Politique de Sécurité de l'Information

Mars 2024

Table des matières

1 Introduction

L'information et le capital intellectuel constituent l'essence des activités de KPMG. Ses missions conduisent le cabinet à détenir un volume de données toujours plus important, dans des contextes le plus souvent soumis à des contraintes réglementaires.

KPMG fait donc de la protection des données et de la cybersécurité une priorité fondamentale, sur laquelle repose la confiance de ses clients, de ses relations d'affaires et des autorités de régulation.

A cet effet, KPMG déploie les mesures nécessaires afin de garantir non seulement la conformité aux réglementations existantes comme le RGPD (Règlement général sur la protection des données), mais aussi l'alignement avec les meilleures pratiques à travers des procédures de prévention des risques, la formation des collaborateurs, ou encore des démarches de certification ou d'audit de ses processus.

Gouvernance en matière de cybersécurité

Rattachée à la Direction des systèmes d'information, la fonction « sécurité des systèmes d'information » reporte également au département de gestion des risques (Risk Management) du cabinet, lequel joue un rôle essentiel dans la maîtrise des risques induits par les usages technologiques, en particulier lorsqu'ils sont porteurs d'innovation ou au cœur des offres de services et de conseil aux clients.

Système de Management de la Sécurité de l'Information

Un Système de Management de la Sécurité de l'Information (SMSI) a été mis en œuvre conformément aux exigences de la norme ISO/IEC 27001:2017.

Il a été certifié en juillet 2022 pour le domaine d'application suivant : « Sécurité de l'information des services de traitement de données et de gestion informatique relatifs à la fourniture des prestations de KPMG France ». La déclaration d'applicabilité afférente reprend exhaustivement les mesures de l'annexe A de la norme.

Activités clé

KPMG applique des mesures couvrant l'ensemble des aspects organisationnels et techniques de la sécurité numérique :

- La sensibilisation des collaborateurs à la cybersécurité, par des formations annuelles obligatoires et des campagnes de simulation d'hameçonnage.
- La validation systématique de la conformité des initiatives technologiques aux contraintes du cabinet.
- L'intégration de la sécurité dans la gestion de projets et les processus de développement logiciel, selon les principes de sécurité dès la conception.
- L'application de mesures de renforcement telles que la protection de la messagerie et des postes de travail, l'usage de l'authentification forte et du chiffrement, la gestion des identités et des habilitations, ou la segmentation des réseaux et des centres de données.
- La gestion des vulnérabilités, sur la base d'analyses fréquentes et d'un suivi rapproché des actions de correction et de mise à jour.
- Le déploiement de capacités techniques et humaines de surveillance du système d'information visant à détecter et à répondre aux évènements suspects et aux incidents.
- L'examen systématique de la posture de sécurité des fournisseurs et partenaires, à travers des évaluations initiales et périodiques.
- L'intégration de clauses, d'annexes ou de documents spécifiques dans les contrats conclus avec les clients et les fournisseurs.

Audits de conformité

KPMG organise depuis de nombreuses années, au niveau international, des campagnes annuelles d'audit de conformité de la sécurité de l'information de ses cabinets membres.

Ces campagnes, dites IPCR (Information Protection Controls Review), appliquent les bonnes pratiques d'audit et vérifient de façon approfondie l'efficacité des mesures en place. En France, KPMG fait appel pour cet exercice à des cabinets indépendants.

Dans le cadre de ces contrôles, des indicateurs de performance permettent d'évaluer l'application des mesures de sécurité en testant leur efficacité notamment à travers des campagnes de tests d'intrusion et de simulations d'hameçonnage.

2 Portée et objet du document

KPMG désigne dans ce document les entités françaises du réseau international KPMG, notamment :

- KPMG S.A., qui porte les activités Audit et les fonctions support du cabinet ;
- KPMG Advisory, qui porte les activités Advisory (Consulting et Deal Advisory) ;
- KPMG ESC & GS, qui porte les activités d'Expertise-Comptable, le Conseil aux Entrepreneurs et la Gestion Sociale ;
- KPMG Avocats, qui porte les activités Juridiques et Fiscales.

Le but de ce document est de présenter les pratiques adoptées par KPMG en matière de sécurité de l'information et de protection des données.

3 Dispositif général

3.1 Politique de sécurité de l'information

Les principes et règles générales relatives à la sécurité des systèmes d'information et la protection des données sont formalisés dans un document « Politique de Sécurité du Système d'Information ». Ce document est revu annuellement, afin de l'adapter aux nouvelles menaces.

3.2 Organisation de la sécurité de l'information

L'équipe responsable de la sécurité de l'information de KPMG est notamment composée de professionnels travaillant dans les fonctions Systèmes d'Information et Risk Management. Elle est chargée de faire évoluer et soutenir les pratiques en matière de sécurité de l'information de KPMG.

En travaillant en étroite collaboration avec les différents métiers de KPMG, elle élabore les normes appropriées visant à assurer la sécurité de ses informations ainsi que celles de ses clients. Grâce à ces différentes activités, le personnel de KPMG dispose d'outils et de ressources lui permettant de comprendre sa responsabilité vis-à-vis de la sécurité et de la protection des informations de ses clients.

3.3 Sécurité des ressources humaines

Quel que soit leur statut, tous les futurs collaborateurs sont soumis à une vérification des antécédents comprenant la vérification des références, des diplômes d'études, de l'identité et du casier judiciaire.

Les règles à suivre par les collaborateurs de KPMG en termes de sécurité des systèmes d'information et de protection des données sont définies dans :

- Une charte informatique qui décrit les modalités d'utilisation des outils informatiques et les règles afférentes. Cette charte est annexée au règlement intérieur ;
- Un document « Règles de Sécurité Informatique pour les Utilisateurs Finaux », mis à jour annuellement, signé par chaque collaborateur lors de son arrivée chez KPMG. Ce document aborde notamment les sujets suivants : propriété de l'information, usage personnel des équipements professionnels, accès aux données de KPMG et des clients, stockage et conservation des données et réaction à incident sur la fuite de donnée.

La sécurité des systèmes d'information et la protection des données fait partie du programme de formation obligatoire que chaque collaborateur KPMG doit suivre à son arrivée au sein du cabinet. Ce sujet est également inclus dans l'engagement annuel signé par tous les collaborateurs de KPMG.

La réalisation effective des formations obligatoires est suivie, les personnes concernées sont relancées et les statistiques d'assiduité sont contrôlées par le Risk Management.

En complément, des campagnes de simulation de phishing testent régulièrement la vigilance de l'ensemble des collaborateurs et délivrent des quiz et des messages de sensibilisation aux collaborateurs n'ayant pas détecté le test.

Par ailleurs, tous les collaborateurs de KPMG sont astreints au **secret professionnel** dans le cadre de leur contrat de travail et soumis à un devoir de discrétion pour les faits, actes et renseignements dont ils peuvent avoir connaissance dans le cadre de leur activité, et après cessation de cette activité. Ces obligations sont par ailleurs rappelées dans le cadre du programme de formation pour les nouveaux collaborateurs.

3.4 Gestion des actifs

Des outils opérés par la DSI de KPMG permettent d'avoir une vision des systèmes connectés au réseau interne (serveurs, terminaux mobiles, etc.). Des schémas d'architecture par application sont maintenus.

Des politiques, des procédures et un outil permettent de classifier et marquer les documents bureautiques selon leur niveau de confidentialité.

3.5 Contrôle d'accès

Chaque collaborateur de KPMG possède une identité numérique unique dédiée et incessible.

Ces identités sont protégées par des mots de passe se conformant à une politique de mot de passe imposant un nombre minimum de caractères, une complexité en termes de type de caractères et une fréquence de renouvellement obligatoire. Les comptes sont verrouillés en cas de tentatives erronées répétées.

Une revue des habilitations est réalisée de manière périodique sur les systèmes critiques et les zones physiques sécurisées.

3.6 Sécurité physique et environnementale

KPMG a mis en place des mesures de sécurité visant à contrôler l'accès physique aux locaux qui hébergent l'information de KPMG et de ses clients. L'accès à ses bureaux est limité aux personnes autorisées utilisant des dispositifs électroniques ou mécaniques de contrôle d'accès, ou aux visiteurs autorisés. L'accès aux centres de données est strictement limité aux seules personnes autorisées.

Destruction sécurisée

Tous les étages du siège et des principales directions régionales sont munis de containers sécurisés afin de recueillir les documents papiers à détruire et de broyeurs. Le contenu des containers est collecté et détruit par une société spécialisée qui délivre un certificat de destruction.

3.7 Sécurité liée à l'exploitation

3.7.1 Postes de travail

Les collaborateurs de KPMG utilisent pour accéder à leurs postes de travail des comptes disposant de droits « utilisateur standard ». Un nombre restreint de collaborateurs, sur la base d'un besoin légitime, peuvent élever leurs privilèges sur leurs postes de travail selon une procédure permettant de le tracer.

Des règles s'appliquent en cas de télétravail ou de déplacement hors des locaux KPMG, cela implique notamment l'utilisation du VPN.

Les postes de travail sont intégrés à l'annuaire.

Les imprimantes, partagées, nécessitent l'usage du badge nominatif pour libérer les impressions.

3.7.2 Smartphones

Les collaborateurs de KPMG disposent de smartphones, gérés au sein d'une solution MDM centralisée. L'intégration du smartphone dans le MDM est nécessaire pour accéder à la messagerie Exchange Online et aux applications mobiles internes, via des flux chiffrés.

Le BYOD (Bring Your Own Device) est interdit, y compris pour les smartphones et les tablettes.

3.7.3 Protection contre les malwares

Les postes de travail des collaborateurs de KPMG et les serveurs sont munis d'une solution antivirale et d'une solution de type « Endpoint Detection & Response » (EDR). Cette solution permet d'administrer les agents déployés sur les postes de travail des collaborateurs de KPMG et les serveurs.

Une protection antimalware, anti-spam et anti-phishing est en place pour les e-mails entrants et sortants.

3.7.4 Gestion des vulnérabilités

Tous les serveurs et postes de travail disposent d'un agent d'inventaire des vulnérabilités.

Le réseau interne de KPMG fait l'objet de scans de vulnérabilités hebdomadaires.

Les serveurs de KPMG exposés sur Internet sont scannés quotidiennement par des solutions de scan de vulnérabilités. Des tests de conformité et de sécurité sont réalisés périodiquement l'aide d'outils spécialisés.

3.7.5 Correctifs de sécurité

Les correctifs de sécurité pour les serveurs et postes de travail Windows sont gérés par une procédure supportée par des outils spécialisés. Cette procédure prévoit l'application mensuelle de la plupart des correctifs, l'installation automatique des correctifs dès leur mise à disposition (p.ex. les navigateurs web), ainsi que l'application en urgence des correctifs critiques. Des tableaux de bord d'état de conformité sont produits.

Un planning de remplacement des logiciels en voie d'obsolescence est suivi.

3.7.6 Administration

Les administrateurs possèdent des comptes personnels non privilégiés distincts des comptes à privilèges.

La politique de gestion des mots de passe est renforcée pour ces administrateurs.

Un bastion d'administration permet la protection des accès à privilèges à travers une authentification forte, la traçabilité des actions, la rotation des mots de passes et la détection des activités suspectes.

Une revue des comptes privilégiés est réalisée hebdomadairement.

3.8 Sécurité des communications

3.8.1 Réseaux

Tous les sites de KPMG sont connectés au réseau KPMG par des liaisons redondantes. L'accès à Internet est centralisé et protégé par des firewalls hébergés dans des datacenters redondants, chacun relié à un opérateur différent.

Les collaborateurs de KPMG en télétravail peuvent se connecter au réseau interne via une architecture VPN depuis des PC KPMG seulement.

L'accès aux espaces collaboratifs est soumis à un accès conditionnel. Le standard d'accès aux applications repose sur un mécanisme SSO (Single Sign-On) et une fédération des environnements.

Une application permet aux collaborateurs KPMG et leurs clients de s'échanger des documents via une plateforme dédiée, dont les flux et le contenu sont chiffrés.

Les sites et applications publiées sur Internet sont hébergés dans des DMZ protégées par des firewalls.

3.9 Développement sécurisé

KPMG suit pour ses développements une méthodologie de gestion de projet qui inclut des volets sécurité des SI, dont la traçabilité des actions. Un outil d'audit de code est inclus dans la plateforme d'intégration et permet d'analyser le code source généré.

Un Comité Architecture & Sécurité se tient toutes les semaines au sein de la DSI.

Les environnements de développement, de test et de production sont séparés. Les données utilisées dans les environnements de développement et de test ne contiennent pas de données réelles de clients.

3.10 Relations avec les fournisseurs

Un processus d'évaluation des fournisseurs est en place et inclut systématiquement un questionnaire d'auto-évaluation de la sécurité des SI.

Les contrats de sous-traitance intègrent des clauses portant sur la sécurité des SI et la protection des données, incluant une clause d'audit.

Les environnements techniques des fournisseurs sont soumis à des tests de sécurité réguliers, opérés soit par le fournisseur, lequel doit alors en fournir la preuve, soit directement par KPMG ou l'un de ses partenaires spécialisés.

Le suivi des fournisseurs critiques de KPMG est en place.

3.11 Gestion des incidents liés à la sécurité de l'information

3.11.1 Surveillance

Une surveillance du SI de KPMG est assurée par le SOC de KPMG International (GSOC) et celui de KPMG France, tous deux en 24/7.

3.11.2 Réponse à incident

Une équipe locale assure le traitement des incidents et le suivi des remédiations. Des compétences en investigation numérique et de gestion de crise sont également activables au besoin.

Des « playbooks » de réponse à incident ont été formalisés et des exercices de simulation de crise sont organisés périodiquement.

3.11.3 Veille / Menaces

Le GSOC souscrit à différents services de Cyber Threat Intelligence (CTI) lui permettant d'enrichir ses services de surveillance.

Il envoie des notifications au RSSI en cas d'incident ou de campagne d'attaque en cours sur l'un des membres du réseau KPMG dans le monde. Il envoie périodiquement des bulletins documentant les tendances de la menace.

3.11.4 Procédure en cas de perte / vol

En cas de perte ou de vol d'un ou plusieurs équipements informatiques ou de documents papier, une procédure décrit aux collaborateurs de KPMG le comportement à suivre.

3.12 Gestion de la continuité

3.12.1 Sauvegarde

Une politique de sauvegarde décrit les solutions mises en place pour assurer les sauvegardes. Les données des serveurs applicatifs et des serveurs de fichiers sont sauvegardées quotidiennement. Une copie des sauvegardes mensuelles est externalisée sur des bandes chiffrées.

3.12.2 Redondance

Des mécanismes de redondance sont en place pour l'infrastructure et pour les applications les plus critiques.

3.12.3 Délais de rétention

Une politique de rétention des données est documentée. En particulier, les activités règlementées telles que la certification des comptes et l'expertise comptable sont assujetties à des obligations de conservation des données afin de répondre aux régulateurs en cas de contrôle.

3.13 Conformité

3.13.1 Revue indépendante de la sécurité de l'information

Comme indiqué en introduction, le SMSI a fait l'objet d'un audit de certification en juillet 2022 et fait l'objet d'audits annuels de surveillance conformément à la norme ISO/IEC 27001:2017.

Un audit annuel est également réalisé par un cabinet tiers pour vérifier la conformité de KPMG à la politique et aux standards de KPMG International en matière de sécurité des systèmes d'information et de protection des données.

Des cabinets tiers réalisent régulièrement des missions d'audit de sécurité et de tests d'intrusion des infrastructures et des applications de KPMG.

Les applications de KPMG exposées sur Internet sont systématiquement testées avant leur mise en production.

4 Pour plus d'informations

Pour plus d’informations, veuillez tout d’abord consulter votre contact KPMG. Le cas échéant, vous serez redirigé vers l'équipe responsable de la sécurité de l'information.

https://www.kpmg.fr