PRÉPARÉ PAR
MARIE CHALLET

R 5-05
GESTION DE LA CONFIDENTIALITÉ ET DU RISQUE

LA GESTION DES RISQUES INFORMATIQUES

RAPPORT

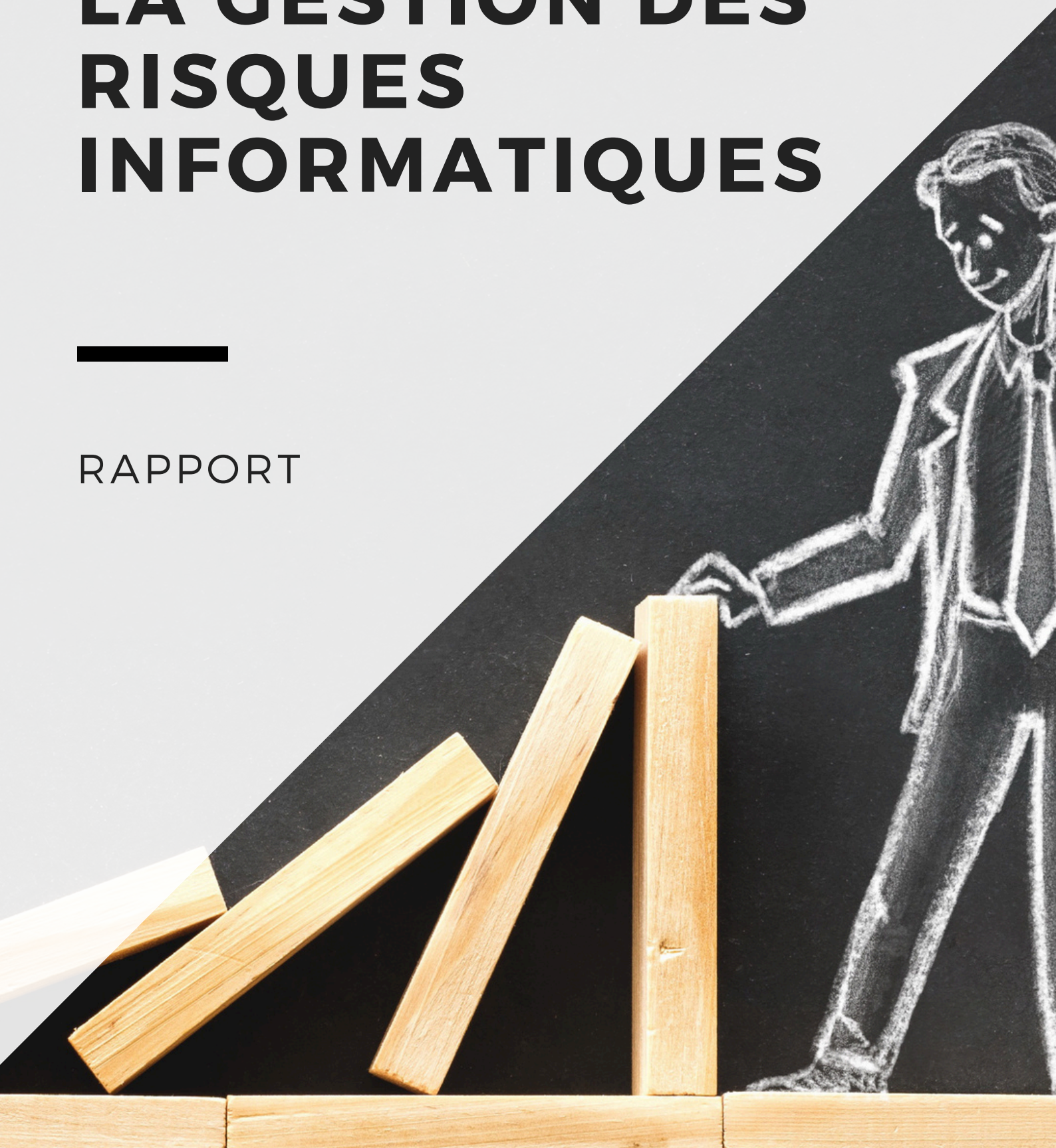

TABLE DES MATIERES

1 INTRODUCTION

La gestion des risques informatiques revêt une importance capitale pour garantir la sécurité, la résilience et la pérennité des organisations dans un environnement numérique en constante évolution et soumis à des menaces accrues. En réduisant les impacts des incidents imprévus tels que les cyberattaques ou les défaillances techniques, elle permet d'éviter des interruptions coûteuses, des pertes financières considérables, voire la cessation d'activité. Un ransomware non anticipé, par exemple, peut immobiliser les opérations d'une entreprise et entraîner des coûts de rançon prohibitifs. Par ailleurs, elle assure la protection des données et des actifs numériques en sécurisant les informations stratégiques et en prévenant les fuites, tout en respectant des réglementations comme le RGPD, qui impose aux responsables de traitement des mesures techniques et organisationnelles adaptées pour minimiser les risques. Cela permet non seulement d'éviter des sanctions financières pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel, mais aussi de préserver la confiance des parties prenantes, qu'il s'agisse des clients, des employés ou des investisseurs.

Sur le plan juridique, la gestion des risques s'appuie sur des obligations spécifiques, générales et sectorielles. Le RGPD, notamment ses articles 5 et 32, impose la mise en œuvre de mesures comme le chiffrement des données sensibles ou la pseudonymisation pour limiter les risques de violation. La Loi Informatique et Libertés, modifiée en alignement avec le RGPD, exige la réalisation d'analyses d'impact pour les traitements à risques ainsi qu'un encadrement strict des sous-traitants. Dans le secteur critique, la Loi de Programmation Militaire (LPM) impose aux Opérateurs d'Importance Vitale (OIV) des audits réguliers et des systèmes de surveillance renforcés pour sécuriser leurs infrastructures essentielles. Par ailleurs, l'article 1240 du Code Civil engage la responsabilité des organisations en cas de négligence entraînant un préjudice, comme dans le cas d'une fuite due à un serveur non sécurisé. Le Code du Travail, via l'article L.4121-1, souligne l'obligation pour l'employeur de protéger les salariés contre les risques, y compris numériques, à travers des actions de sensibilisation et des dispositifs de sécurité comme les VPN et l'authentification forte. Au niveau européen, la directive NIS 2 renforce les exigences en matière de sécurité des systèmes d'information pour les entités essentielles et impose un signalement rigoureux des incidents, avec des amendes substantielles en cas de manquements.

En complément de ces obligations, les normes ISO 27001 et 27005 offrent des référentiels reconnus pour structurer la gestion des risques. L'ISO 27001 définit un Système de Management de la Sécurité de l'Information (SMSI), qui repose sur le cycle PDCA pour établir, déployer, contrôler et améliorer en continu la sécurité de l'information. Elle fixe un cadre global pour intégrer la sécurité dans les processus organisationnels. À l'inverse, l'ISO 27005 se concentre spécifiquement sur la gestion des risques en proposant des méthodologies pour identifier, analyser, évaluer et traiter les vulnérabilités, ce qui la rend complémentaire à l'ISO 27001. Ainsi, l'ISO 27005 soutient la mise en œuvre du SMSI en détaillant les étapes d'une évaluation structurée des risques, essentielle pour adapter les contrôles de sécurité aux menaces émergentes.

La distinction entre mesures techniques et organisationnelles constitue une autre pierre angulaire de la gestion des risques. Les mesures techniques englobent les solutions matérielles et logicielles pour protéger les systèmes et les données, comme le chiffrement, les pare-feux, les systèmes de détection d'intrusion, les sauvegardes régulières ou l'authentification multifactorielle. À titre d'exemple, un serveur sécurisé avec cryptage AES empêche la

compromission des données même en cas de fuite physique. Les mesures organisationnelles, quant à elles, relèvent de la gouvernance et des politiques internes. Elles incluent la définition de chartes informatiques, la sensibilisation des employés aux cyberattaques comme le phishing, la gestion des incidents ou encore la réalisation d'audits réguliers pour garantir la conformité et identifier les failles. Ensemble, ces deux types de mesures assurent une protection globale, pérenne et conforme aux exigences du RGPD.

Les principaux risques auxquels les organisations sont confrontées aujourd'hui incluent la cybercriminalité, les erreurs humaines, les défaillances techniques, les catastrophes naturelles et la non-conformité. Les attaques par ransomware ou phishing connaissent une progression fulgurante, comme en témoigne la cyberattaque contre Colonial Pipeline, qui a paralysé une partie de l'approvisionnement énergétique américain. Les erreurs humaines, telles que la perte d'un appareil non sécurisé ou la suppression accidentelle de données, engagent la responsabilité des organisations, soulignant l'importance de la sensibilisation et des contrôles d'accès stricts. Les pannes matérielles et logicielles, quant à elles, nécessitent la mise en place de plans de reprise d'activité (PRA) pour assurer la continuité des opérations. Face aux catastrophes naturelles comme l'incendie des serveurs OVH en 2021, les solutions de redondance géographique et de sauvegardes externes s'avèrent indispensables. Enfin, la non-conformité expose les entreprises à des sanctions financières importantes, comme l'amende infligée à Google pour non-respect du RGPD.

Pour pallier ces risques, le concept de *privacy by design* et *by default* joue un rôle essentiel en intégrant la protection des données dès la conception des systèmes et en garantissant que seules les informations strictement nécessaires sont traitées par défaut. Cette approche proactive permet d'anticiper les menaces, de limiter les risques de violation et de renforcer la conformité avec les exigences légales. Ainsi, la gestion des risques informatiques, en conciliant mesures techniques, organisationnelles et approche privacy by design, s'impose comme un levier stratégique pour assurer la sécurité des actifs numériques, la continuité des opérations et la confiance des parties prenantes face aux défis numériques contemporains.

2 ETUDE DE CAS

Afin d'illustrer concrètement les enjeux de la gestion des risques informatiques et l'importance des mesures techniques et organisationnelles, examinons le cas d'une PME spécialisée dans la fabrication de jouets en bois et opérant exclusivement en ligne. Cette entreprise repose sur un écosystème numérique intégré pour la gestion de ses opérations, et l'analyse des risques a révélé des menaces critiques qui pourraient gravement affecter sa continuité d'activité. Ce cas pratique permet d'analyser les défis auxquels une organisation de cette envergure peut être confrontée, tout en explorant les solutions stratégiques adaptées à son contexte spécifique.

2.1 INTRODUCTION DU CAS

2.1.1 Contexte et périmètre d'évaluation

La présente analyse s'inscrit dans le cadre d'un exercice de gestion des risques informatiques, conformément à la norme ISO/CEI 27005:2022, au sein d'une PME spécialisée dans la fabrication de jouets en bois. Ladite entreprise assure la vente de ses produits en ligne et dispose d'une usine et d'un entrepôt pour la production, la préparation, le traitement et l'expédition des commandes, ainsi que de l'ensemble de ses données informatiques hébergées en mode SaaS (site internet,

CRM, traitement des commandes, paiement en ligne, gestion administrative et comptable). L'objectif principal consiste à garantir la disponibilité, la confidentialité et l'intégrité (trois piliers classiques de la sécurité de l'information) des actifs critiques de l'entreprise. Dans ce cadre, l'analyse porte sur l'identification des vulnérabilités, la classification des actifs et des risques, la priorisation et le traitement de ces risques, ainsi que sur la définition d'un dispositif de surveillance continue.

2.1.2 Cadre juridique et exigences légales

2.1.2.1 Majeure (principe légal applicable)

En vertu du Règlement Général sur la Protection des Données (RGPD), toute entreprise manipulant des données à caractère personnel doit mettre en place des mesures organisationnelles et techniques adéquates pour protéger la confidentialité et l'intégrité des données. Par ailleurs, le Code du commerce et le Code civil imposent à l'entreprise de prendre les mesures nécessaires pour assurer la continuité de ses activités et éviter tout préjudice financier majeur. De surcroît, la responsabilité contractuelle et délictuelle de l'entreprise peut être engagée en cas de manquement dans la livraison des produits ou de fuite de données.

2.1.2.2 Mineure (application au cas d'espèce)

Au regard des considérations légales susmentionnées, il apparaît que l'entreprise, en tant que PME vendant en ligne, gère des données personnelles (fichiers clients, informations de paiement, adresses, etc.) et doit, à ce titre, respecter les principes du RGPD, particulièrement en matière de sécurité des données personnelles. En outre, elle reste tenue de respecter ses obligations contractuelles relatives aux délais de livraison et à la disponibilité du site web.

2.1.2.3 Conclusion (règle de droit appliquée au cas d'espèce)

En application de la norme ISO 27005:2022 et du RGPD, l'entreprise est tenue d'élaborer un dispositif de gestion des risques adapté, incluant des mesures organisationnelles et techniques efficaces, afin de limiter l'impact potentiel d'une indisponibilité, d'un vol de données ou d'une fuite de données personnelles.

2.2 IDENTIFICATION ET CLASSIFICATION DES ACTIFS

Afin de répondre aux obligations précitées, une première étape d'identification et de classification des actifs a été conduite pour mesurer l'impact potentiel des risques afférents à chacun d'eux.

2.2.1 Actifs informationnels

- **Base de données clients** : Elle regroupe toutes les informations personnelles (noms, adresses postales, adresses e-mail, historiques de commandes, coordonnées bancaires partiellement masquées, etc.). Sa criticité est élevée en termes de confidentialité stratégique, notamment du fait des exigences liées au RGPD.
- **Serveurs (hébergés en mode SaaS)** : Hébergent les modules de gestion (CRM, commandes, comptabilité, etc.). Leur criticité est axée sur la haute disponibilité, une interruption de service impactant directement la livraison et la facturation.
- **Site web e-commerce** : Il constitue la vitrine de l'entreprise et le cœur des ventes en ligne (catalogue, panier, paiement, gestion des comptes clients, etc.). Sa criticité réside dans sa disponibilité, puisque tout temps d'arrêt compromet immédiatement le chiffre d'affaires et l'image de marque.

- **Flux de commandes** : Ils concernent l'ensemble des procédures métiers associées (réception, validation, préparation, expédition). Leur criticité est également élevée en termes de disponibilité, en raison du risque de perte d'exploitation en cas d'interruption.

2.2.2 Actifs humains et organisationnels

Sont notamment recensés les employés en usine (préparation des commandes, logistique), le personnel administratif (traitement et suivi des commandes, relation clients, facturation), les partenaires transporteurs (acheminement et livraison) et les fournisseurs d'hébergement SaaS et de solutions logicielles tierces.

2.3 IDENTIFICATION ET CLASSIFICATION DES VULNÉRABILITÉS

Dans un second temps, l'analyse a mis en évidence diverses vulnérabilités, à la fois techniques et organisationnelles.

2.3.1 Vulnérabilités techniques

- **Risque de panne de serveur ou de service SaaS** : Absence ou insuffisance de redondance, SLA (Service Level Agreement) trop faible ou non adapté, absence de tests réguliers des mécanismes de reprise.
- **Risque d'attaque informatique (hacker)** : Failles de sécurité dans les modules SaaS, absence de chiffrement des données sensibles, manque de solutions d'authentification forte (MFA).
- **Risque d'indisponibilité du site web** : Attaques de type DDoS, maintenance non planifiée ou mal exécutée, défaillance d'un hébergeur unique (absence de multi-Cloud).

2.3.2 Vulnérabilités organisationnelles

- **Procédures internes non formalisées ou incomplètes** : Absence de plan de continuité (PCA/PRA) testé, inexistence d'une politique de sécurité clairement définie, manque de sensibilisation des employés.
- **Gestion des habilitations et accès** : Droits trop larges (pas de principe du moindre privilège), manque de suivi des comptes inactifs.
- **Externalisation et dépendance vis-à-vis des fournisseurs** : Manque de clauses contractuelles solides (réversibilité, disponibilité), défaut d'audit sur la sécurité des tiers.

2.4 CLASSEMENT DES RISQUES (MATRICE DE RISQUES)

Après analyse, trois risques de niveau élevé ont été identifiés :

1. **Risque 1 : Impossibilité de livrer les commandes pendant 4 jours** en raison d'une panne de serveur (perte d'exploitation).
    - Impact : Élevé (perte financière et insatisfaction client).
    - Probabilité : Moyenne (dépendance unique vis-à-vis de l'hébergeur SaaS).
2. **Risque 2 : Récupération d'une copie de la base clients par un hacker** (fuite de données à caractère personnel).
    - Impact : Très élevé (sanctions RGPD, perte de confiance des clients, atteinte à l'image).

- Probabilité : Moyenne à élevée (tentatives d'attaque régulières sur des bases clients).

3. **Risque 3 : Indisponibilité du site web et de toutes ses fonctions intégrées** (catalogue, soumission de commandes, gestion du compte client).
    - Impact : Élevé (impact sur le chiffre d'affaires, réclamation clients).
    - Probabilité : Moyenne (attaques DDoS, erreurs techniques, absence de redondance).

2.5 TRAITEMENT ET PLAN DE RÉPONSE AUX RISQUES

Conformément à la norme ISO 27005:2022, chaque risque peut être traité selon les approches suivantes : réduire, transférer, accepter ou éliminer (éviter), en fonction du contexte propre à l'entreprise.

2.5.1 Risque 1 : Impossibilité de livrer les commandes pendant 4 jours (indisponibilité)

Le besoin principal identifié est la **disponibilité (sous 24h)**.

2.5.1.1 Mesures organisationnelles

Parmi les mesures déjà préconisées figurent : la formalisation de la procédure de gestion de commandes, l'identification de sources de recrutement rapide pour pallier l'indisponibilité d'un employé, le maintien d'un stock suffisant de fournitures d'expédition, la négociation de tarifs avec divers transporteurs et l'élaboration de procédures de reprise d'activité (PRA/PCA) régulièrement testées.

2.5.1.2 Mesures techniques

- **Redondance et haute disponibilité** : Mise en place d'une architecture redondante (serveur secondaire ou cluster) chez le fournisseur SaaS ou chez un prestataire différent, accompagnée d'un back-up régulier des données de commandes sur un autre site ou un autre cloud.
- **Plan de reprise après sinistre (PRA) et plan de continuité d'activité (PCA)** : Documentation précise des procédures de restauration des services en moins de 24h, à tester au moins une fois par an.
- **SLA (Service Level Agreement) renforcé** : Renégociation des contrats avec le prestataire SaaS afin de garantir un RTO (Recovery Time Objective) inférieur à 24h et un RPO (Recovery Point Objective) très faible.
- **Solutions de monitoring et d'alerte en temps réel** : Mise en place d'un outil de supervision pour alerter immédiatement l'équipe IT en cas de panne ou de comportement anormal, assorti d'une mesure continue de la performance du service.

2.5.2 Risque 2 : Récupération d'une copie de la base clients par un hacker (fuite de données personnelles)

Le besoin principal visé est la **confidentialité (caractère stratégique)**.

2.5.2.1 Mesures organisationnelles

- **Politiques et procédures de sécurité interne** : Rédaction et diffusion d'une politique de gestion des données, accompagnée d'un contrôle strict des accès et de clauses de confidentialité dans les contrats de travail et avec les sous-traitants.

- **Gestion des habilitations et sensibilisation** : Mise en œuvre du principe du moindre privilège, formation régulière des employés aux bonnes pratiques (hameçonnage, mots de passe complexes, etc.) et désactivation immédiate des comptes des salariés quittant l'entreprise.

- **Gestion des tiers et contrats** : Vérification des clauses de sécurité et de confidentialité avec les prestataires SaaS, imposition d'audits de sécurité périodiques chez le prestataire et insertion de pénalités en cas de manquement.

2.5.2.2 Mesures techniques

- **Chiffrement des données (at rest et in transit)** : Utilisation d'algorithmes forts (AES-256) et chiffrement TLS pour tous les échanges.

- **Contrôle des accès (authentification forte)** : Mise en place d'une authentification multi-facteurs (MFA) pour tous les accès sensibles, avec journalisation des connexions et des actions (audit logs).

- **Système de détection et de prévention des intrusions (IDS/IPS)** : Surveillance en temps réel des tentatives d'intrusion, accompagnée de solutions SIEM (Security Information and Event Management).

- **Pare-feu applicatif (WAF) et segmentation réseau** : Protection du front-end et segmentation pour limiter les déplacements latéraux (Zero Trust Architecture).

- **Sauvegardes protégées et tests de restauration** : Sauvegardes régulières, chiffrées et stockées hors site, avec vérification systématique de leur intégrité et de leur restaurabilité.

2.5.3 Risque 3 : Indisponibilité du site web (toutes ses fonctions intégrées)

Le besoin principal identifié est la disponibilité (sous 4h).

2.5.3.1 Mesures organisationnelles

- **Procédures de gestion d'incident** : Rédaction d'un plan de gestion d'incident dédié au site web (définition des rôles, responsabilités, escalades, procédures de communication) et formation des équipes.
- **Contrats avec un hébergeur disposant de redondances** : Vérification de la localisation des data centers, exigence de garanties de disponibilité (SLA strict) et mise en place d'un support 24/7.
- **Communication de crise** : Prévision d'un canal de communication alternatif (mini-site externalisé, réseaux sociaux) pour informer la clientèle en cas d'incident et mise à jour en temps réel de l'état des services.

2.5.3.2 Mesures techniques

- **Redondance d'hébergement (multisite ou multi-cloud)** : Hébergement du site web sur plusieurs data centers géographiquement distincts, associé à un système de répartition de charge (load balancing).
- **Plan de continuité d'activité (PCA) adapté au site web** : Définition d'un RTO (Recovery Time Objective) de moins de 4h, assortie de tests réguliers de basculement.
- **Maintenance préventive et mises à jour régulières** : Vérification du CMS, des plugins, du serveur web et du système d'exploitation (patch management), en s'appuyant sur les standards de sécurité OWASP.

- **Protection contre les attaques DDoS** : Mise en place d'un service de mitigation DDoS (via un pare-feu applicatif ou un prestataire spécialisé), avec surveillance continue du trafic afin de détecter les pics anormaux.
- **Monitoring 24/7 et alertes automatisées** : Implantation de sondes de disponibilité (ping, http checks, etc.) et réception d'alertes par mail/SMS pour intervention rapide.

2.6 SURVEILLANCE CONTINUE DES RISQUES

Conformément aux exigences de la norme ISO 27005:2022, la gestion des risques doit s'inscrire dans une dynamique d'amélioration continue, selon le cycle PDCA (Plan-Do-Check-Act). D'abord, les actions sont planifiées (Plan) par l'identification des risques et la définition de politiques de sécurité et de mesures adaptées. Ensuite, ces politiques et mesures sont mises en œuvre sur le terrain (Do), avant d'en vérifier l'efficacité par le biais d'audits internes et externes, ainsi que d'analyses régulières d'indicateurs de performance et de conformité (Check). Enfin, les dispositifs sont améliorés de manière continue par des actions correctives et préventives (Act).

Dans cette perspective, il est indispensable de mettre à jour la matrice des risques au moins une fois par an ou dès qu'un événement significatif (nouvelle technologie, nouveau fournisseur, etc.) survient. Des audits réguliers, internes et externes, doivent être réalisés afin de vérifier la conformité avec le RGPD et le respect des exigences de la norme ISO 27005. La documentation afférente (plans de continuité et de reprise d'activité, consignes de sécurité, politiques internes) doit être tenue à jour de manière rigoureuse. Enfin, l'analyse approfondie des incidents passés constitue un levier essentiel pour identifier d'éventuelles failles et renforcer en continu le dispositif de sécurité.

2.7 CONCLUSION GÉNÉRALE ET RECOMMANDATIONS

Au terme de l'analyse, il apparaît nécessaire que l'entreprise mette en œuvre des mesures spécifiques pour faire face aux principaux risques identifiés. En premier lieu, afin d'assurer la continuité des livraisons (Risque 1), la mise en place de solutions techniques, telles que la redondance des systèmes et un plan de reprise d'activité (PRA), doit s'accompagner de mesures organisationnelles, incluant la répartition des tâches, la constitution de stocks de fournitures et la contractualisation avec plusieurs transporteurs. Ensuite, pour préserver la confidentialité de la base clients (Risque 2), des dispositifs organisationnels (sensibilisation des équipes, clauses contractuelles adaptées, gestion stricte des habilitations) doivent être associés à des solutions techniques (chiffrement des données, MFA, segmentation des accès, IDS/IPS). Enfin, afin de renforcer la disponibilité du site web (Risque 3), l'entreprise doit se doter d'un plan de gestion des incidents, d'une communication de crise efficace et de SLA stricts, ainsi que de dispositifs techniques tels que l'hébergement multisite, l'équilibrage de charge, la mise en place de solutions anti-DDoS et l'exécution d'opérations de maintenance régulières.

La mise en œuvre rigoureuse de ces recommandations permettra à l'entreprise de consolider sa conformité au RGPD, de préserver la confiance de sa clientèle et de prévenir des pertes d'exploitation susceptibles de porter atteinte à ses intérêts financiers et à son image. Enfin, une veille continue sur l'évolution des menaces et une adaptation permanente aux nouveaux contextes réglementaires et technologiques s'avèrent indispensables pour pérenniser la sécurité des actifs critiques de l'entreprise.

3 CAS DE VIOLATION DE DONNEES PERSONNELLES

Dans l'hypothèse d'une cyberattaque ayant entraîné une violation de données à caractère personnel, l'organisation concernée est légalement tenue, au titre du Règlement Général sur la Protection des Données (RGPD), d'effectuer une notification rapide à l'autorité de contrôle compétente (en France, la CNIL), et ce dans un délai de 72 heures à compter de la découverte de ladite violation (article 33 du RGPD). Parallèlement, lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, l'organisation doit également informer sans délai les personnes concernées, de manière claire et compréhensible, des conséquences potentielles de l'incident et des mesures mises en place pour y remédier (article 34 du RGPD). Cette obligation d'information poursuit l'objectif de protéger la confidentialité et de permettre aux individus affectés de prendre les dispositions nécessaires (par exemple, la modification de mots de passe ou la vigilance accrue quant aux tentatives de fraude). Outre la notification, l'organisation doit impérativement documenter l'incident, recenser les circonstances, identifier les causes de la violation et mettre en œuvre, dès que possible, les mesures correctives ou préventives visant à éviter qu'une telle situation ne se reproduise (mise à jour des politiques de sécurité, renforcement des contrôles d'accès, actions de sensibilisation du personnel, etc.). Ainsi, tant l'exigence de notification aux autorités que l'obligation d'informer les personnes concernées et de sécuriser l'infrastructure technique et organisationnelle s'inscrivent dans le prolongement du principe de confidentialité prévu par le RGPD et contribuent à la protection effective des droits fondamentaux des individus.

4 CONCLUSION

En définitive, la gestion des risques informatiques ne se limite pas à la mise en place de mesures isolées, mais requiert une démarche globale et méthodique, reposant aussi bien sur des solutions techniques que sur un cadre organisationnel solide. Les dispositifs de redondance, de chiffrement, de gestion fine des habilitations et de communication de crise jouent ainsi un rôle essentiel dans la protection des actifs numériques, la continuité des opérations et le maintien de la confiance des parties prenantes. La conformité aux normes ISO 27001 et 27005, de même que le respect du RGPD et des lois sectorielles ou nationales, apparaît dès lors comme un levier stratégique pour assurer la résilience et la pérennité de l'entreprise face à des risques de plus en plus complexes et évolutifs.

Au-delà de l'application immédiate des recommandations exposées, il convient d'anticiper les mutations futures de l'environnement numérique. L'essor des technologies émergentes, comme l'intelligence artificielle ou l'Internet des objets (IOT), ouvre de nouvelles perspectives tout en suscitant de nouveaux défis pour la sécurité de l'information et la protection des données. Il est donc primordial de prévoir des processus de veille et d'adaptation continue pour intégrer ces évolutions dans la stratégie de gestion des risques. Cette approche dynamique, conjuguée à une sensibilisation constante des équipes et une gouvernance adaptée, permettra aux organisations de rester proactives et d'assurer une protection optimale de leurs actifs dans un contexte en constante mutation.