technique avancée : - Man-in-the-middle sur connexion WiFi - Fausse technique Exhibitor - Prétendant être un collègue/prestataire - Compromission physique (phisher surfing)	- Menace intime : - Admin système avec arrière-péries - Keylogger sur poste compromis - Session hijacking via XSS/CORS - Exploitation vulnérabilité 0-day API	- Accès non autorisé aux données personnelles, Modification suppression de notices, Vol d'identifiants, Violation LD, Atteinte réputation et confiance, Arrêt services pendant investigation	T1078- Valid Accounts T1101- Brute Force T1555- Credentials from Password Stores T1807- Account Discovery T1552-001- Credentials In Files	D3-MFA- Multi-factor Authentication D3-U- User Account Lifecycle D3-CA- Login Analysis D3-CP- Credential Stuffing Prevention	Intrusion et phishing, Revente/transfert de credentials, Fraude et sabotage académique, Erreurs humaines, Négligences et Shadow IT	Identify and access management Credential compromise Privilege escalation Data breaches	- MFA obligatoire pour tous les comptes admin - Rotation automatique des clés API - Rôle et privilégiés par fonction métier - Journalisation détaillée avec SEM - Détection d'anomalies comportementales - Coffre-fort (Vault) - Tests de pénétration	Niveau 2, Niveau 3 (reconstruction)	Z Réseau interne
S5	Perte d'accès au bâtiment ou réseau/local (Risques opérationnelles et logistiques)	Accès physique, réseau, services locaux	Réseau/cœur / Core Switches, WAN interne, DNS, Pare-feu, Ordinateurs, Générateurs, Accès physique	Accès physique, Réseau services locaux	Tous les processus (impact transversal) en particulier : Accès aux ressources électroniques, Services aux usagers, Dépôts de données de recherche, Dépôts de publications	- Catastrophe naturelle : - Inondation, coupure technique/serveurs - Incendie dévastant infrastructure réseau - Tempête/orage couplant alimentation longue durée - Séisme endommageant bâtiment	- Incident de sécurité : - Coupure électrique générale (>24h) - Panne climatisation avec surchauffe serveurs - Rupture liaison Internet principale - Tempête/orage couplant alimentation longue durée	- Panne technique majeure : - Grève avec occupation des locaux	- Confit social : - Grève avec occupation des locaux	- Fermeture complète des services (prêt) Personnes sans accès aux outils	T1209- Hardware Additions T1501-002- BusinessRelationships T1102- Web-Service	D3-NTF- Network Traffic Filtering D3-EC- Encrypted Channels D3-SP- Software Process and Device Rules	Catastrophes physiques et climatiques, Problèmes d'alimentation électrique, Défaillances réseau, Natural disasters Inside threat Business continuity risks	Infrastructure attacks Physical security threats Natural disasters Inside threat Business continuity risks	- PCA local avec site de repli - VPN sécurisé pour télétravail - Documentation accessible en ligne - Accords avec bibliothèques partenaires - Kit de communication d'urgence - Solutions mobiles (4G/5G backup) - Tests PCA annuel	Niveau 3 (reconstruction depuis site distant)	Z, auxCloud	
S6	Perte d'accès aux ressources électroniques (Risques cyber)	Bases éditeurs, portail ressources	OpenAthens, DNS, Réseau (WAN/LAN), Plateformes éditeurs, Infrastructure proxy	Accès aux ressources électroniques, Services aux usagers, Accès aux ressources électroniques+ Services aux usagers, Services de recherche spécialisées	Changement modèle économique : - Passage à un modèle pay-per-use - Suppression tarifs consommateurs - Augmentation tarif bruto - Nouvelles restrictions d'usage (P, simulatej) - Fin des archives perpétuelles gratuites	- Défaillance proxy : - Détection usage "anormal", blocage IP	- Problème d'authentification : - Panne annuelle LDAP/Active Directory - Certificats OpenAthens ou Shibboleth expirés	- Attaque cible : - Man-in-the-middle sur connexions proxy - Violation des conditions d'utilisation - Suspension de partage non autorisé - Robo/crawler mal configuré générant trafic - Bug/exploit lors mise à jour proxy - Expiration certificats non renouvelés	- Couper accès bases de données, Impact direct sur recherche/pédagogie, Perturbation services extérieurs, Contournement par voies illégales, Degravitation image qualité service	T1099- Proxy T1138- External Remote Services T1078-004- Cloud Accounts	D3-NTF- Network Traffic Filtering D3-U- User Account Monitoring D3-U- Local Account Monitoring	DoS, DDoS, Défaillances des fournisseurs d'identité, Faillite d'éditeur ou agresseurs, Restrictions budgétaires, Dépendance SaaS/ISaaS, Robots et scraping/IA	Authentication bypass Network security failures Third-party service disruption	- Monitoring proxy avec seuil d'alerte - VPN institué pour le backup - Cache local des articles populaires - Documentation alternative (archives locales) - Support utilisateur renforcé - Tests réguliers de connectivité - Accord SIA avec hébergeur proxy	Niveau 2, Niveau 3 (failback/Cloud)	Z Réseau interne		
S7	Evolution restrictive d'une licence éditeur	Contractuel / Financier (Risques dépendances)	Accès aux revues	Contrats éditeurs, Plateformes éditeurs (cloud), Réseau, DNS, Réseau	Acquisition des ressources électroniques, Accès aux ressources électroniques, Services de recherche spécialisées	- Changement modèle économique : - Nouvel éditeur revire conditions - Concentration marché aug. renouvellement - Tarif domine - Harmonisation vers tarifs les plus élevés - Suppression de certaines collections	- Rachat/édition d'éditeur : - Désaccord sur conditions de renouvellement	- Evolution technique : - Passer à une nouvelle plateforme, abandon support ancienne version - Incompatibilité avec systèmes existants - Personnalisation sur contenu - Non-paiement par contrainte budgétaire	- Confit institutionnel : - Nouvel éditeur revire conditions - Concentration marché aug. renouvellement	- Couper brutalité de collections stratégiques, Impact pédagogique immédiat, Coût de rebonnement majoré, Liens contractuels, Perte d'historique de recherche, Nécessité solutions alternatives urgentes	T1199- Trusted Relationship T1584- Compromise Infrastructure	D3-SP- Software Process and Device Rules D3-U- Data Backup	Faillite d'éditeur ou agresseurs, Confits de propriété intellectuelle, Restrictions budgétaires, Dépendance SaaS/ISaaS, Décisions politiques et censure	Third-party dependency risk Contract and legal risks Financial constraints	- Archivage local systématique (droits réservés) - Causes perpétruelles dans contrats - Négociation consulaire (mutualisation) - Veille juridique et tarifaire - Solutions Open Access prioritaires - Relations diversifiées éditeurs	Niveau 3 (archives, SPN, backups, solutions alternatives)	Z Réseau interne	

S8	Fuite de données personnelles (LPO)	Protection des données (Risque cyber / Risques informationnels)	Fichiers usagers, formulaires	H365 / OneDrive, Bases de données (Oracle, MSSQL, PostgreSQL, MariaDB), Réseau, ADFS / Identity Manager	Accès aux ressources électroniques, Services aux usagers, Dépôts de données de recherche, Dépôts de publications	<b>Cyberattaque externe :</b> - Ransomware avec infiltration préalable - Exploitation vulnérabilité serveur web - Attaque API avec persistance long terme - Compromission par supply chain - Attaque via IoT mal sécurisé (imprimantes)  <b>Négligence/fourre humaine :</b> - Email avec pièce jointe non chiffrée - Publication accidentelle sur site web - Sabotage avant départ (ex-employé) - Mauvaise configuration serveur (indexation) - USB portable perdu contenant données sensibles - Logs système contenant données sensibles - Bug applicatif exposant données publiées	<b>Maintenance interne :</b> - Sauvegarde non chiffrée - Vol de données pour usage personnel - Base de données exposée sans authentification - Logs système contenant données sensibles - Bug applicatif exposant données publiées	<b>Défaillance technique :</b> - Sauvegarde non chiffrée - Attente réputation durable, Coûts juridiques et techniques, Perte de confiance communautaire, Impact sur partenariats	T1005 - Data from Local System T1039 - Data from Network Shared Drive T1048 - Extrusion Over Alternative Protocol T1041 - Extrusion Over C2 Channel T1042 - File Integrity Analysis	D3-DA - Data Backup D3-NFD - DNS Denying D3-NTF - Network Traffic Filtering D3-PA - File Integrity Analysis	Efiltration et publication de données, Ransomware et cryptolocker, Intrusion et phishing, Erreurs humaines, Fraudes et sabotage académique, Revente/transfert de crédentiels	Data breaches Phishing violations Regulatory compliance failures Revente/transfert de crédentiels	Anonymisation/ pseudonymisation systématique Chiffrement bout-en-bout des exports Limitation drastique des extractions Audit annuel externe Formation pour tous les agents Registre des traitements à jour Procédure incident OFCS documentée	Niveau 2 (rollback, investigation), Niveau 3 (archives immuables)	2. Réseau interne
S9	Indisponibilité d'un personnel clé	Organisationnel / RH (Risques internes / Risques gouvernance)	Compétences	Github, Fedora, DCLM, SharePoint, Identity Manager, Réseau	Tous les processus indirectement (pointant au métier), en particulier : Services aux usagers, Services de recherche spécialisées, Dépôts de données de recherche	<b>Départ imprévu d'un expert métier ou technique :</b> - Démission soudaine sans transfert de compétences sans archive de ses données - Départ en retraite mal anticipé - Accident grave empêchant la reprise immédiate - Maladie grave avec arrêt prolongé - Décès brutal d'un personnel clé - Absence de documentation sur les processus spécialisés	<b>Situation de crise sociale ou RH :</b> - Mouvement de protestation avec arrêt de travail prolongé - Congé maternité / paternité prolongé - Climat social dégradé entraînant absentéisme massif - Départs collectifs non anticipés - Retards dans le recrutement et blocage RH	- Bloage processus métier spécialisé - Pertes savoir-faire technique - Retard projets stratégiques - Surcharge équipes restantes - Risque d'erreurs de méconnaissance - Coût remplacement/formation	T1591-001 - Identity Roles T1598-001 - Credentials T1087-002 - Domain Account	D3-UL - User Account Lifecycle D3-SPP - Software Process and Device Rules	Départs de personnel clé, Confits internes, Fragmentation des responsabilités, PCA/PRA insuffisants, Problèmes de préservation numérique (perte savoir-faire)	Human resource risks Knowledge management failures Business continuity threats	Documentation exhaustive des procédures Formation croisée obligatoire (2 pers/poste) Cartographie des compétences critiques Contrats de filance/contrat d'urgence Plan de succession formalisé Transfert de connaissances structuré Évaluation continue des risques RH	Non lié à la sauvegarde mais archivage de son environnement de travail, PCA RH	1. Local isolé, 2. Réseau interne
S10	Ransomware ciblé (double extension)	Cyber sécurité / Cyberattaque MAJURE (Risque cyber)	Bases de données, fichiers utilisateurs, identifiants, backups	Active Directory (MSAD), Identity Manager, ADFS, SIEM / SOC, Backup TSM / Tape / Veeam, SAN / NAS / S3	Tous les processus fortement impactés – priorité : Accès aux ressources électroniques, Services aux usagers, Dépôts de données de recherche, Dépôts de publications	<b>Ransomware avec infiltration :</b> - Infection via phishing - Movements latéraux dans le réseau - Chiffrement des données critiques - Extrusion de données sensibles vers des serveurs externes - Effacement ou sabotage des logs pour masquer la compromission	<b>Double extension :</b> - Menace explicite de publication des données volées sur le darkweb - Maintenance d'un accès persistant sur l'infrastructure (backdoor active) - Demande de rançon pour fournir la clé de déchiffrement - Demande de rançon complémentaire pour suppression des sauvegardes - Infection des systèmes de sauvegarde des copies - Publication partielle de preuves pour accentuer la pression (échantillons sur forums de leaks)	<b>Persistence et réinfection post-sauvegarde :</b> - Maintien d'un accès persistant sur toute masse de données personnelles, Risques LPO, perte réputationnelle majeure, Coûts élevés de récupération / reconstruction	T1566-001 - Phishing Spearphishing Attachment T1566-002 - Phishing Spearphishing Link T1021-001 - Remote Services Remote Desktop Protocol (RDP) T1489 - Data Encrypted for Impersonation T1048 - Extrusion Over C2 Channel T1048-003 - Extrusion Over Alternative Protocol T1041 - Extrusion Over C2 Channel T1042 - File Integrity Analysis T1042-001 - Indicator Removal on Host T1589-002 - Gather Victim Identity Information T1586 - Dynamic resolution T1584-004 - Compromise Infrastructure T1102-002 - Web Service: Dead Drop Resolver T1005 - Process Injection T1543-003 - Create or Modify System Process T1005-003 - Server Software Component: Web Shell T1078 - Valid Accounts	D3-MFA - Multi-factor Authentication D3-UU - User Account Lifecycle D3-NTF - Network Traffic Filtering D3-DA - Data Backup D3-UL - User Account Lifecycle D3-PA - File Integrity Analysis D3-HA - Hardware Component Inventory Analysis D3-DG - Data Segmentation D3-OCS - Data Content Separation D3-BAC - Backup and Recovery D3-ITR - Integrity Testing and Policy Rules D3-EDR - Endpoint Detection and Response D3-SPN - Software Patch Analysis D3-PRM - Privileged Role Management	Ransomware et cryptolocker, Extrition et publication de données, Intrusion et phishing, Insuffisance des sauvegardes, PCA/PRA insuffisants, Cyber-conflits et attaques sponsorisées, Communication de crise défaillante	Ransomware Data breaches Business continuity threats	Segmentation réseau stricte Sauvegarde immuable MFA renforcée pour tous comptes Détection comportementale (EDR) Simulation d'attaques régulières Procédures de restauration rapide Plan de communication de crise	Niveau 2 (sauvegarde immuable pour rollback rapide), Niveau 3 (reconstruction complète si perte totale)	2. Réseau interne
S11	Panne authentication massive	Authentification / Infrastructure critique (Risque cyber / Risques technologiques et infrastructure)	Comptes utilisateurs, Identity Manager, MSAD, DNS, Switch EduID, OpenAthens	Identity Manager, MSAD, DNS, Switch EduID, OpenAthens	Accès aux ressources électroniques, Services aux usagers, [Accès aux ressources électroniques + Services aux usagers], Dépôts de données de recherche, Dépôts de publications	<b>Panne infrastructure d'authentification :</b> - Expiration certificat SAML - Détailance serveur AD/LDAP - Corruption base de comptes - Panne cluster ADFS	<b>Incident certificat :</b> - Expiration certificat SAML - Problème de synchronisation identité - Échec configuration DNS / Fédération	-	T1078 - Valid Accounts T1552-001 - Credentials in Files T1071-001 - Application Layer Protocol	D3-MFA - Multi-factor Authentication D3-SPP - Software Process and Device Rules D3-NTF - Network Traffic Filtering	Défaillance des tourniseurs d'identité, Défaillance de l'infrastructure, Dépendance aux identifiants persistants, PCA/PRA insuffisants, Infrastructure veillanteuse	Identity and access management Availability/risk	Infrastructure redondante pour ADFS Surveillance proactive des certificats Système de failback/authentification Authentification locale temporaire (mode dégradé SIG8) Documentation de procédures d'urgence Tests de bascule réguliers	Niveau 2, Niveau 3	1 Local isolé / accès SIG8 autonome, 2. Réseau interne (mode secours)
S12	Incident de sécurité physique et insuffisante des sauvegardes	Sécurité physique / Cyber physique (PCA) Risques technologiques et infrastructure / Risques opérationnels et logistiques	Systèmes physiques, bandes LTO, NAS, équipements réseau, serveurs, sauvegardes critiques	Stockage (SAN / NAS), Sauvegarde (TSM / Tape, Kasten, Veeptect), Réseau (Core Switches, DNS, Ordinateurs, Générateurs, Accès physique)	Tous les processus fortement impactés en particulier : Accès aux ressources électroniques, Services aux usagers, Dépôts de données de recherche, Dépôts de publications	<b>Intrusion physique :</b> - Vol cité de bandes LTO / serveurs - Sabotage volontaire (vol/épigée physique) - Implant matériel (backdoor physique) - Dégâagement physique des supports critiques - Erreurs de gestion des accès physiques	<b>Compromission matérielle :</b> - Absence de test de restauration complète et conditions réelles - Sauvegardes corrompues ou incomplètes, Coûts de reconstruction élevés - Incident réputationné possible	-	T1200 - Hardware Additions T1562-004 - Disable or Modify System Component T1119 - Automated Collection T1485 - Data Destruction T1070 - Indicator Removal on Host	D3-HA - Hardware Component Inventory Analysis D3-SPP - Software Process and Device Rules D3-NTF - Network Traffic Filtering D3-DA - Data Backup	Gestion des accès physiques, Catastrophes physiques et climatiques, Intrusion et phishing, Fraudes et sabotage académique, Perte de contexte et d'intelligibilité, Insuffisance des sauvegardes, Obsolétesse technologique, Fragmentation des responsabilités	Physical security threats Insider threat Journalisation des accès aux serveurs Chiffrement des bandes LTO / supports amovibles Stockage LTO en site distant sécurisé Délocalisation de zones sensibles Audits physiques périodiques Plan PCP pour reconstruction intégrale Tests complets de restauration au moins semestriel Vérification automatique d'intégrité des sauvegardes Automatisation du reporting de validation des sauvegardes	Niveau 3 (laS Cloud) (reprise à froid ou à chaud), éventuellement failback en mode réseau interne secondaire	3. laS Cloud (reprise à froid ou à chaud), éventuellement failback en mode réseau interne secondaire	
S13	Panne éditeur majeur (coupe des ressources électroniques)	Contractuel / Fournisseur	Accès distant aux ressources électroniques (cloud, Réseaux, DNS, Réseau, Archives mutualisées ou locales) (P2V / LOVSS / backup)	Plateformes éditeurs (cloud), Réseaux, DNS, Réseau, Archives mutualisées ou locales (P2V / LOVSS / backup)	Accès aux ressources électroniques, Services aux usagers, Services de recherche spécialisées, Acquisition des ressources électroniques	<b>Incident technique éditeur :</b> - Panne massive plateforme éditeur - Bug logiciel majeur sur portail ressources - Détailance cloud hébergé de l'éditeur	<b>Incident contractuel :</b> - Litige contractuel bloquant les accès - Suspension des droits d'accès - Rupture unilatérale du contrat	-	T1049 - Network Denial of Service T1199 - Trusted Relationship T1584 - Compromise Infrastructure	D3-DA - Data Backup D3-NTF - Network Traffic Filtering D3-WCAP - Web Content Analysis and Prevention	Faille d'éditeurs ou agrégateurs, Défaillance chaîne d'approvisionnement logistique, Dépendance SaaS/IaaS, Conflit de propriété intellectuelle, Restrictions budgétaires	Third-party dependency Service availability risk Contract and legal risks	Archivage local systématique des contenus autorisés (LOCKSS / P2V) Négociation clauses de continuité de service Communication usagers anticipée (plan d'information) Veille juridique active sur contrats éditeurs Identification et mise en place d'alternatives temporaires (archives ouvertes, accès partenaire)	Niveau 3 (archives PLN)	2. Réseau interne avec contenu local, 3. laS Cloud (accès à ressources de secours ou partenaires)

## Annexe 23 : Scénarios combinés et seuils d'alerte

Matrice des dépendances inter-scénarios et effets cascade		
Scénarios déclencheurs primaires (effet cascade)	Scénarios secondaires induits	Impact combiné
<b>Scénario déclencheur</b>		
<b>S10 - Ransomware ciblé</b>	S4 (compromission comptes) → S8 (fuite LPD) → S11 (panne authentification) → S14 (incident sécurité physique si sabotage associé)	<b>CRITIQUE</b>
<b>S11 - Panne authentification massive</b>	S3 (catalogue Primo inaccessible) + S6 (ressources électroniques) + S1 (impact Alma / SIGB)	<b>CRITIQUE</b>
<b>S5 - Perte d'accès bâtiment / réseau local</b>	S9 (indisponibilité personnel clé) + S12 (sécurité physique / sauvegardes corrompues) + S14 (vol / sabotage)	<b>ÉLEVÉ</b>
<b>S4 - Compromission comptes Alma / API</b>	S2 (corruption métadonnées) + S8 (fuite LPD) + S11 (panne authentification)	<b>ÉLEVÉ</b>
<b>S1 - Rupture contrat Alma / SLSP</b>	S3 (recherche impossible) + S6 (authentification proxy dégradée) + S13 (panne éditeur majeur) + S15 (panne écosystème documentaire)	<b>ÉLEVÉ</b>
<b>Amplifications mutuelles</b>		
Combinaison	Mécanisme d'amplification	
<b>S10 + S8 + S11</b>	Ransomware → Fuite LPD → Paralysie authentification → Crise médiatique	
<b>S11 + S6 + S3</b>	Panne auth → Perte ressources → Inaccessibilité catalogue (trio SaaS)	
<b>S1 + S7 + S15</b>	Rupture SIGB + Licences + Éditeur (perte écosystème documentaire)	
<b>S5 + S12 + S14</b>	Perte accès physique + sabotage + vol + sauvegardes compromises → Paralysie SI	
<b>Scénarios composés fréquents</b>		
Nom composite	Scénarios impliqués	Durée impact
<b>Blackout numérique</b>	S11 + S3 + S6 (authentification + catalogue + ressources)	2-5 jours
<b>Cyber-incident majeur</b>	S10 + S4 + S8 + S11 (ransomware + comptes + LPD + authentification)	2-8 semaines
<b>Crise contractuelle</b>	S1 + S7 + S15 (SIGB + licences + éditeur)	1-6 mois
<b>Incident physique total</b>	S5 + S9 + S14 (bâtiment + personnel + sécurité / sabotage)	1-3 semaines
<b>Seuils de crise</b>		
<b>2 scénarios simultanés</b> : Activation cellule de crise		
<b>3 scénarios liés</b> : Plan de continuité d'activité déclenché		
<b>4+ scénarios cascade</b> : Gestion de crise majeure + communication externe		

## Annexe 24 : Synthèse des livrables

- Une revue de littérature comprenant une synthèse d'études de cas d'institutions comparables qui permet de situer les défis spécifiques, les menaces et les vulnérabilités des environnements de la préservation et de diffusion et d'inspirer des solutions pragmatiques (Annexe 8).
- Analyse comparative des normes pour une mise en évidence des complémentarités et des similitudes entre les normes de cybersécurité, les standards de préservation numérique, et les référentiels métiers. Cette comparaison a permis de sélectionner d'aligner et d'appliquer ces standards au système d'information d'une bibliothèque académique (Annexe 1).
- Synthèse des entretiens semi-dirigés interne et externe pour l'identification des besoins, contraintes et priorités des acteurs impliqués (bibliothécaires, responsables IT, RSSI). Cette étape a révélé une forte dépendance aux services tiers, une nécessité de partage et de communication des plans de continuité (Annexe 6 et 7).
- Matrice de maturité pour formaliser les écarts et permis l'évaluation du niveau de préparation de l'institution sur plusieurs axes. L'analyse a révélé un déficit de procédures formalisées et un cloisonnement entre métiers et IT dans la gestion des risques et de la visibilité des actifs entre secteurs (Annexe 9).
- Cartographie des processus métier critiques afin de reconnaître les chaînes actifs et dépendances fonctionnelles permettant l'accès aux ressources électroniques. Le SIGB est apparu comme le point névralgique du dispositif, avec une dépendance directe à des infrastructures critiques et aux services d'authentification externes (Annexe 11).
- Cartographie des actifs essentiels pour l'inventorisation et la hiérarchisation des ressources selon leur criticité pour l'activité au niveau applicatif et des données. Cette cartographie a servi de base à la stratégie de sauvegarde différenciée et à la définition de priorités de restauration. Avec un focus et une réflexion sur les critères de priorisation des ressources électroniques (Annexe 10 et 12).
- Analyse d'impact métier pour formaliser des délais maximaux de reprise (RTO), des pertes de données tolérables (RPO), les impacts métier de cette analyse ont appuyés la priorisation des mesures de résilience et orienté les scénarios de crise testés (Annexe 15).
- Inventaire et matrice des risques. Identification croisée des menaces, des vulnérabilités et des impacts, et de la probabilité potentielle. Le livrable intègre des fiches de suivi des risques. Nous avons pu relever lesquelles sont à traiter en priorité selon une matrice de criticité, attribuer des responsables, simuler des mesures et des plans d'amélioration continue (Annexe 16 et 17).
- Protocole de sauvegarde et d'accès modélisé de continuité structuré autour d'une couche contractuelle, d'une procédure d'extraction d'un dispositif de sauvegarde et de préservation et de modes d'accès pérenne aux données en cas de rupture de service au niveau fournisseur applicatif et éditeurs scientifique. Ainsi trois niveaux de protection et trois modes d'accès dégradé graduel (Annexe 18 et 19).
- Cartographie de scénarios de crise. Construction de scénarios combinant plusieurs vecteurs probables. Une conceptualisation des effets les entre scénarios a permis de simuler les effets domino et d'identifier des seuils d'activation d'une cellule de crise. Ces scénarios sont à même de tester la robustesse des solutions proposées et d'entraîner les équipes via des exercices pratiques de gestion de crise (Annexe 22 et 23).
- Fiche d'urgence à destination des équipes pour étayer la proposition visant à communiquer les bons réflexes de réaction face à une attaque par rançongiciel : L'élaboration de cette fiche est conçue pour être mobilisée directement en situation de crise et partagée avec les équipes non spécialistes, en bibliothèque ou en administration de la coordination (Annexe 20 et 21).