DGSI01

POLITIQUE DE SÉCURITÉ

CYPE Ingenieros

ÉDITION	00
MODIFICATION	Édition initiale
DATE	17/12/2024
ÉLABORÉ	Responsable de la sécurité
RÉVISÉ ET APPROUVÉ	Direction générale

INDEX

1. DÉCLARATION DE PRINCIPES **3**
- 1.1. Objectifs généraux 4
- 1.2. Engagement de la direction générale 5
- 1.3. Développement de la politique de sécurité 7

2. POLITIQUE **7**
- 2.1. Prévention 7
- 2.2. Détection 8
- 2.3. Réponse 8
- 2.4. Récupération 8
- 2.5. Organisation de la sécurité 8
  - 2.5.1. Comité de sécurité 9
  - 2.5.2. Rôles : Fonctions et responsabilités 11
  - 2.5.3. Procédures de nomination 13
  - 2.5.4. Révision de la politique de sécurité 14
- 2.6. Données à caractère personnel 14
- 2.7. Gestion des risques 14
- 2.8. Obligations du personnel 14
- 2.9. Tiers 15

3. LÉGISLATION APPLICABLE **15**

1. DÉCLARATION DE PRINCIPES

CYPE INGENIEROS S.A., ci-après dénommée **LA SOCIÉTÉ,** est une entreprise ayant plus de 40 ans d'expérience dans la commercialisation, la distribution et le service après-vente de logiciels techniques destinés aux **professionnels de l'Architecture et de l'Ingénierie de la Construction**. LA SOCIÉTÉ offre une variété de logiciels innovants conçus pour aider les professionnels à effectuer des calculs structuraux, à gérer des projets et à contrôler la qualité de manière efficace et précise, tant au niveau national qu'international.

En raison de notre activité, LA SOCIÉTÉ est consciente que l'information est un actif de grande valeur pour notre organisation et qu'elle nécessite donc une protection et une gestion adéquates afin d'assurer la continuité de notre secteur d'activité et de minimiser les dommages éventuels causés par des défaillances au niveau de l'intégrité, de la disponibilité et de la confidentialité de l'information. De même, la législation actuelle sur la protection des données personnelles (règlement européen RGPD et règlement espagnol de protection des données personnelles et garantie des droits numériques LOPDGDD) et l'engagement de LA SOCIÉTÉ envers ses clients signifient que nous sommes particulièrement conscients du traitement des données personnelles auxquelles nous avons accès dans le cadre de nos activités.

À cette fin, LA SOCIÉTÉ établit un ensemble d'activités de gestion visant à préserver les principes de confidentialité, d'intégrité, de disponibilité, d'authenticité, de traçabilité et de conformité réglementaire des informations. À leur tour, ces principes sont définis comme suit :

- **Confidentialité** : c'est la propriété qui garantit que l'accès à l'information ne peut être exercé que par les personnes autorisées à le faire.
- **Intégrité** : c'est la propriété qui permet de sauvegarder l'exactitude et l'exhaustivité des actifs informationnels.
- **Disponibilité** : c'est la qualité qui garantit que les personnes autorisées peuvent accéder à l'information et la traiter à tout moment lorsqu'elles en ont besoin.
- **Authenticité** : c'est la propriété ou la caractéristique selon laquelle une entité est bien celle qu'elle prétend être, ou qui garantit la source d'où proviennent les données.
- **Traçabilité** : c'est la propriété ou la caractéristique selon laquelle les actions d'une entité peuvent être retracées jusqu'à cette seule entité.
- **Conformité réglementaire** : c'est la propriété qui garantit que l'information est gérée conformément aux principes éthiques, professionnels et juridiques établis par les réglementations applicables dans chaque contexte.

Les systèmes doivent être protégés contre les menaces qui évoluent rapidement et qui sont susceptibles d'avoir un impact sur les informations et les services. Pour se défendre contre

ces menaces, une stratégie qui s'adapte à l'évolution de l'environnement est nécessaire pour assurer la continuité de la fourniture des services.

Cela implique que les différents départements doivent appliquer les mesures de sécurité minimales requises par la réglementation espagnole sur la sécurité dans l'utilisation des médias électroniques liés à l'administration publique « Esquema Nacional de Seguridad » (ci-après ENS), ainsi que surveiller en permanence les niveaux de prestation de services, suivre et analyser les vulnérabilités signalées, et préparer une réponse efficace aux incidents afin d'assurer la continuité des services fournis.

Les différents services de l'organisation doivent veiller à ce que la sécurité fasse partie intégrante de chaque étape du cycle de vie du système, depuis la conception jusqu'au déclassement, en passant par le développement, les décisions d'achat et les activités opérationnelles. Les exigences en matière de sécurité et les besoins de financement doivent être identifiés et inclus dans la planification, les appels d'offres et les documents d'appel d'offres pour les projets TIC.

Les départements doivent être prêts à prévenir, détecter, réagir et récupérer les incidents, conformément à l'article 8 de l'ENS.

La protection de la vie privée fait partie intégrante de ce qui précède. Les systèmes de LA SOCIÉTÉ traitent des données personnelles sensibles et, par conséquent, la protection de la vie privée est un pilier essentiel dans le cadre d'un système de gestion de la sécurité de l'information (SGSI) et est une nécessité sociale que les entreprises doivent respecter et protéger, ainsi qu'un sujet de législation et/ou de réglementation spécifique dans le monde entier.

1.1. Objectifs généraux

La politique de sécurité fournit la base pour définir et délimiter les objectifs et les responsabilités pour les diverses actions techniques, juridiques et organisationnelles requises pour garantir la sécurité et la confidentialité des informations, conformément au cadre juridique applicable et aux politiques globales et spécifiques de LA SOCIÉTÉ, ainsi qu'aux procédures définies.

Ces actions, du point de vue de la sécurité et de la confidentialité, sont sélectionnées et implémentées sur la base d'une analyse des risques et de l'équilibre entre les risques acceptables et le coût des mesures.

L'objectif de la politique de sécurité est d'établir le cadre d'action nécessaire pour protéger les ressources d'information et de données contre les menaces, internes ou externes, délibérées ou accidentelles.

Les informations et les données peuvent exister dans une variété de formats, qu'ils soient électroniques, sur papier ou sur d'autres supports, et comprennent parfois des données critiques sur les opérations, les stratégies ou les activités de LA SOCIÉTÉ et de ses clients,

y compris, le cas échéant, des données sensibles comme l'exigent les réglementations en matière de protection des données à caractère personnel. La perte, la corruption ou le vol d'informations ou des systèmes qui les gèrent ont un impact important sur LA SOCIÉTÉ.

LA SOCIÉTÉ est convaincue qu'une gestion efficace de la sécurité de l'information et de la vie privée permet à l'organisation de comprendre pleinement les risques auxquels l'information est exposée et d'agir de manière appropriée, ainsi que d'être en mesure de répondre et de s'adapter efficacement aux exigences croissantes des régulateurs, des lois et, bien entendu, de ses clients.

1.2. Engagement de la direction générale

Le système de gestion de la sécurité de l'information a pour objet de garantir que les risques liés à la sécurité de l'information et à la protection de la vie privée sont connus, acceptés, gérés et réduits au minimum d'une manière documentée, systématique, structurée, reproductible, gérable et adaptable, et qu'ils sont adaptés à l'évolution des risques, de l'environnement et des technologies.

À cette fin, la direction déclare l'engagement de LA SOCIÉTÉ à :

- Établir comme objectif principal le service de voyages à l'étranger dans le respect absolu des normes de qualité, en préservant l'information, avec une attention particulière à la sensibilité des données personnelles traitées, avec toutes les mesures nécessaires à sa portée.
- Appliquer le principe de l'amélioration continue à tous les processus de l'organisation, avec l'objectif supplémentaire d'atteindre le plus haut degré de satisfaction des clients.
- Assurer la conformité aux exigences légales et réglementaires applicables (en particulier celles relatives à la protection des données à caractère personnel), ainsi que celles que l'organisation a volontairement assumées.
- Promouvoir la participation, la communication, l'information et la formation de l'équipe professionnelle afin qu'elle se sente impliquée dans le travail de l'organisation dans son ensemble.
- Promouvoir un engagement de responsabilité parmi les membres de l'équipe conformément aux exigences de qualité, ainsi qu'à celles relatives à la vie privée et à la sécurité de l'information convenues tant en interne qu'avec les clients, par le biais de formations et d'actions de sensibilisation appropriées et régulières.
- Assurer la continuité de l’entreprise en élaborant des plans de continuité des activités conformément à des méthodologies reconnues.

- Effectuer et réviser périodiquement une analyse des risques basée sur des méthodes reconnues qui nous permettent d'établir le niveau à la fois de la confidentialité des données personnelles et de la sécurité des informations au niveau général et des projets et services en cours, et de minimiser les risques en développant des politiques spécifiques, des solutions techniques et des accords contractuels avec des organisations spécialisées.

- Informer les parties intéressées.

- Sélectionner les fournisseurs et les sous-traitants sur la base de critères liés à la protection de la vie privée et à la sécurité de l'information.

En ce qui concerne spécifiquement la protection des données à caractère personnel, LA SOCIÉTÉ s'engage à respecter les principes énoncés dans la législation pertinente. Ces principes sont les suivants :

- **Principe de « légalité, transparence et loyauté »**. Les données doivent être traitées de manière légale, équitable et transparente pour la personne concernée.

- **Principe de « finalité »**. Les données doivent être traitées pour une ou plusieurs finalités déterminées, explicites et légitimes, et les données collectées pour des finalités déterminées, explicites et légitimes ne peuvent être traitées ultérieurement de manière incompatible avec ces finalités.

- **Principe de « minimisation des données »**. Appliquer des mesures techniques et organisationnelles pour garantir que seules les données nécessaires à chacune des finalités spécifiques du traitement sont traitées, en réduisant l'étendue du traitement et en limitant la période de stockage et son accessibilité à ce qui est nécessaire.

- **Principe d'« exactitude »**. Des mesures raisonnables doivent être prises pour que les données soient mises à jour, effacées ou modifiées rapidement si elles sont inexactes au regard des finalités pour lesquelles elles sont traitées.

- **Principe de « limitation de la durée de conservation »**. La conservation des données doit être limitée dans le temps à la réalisation des finalités pour lesquelles les données sont traitées.

- **Principe de « sécurité »**. Effectuer une analyse des risques visant à déterminer les mesures techniques et organisationnelles nécessaires pour garantir l'intégrité, la disponibilité et la confidentialité des données à caractère personnel traitées.

- **Principe de « responsabilité active » ou de « responsabilité démontrée »**. Maintenir en permanence une diligence raisonnable pour protéger et garantir les droits et libertés des personnes physiques dont les données sont traitées sur la base d'une analyse des risques que le traitement représente pour ces droits et

libertés, afin de pouvoir garantir et démontrer que le traitement est conforme aux dispositions du RGPD et du règlement espagnol LOPDGDD.

- Diriger, soutenir et superviser le système de gestion de la sécurité de l'information, tel qu'il est établi dans le décret royal 311/2022 et ses modifications ultérieures, et s'efforcer d'atteindre ses objectifs.

La direction de LA SOCIÉTÉ s'engage à soutenir et à promouvoir les principes énoncés dans la présente politique, pour laquelle elle demande au personnel de l'entreprise d'assumer et de respecter les dispositions du système de gestion documenté pour l'ENS.

1.3. Développement de la politique de sécurité

La présente politique de sécurité complète les politiques de sécurité de LA SOCIÉTÉ dans différents domaines et est développée au moyen de règlements de sécurité qui traitent d'aspects spécifiques. Le règlement de sécurité est mis à la disposition de tous les membres de l'organisation qui ont besoin de le connaître, et en particulier de ceux qui utilisent, exploitent ou administrent les systèmes d'information et de communication.

La documentation relative à la sécurité de l'information est classée en trois niveaux, de sorte que chaque document d'un niveau s'appuie sur ceux d'un niveau supérieur :

- **Premier niveau** : politique de sécurité.
- **Deuxième niveau** : normes et procédures de sécurité.
- **Troisième niveau** : rapports, registres et preuves électroniques.

2. POLITIQUE

2.1. Prévention

Les départements doivent éviter, ou du moins empêcher autant que possible, que des informations ou des services soient compromis par des incidents de sécurité. À cette fin, ils doivent implémenter les mesures de sécurité minimales déterminées par l'ENS, ainsi que tout contrôle supplémentaire identifié par une évaluation des menaces et des risques. Ces contrôles, ainsi que les rôles et responsabilités de l'ensemble du personnel en matière de sécurité, doivent être clairement définis et documentés.

Pour assurer la conformité avec la politique, les départements doivent :

- Autoriser les systèmes avant leur mise en service.
- Évaluer régulièrement la sécurité, y compris les changements de configuration effectués systématiquement.
- Demander un examen périodique par des tiers afin d'obtenir une évaluation indépendante.

2.2. Détection

Étant donné que les services peuvent se dégrader rapidement en raison d'incidents, allant d'un simple ralentissement à une immobilisation, les services doivent surveiller l'exploitation en permanence afin de détecter les anomalies dans les niveaux de fourniture de services et d'agir en conséquence, comme le prévoit l'article 9 de l'ENS.

Le suivi est particulièrement important lors de l'établissement des lignes de défense conformément à l'article 8 de l'ENS. Des mécanismes de détection, d'analyse et de rapport doivent être mis en place pour atteindre les parties responsables de manière régulière et lorsqu'il y a un écart significatif par rapport aux paramètres qui ont été préétablis comme étant normaux.

2.3. Réponse

Les départements doivent :

- Mettre en place des mécanismes permettant de réagir efficacement aux incidents de sécurité.
- Désigner un point de contact pour les communications relatives aux incidents détectés dans d'autres départements ou d'autres organismes.
- Établir des protocoles pour l'échange d'informations relatives à l'incident. Cela inclut les communications bilatérales avec les équipes d'intervention en cas d'urgence informatique (CERT en anglais).

2.4. Récupération

Pour garantir la disponibilité des services essentiels, les départements doivent élaborer des plans de continuité des systèmes dans le cadre de leur plan global de continuité des activités et de leurs activités de récupération.

2.5. Organisation de la sécurité

Cette politique s'applique à tous les systèmes de LA SOCIÉTÉ et à tous les membres de l'organisation, sans exception.

LA SOCIÉTÉ s'engage à fournir ses services de manière gérée et en conformité avec les exigences définies dans son système de gestion intégré afin d'assurer un service ininterrompu conformément aux exigences de disponibilité, de sécurité et de qualité pour les clients.

En raison de notre activité, nous savons, au sein de LA SOCIÉTÉ, que l'information est un actif de grande valeur pour notre organisation, en particulier pour nos clients, et qu'elle nécessite donc une protection et une gestion adéquates afin d'assurer la continuité de notre secteur d'activité et de minimiser les dommages éventuels causés par des défaillances dans la sécurité de l'information.

À cette fin, l'organisation :

- Protège de manière adéquate la confidentialité, la disponibilité, l'intégrité, l'authenticité et la traçabilité de ses actifs informationnels en introduisant une série de contrôles pour gérer les risques de sécurité pertinents.
- Fait de la protection et de la sauvegarde des clients et de leurs données une priorité de l'entreprise.
- Établit, implémente, surveille, maintient et améliore continuellement sa gestion de la sécurité de l'information dans le cadre de son approche plus large de la gestion de l'entreprise, et maintient une certification accréditée selon les standards appropriés.
- Gère toute atteinte à la sécurité de l'information de manière opportune et responsable, et investit dans des stratégies appropriées de détection, de réaction et de remédiation.
- Teste, à intervalles réguliers, les contrôles de la sécurité de l'information et les réponses aux scénarios susceptibles de constituer une menace pour ses activités.
- Fournit à l'organisation les ressources adéquates pour mettre en place, maintenir et améliorer l'environnement de sécurité en fonction de l'évolution du paysage des risques.
- Investit dans les compétences du personnel pour qu'il puisse s'acquitter de ses tâches et lui fournit une formation et une sensibilisation appropriées à son rôle et aux informations auxquelles il a accès.
- Veille à ce que ses fournisseurs et organisations partenaires fassent de même et à ce qu'ils fixent et appliquent des règles de sécurité aux personnes à qui des informations sont transmises.

2.5.1. Comité de sécurité

Les membres du comité de sécurité sont désignés dans une charte qui indique la personne désignée et la fonction qu'elle occupe.

Le secrétaire du comité de sécurité est le RESPONSABLE DE LA SÉCURITÉ et exerce les fonctions suivantes :

- Convoquer les réunions du comité de sécurité.
- Préparer les sujets à traiter lors des réunions du comité, en fournissant des informations nécessaires à la prise de décision.
- Rédiger les comptes-rendus des réunions.
- Exécuter les décisions du comité directement ou par délégation.
- Le comité de sécurité fait rapport au directeur général.

Le comité de sécurité a les fonctions suivantes :

- Répondre aux préoccupations de la direction générale et des différents départements.
- Rendre compte régulièrement de l'état de la sécurité de l'information à la direction générale.
- Promouvoir l'amélioration continue du système de gestion de la sécurité de l'information.
- Élaborer la stratégie de l'organisation pour l'évolution de la sécurité de l'information.
- Coordonner les efforts des différents secteurs en matière de sécurité de l'information, afin d'assurer la cohérence des efforts, de les aligner sur la stratégie décidée et d'éviter les duplications.
- Élaborer (et réviser régulièrement) la politique de sécurité pour approbation par la direction.
- Approuver les règles de sécurité de l'information.
- Coordonner toutes les fonctions de sécurité de l'organisation.
- Veiller au respect des réglementations légales et sectorielles applicables.
- Veiller à ce que les activités de sécurité soient alignées sur les objectifs de l'organisation.
- Coordonner les plans de continuité des différents domaines, afin de garantir une action sans faille en cas d'activation de ces plans.
- Coordonner et approuver, le cas échéant, les propositions de projets reçues des différents domaines de sécurité, en contrôlant et en présentant régulièrement l'état d'avancement des projets et en annonçant les déviations éventuelles.
- Recevoir les préoccupations de la direction de l'entité en matière de sécurité et les transmettre aux responsables des départements concernés, en obtenant d'eux les réponses et les solutions correspondantes qui, une fois coordonnées, doivent être communiquées à la direction.
- Recueillir les rapports réguliers des responsables de la sécurité des départements sur l'état de la sécurité de l'organisation et les incidents éventuels. Ces rapports sont consolidés et résumés pour être communiqués à la direction de l'entité.
- Coordonner et répondre aux préoccupations transmises par les responsables départementaux de la sécurité.

- Définir, dans le cadre de la politique de sécurité de l'entreprise, l'attribution des rôles et les critères permettant d'obtenir les garanties nécessaires en matière de séparation des fonctions.
- Élaborer et approuver les exigences en matière de formation et de qualification des administrateurs, des opérateurs et des utilisateurs du point de vue de la sécurité de l'information.
- Contrôler les principaux risques résiduels assumés par l'organisation et recommander des actions possibles pour y remédier.
- Contrôler les performances des processus de gestion des incidents de sécurité et recommander des actions possibles pour y remédier. En particulier, assurer la coordination des différents domaines de sécurité dans la gestion des incidents de sécurité de l'information.
- Promouvoir des audits périodiques pour vérifier le respect des obligations de l'organisme en matière de sécurité.
- Approuver les plans visant à améliorer la sécurité de l'information de l'organisation. En particulier, assurer la coordination des différents plans qui peuvent être mis en œuvre dans différents domaines.
- Donner la priorité aux mesures de sécurité lorsque les ressources sont limitées.
- Veiller à ce que la sécurité de l'information soit prise en compte dans tous les projets, depuis les spécifications initiales jusqu'à la mise en œuvre. En particulier, veiller à la création et à l'utilisation de services horizontaux qui réduisent les duplications et soutiennent le fonctionnement harmonieux de tous les systèmes TIC.
- Résoudre les conflits de responsabilité qui peuvent survenir entre les différents responsables et/ou entre les différents domaines de l'organisation.

2.5.2. Rôles : Fonctions et responsabilités

Les rôles des responsables de l'organisation sont décrits ci-dessous :

Responsable de l'information

Ses fonctions sont les suivantes :

- Responsabilité en dernier ressort de l'usage qui est fait de certaines informations et, par conséquent, de leur protection.

- Responsabilité en dernier ressort de toute erreur ou négligence entraînant un incident de confidentialité ou d'intégrité (pour la protection des données) et de disponibilité (pour la sécurité de l'information).
- Établir les exigences en matière de sécurité de l'information.
- Déterminer et approuver les niveaux de sécurité de l'information.
- Approuver la catégorisation du système en ce qui concerne les informations.
- Remplir les fonctions qui seront indiquées dans les documents relevant du champ d'application de l'ENS.

Responsable du service

Ses fonctions sont les suivantes :

- Établir les exigences de sécurité du service.
- Déterminer les niveaux de sécurité des services.
- Approuver la catégorisation du système en ce qui concerne les services.
- Remplir les fonctions indiquées dans les documents relevant du champ d'application de l'ENS.

Responsable de la sécurité

Ses fonctions sont les suivantes :

- Maintenir la sécurité des informations traitées et des services fournis par les systèmes d'information dans son domaine de responsabilité, conformément à la politique de sécurité de l'information de l'organisation.
- Promouvoir la formation et la sensibilisation à la sécurité de l'information dans son domaine de responsabilité.
- Approuver la déclaration d'applicabilité.
- Canaliser et superviser le respect des exigences de sécurité du service fourni ou de la solution qu'il propose, ainsi que les communications relatives à la sécurité de l'information et à la gestion des incidents pour le périmètre dudit service (PoC).
- Remplir les fonctions qui seront indiquées dans les documents relevant du champ d'application de l'ENS.

Le responsable de la sécurité est le secrétaire du comité de sécurité, avec les fonctions indiquées au point 2.5.1 de la présente politique.

Responsable du système

Ses fonctions sont les suivantes :

- Développer, exploiter et maintenir le système d'information tout au long de son cycle de vie, y compris ses spécifications, son installation et la vérification de son bon fonctionnement.
- Définir la topologie et la gestion du système d'information, en établissant les critères d'utilisation et les services disponibles.
- Veiller à ce que les mesures de sécurité soient correctement intégrées dans le cadre général de sécurité.
- Le pouvoir de proposer la suspension du traitement de certaines informations ou de la fourniture d'un certain service si de graves lacunes en matière de sécurité sont identifiées et pourraient affecter le respect des exigences établies.
- Remplir les fonctions indiquées dans les documents relevant du champ d'application de l'ENS.

Responsable de la confidentialité

Ses fonctions sont les suivantes :

- Coordonner tous les aspects liés à l'adéquation des actions de LA SOCIÉTÉ en ce qui concerne la protection des données à caractère personnel.
- Coordonner, avec le responsable de la sécurité, la conformité avec l'ENS en ce qui concerne la protection des données à caractère personnel.

2.5.3. Procédures de nomination

Le responsable de la sécurité est nommé par le comité de sécurité. La nomination est réexaminée tous les deux ans ou lorsque le poste devient vacant.

De même, les autres postes indiqués dans la section précédente sont nommés par le comité de sécurité sur la base d'un compte-rendu de réunion.

2.5.4. Révision de la politique de sécurité

Le comité de sécurité est responsable de la révision annuelle de la présente politique de sécurité et de la proposition de la réviser ou de la maintenir. Elle est approuvée par la direction générale et diffusée de manière à ce que toutes les parties concernées en aient connaissance.

2.6. Données à caractère personnel

LA SOCIÉTÉ, dans le cadre de la fourniture de ses services, traite des données personnelles particulièrement sensibles.

La documentation correspondante, à laquelle seules les personnes autorisées auront accès, contient les enregistrements de l'activité de traitement des données concernées et des contrôleurs de données correspondants. Tous les systèmes d'information de LA SOCIÉTÉ doivent être conformes aux niveaux de sécurité requis par les réglementations relatives à la nature et à la finalité des données personnelles.

2.7. Gestion des risques

Tous les systèmes soumis à cette politique effectueront une analyse des risques, en évaluant les menaces et les risques auxquels ils sont exposés. Cette analyse est répétée :

- Régulièrement, au moins une fois par an ;
- Lorsque les informations traitées changent ;
- Lorsque les services fournis changent ;
- Lorsqu'un incident de sécurité grave se produit ;
- Lorsque des vulnérabilités graves sont signalées.

Pour harmoniser les analyses de risque, le comité de sécurité établit une évaluation de référence pour les différents types d'informations traitées et les différents services fournis. Le comité de sécurité rationalise la disponibilité des ressources pour répondre aux besoins de sécurité des différents systèmes en encourageant les investissements horizontaux.

2.8. Obligations du personnel

Tous les membres de LA SOCIÉTÉ sont tenus de connaître et de respecter la présente politique de sécurité et le règlement de sécurité, et il incombe au comité de sécurité de fournir les moyens nécessaires pour s'assurer que les informations parviennent aux personnes concernées.

Tous les membres de LA SOCIÉTÉ assisteront à une session de sensibilisation à la sécurité de l'information au moins une fois par an. Un programme de sensibilisation continue sera mis en place pour répondre aux besoins de tous les membres de LA SOCIÉTÉ, en particulier des nouvelles recrues.

Les personnes responsables de l'utilisation, de l'exploitation ou de l'administration des systèmes recevront une formation sur l'exploitation sûre des systèmes dans la mesure où cela est nécessaire à l'exécution de leur travail. La formation est obligatoire avant d'assumer

une responsabilité, qu'il s'agisse de leur première mission ou d'un changement d'emploi ou de responsabilités professionnelles.

2.9. Tiers

Lorsque LA SOCIÉTÉ fournit des services à d'autres organisations publiques ou privées ou traite des informations provenant d'autres organisations publiques ou privées, celles-ci seront informées de la présente politique de sécurité, des canaux seront établis pour informer et coordonner les comités de sécurité respectifs et des procédures seront établies pour réagir aux incidents de sécurité.

Lorsque LA SOCIÉTÉ utilise les services de tiers ou transfère des informations à des tiers, ceux-ci seront informés de la présente politique de sécurité et des règlements de sécurité qui s'appliquent à ces services ou informations. Ce tiers sera soumis aux obligations énoncées dans ces règlements et pourra développer ses propres procédures d'exploitation pour s'y conformer. Des procédures spécifiques de notification et de résolution des incidents sont établies. Il convient de veiller à ce que le personnel du tiers soit suffisamment sensibilisé à la sécurité, au moins au niveau défini dans la présente politique.

Lorsqu'un aspect de la politique ne peut être satisfait par un tiers comme décrit dans les paragraphes précédents, un rapport du responsable de la sécurité est exigé, décrivant les risques encourus et la manière dont ils seront traités. Ce rapport doit être approuvé par les responsables des informations et des services concernés avant de poursuivre la procédure.

3. LÉGISLATION APPLICABLE

Les lois considérées comme applicables au SGSI sont énumérées ci-dessous, accompagnées d'une définition du domaine responsable de l'évaluation de leur impact sur l'organisation.

LOI / RÉGULATION	RESPONSABILITÉ
Loi (Espagne) 39/2015, du 1er octobre, sur la procédure administrative commune des administrations publiques.	Conseil juridique
Loi (Espagne) 40/2015, du 1er octobre. Établit et réglemente les bases du régime juridique des administrations publiques, les principes du système de responsabilité des administrations publiques et le pouvoir d'imposer des sanctions, ainsi que l'organisation et le fonctionnement de l'administration générale de l'État et de son secteur public institutionnel pour le développement de ses activités.	Conseil juridique

Décret royal (Espagne) 311/2022, du 3 mai, qui régit la sécurité dans l'utilisation des médias électroniques liés à l'administration publique « Esquema Nacional de Seguridad ».	Conseil juridique
Loi organique (Espagne) 1/2015, du 30 mars, modifiant la loi organique 10/1995, du 23 novembre, sur le code pénal.	Conseil juridique
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.	Conseil juridique
Loi organique (Espagne) 3/2018, du 5 décembre, sur la protection des données à caractère personnel et la garantie des droits numériques.	Conseil juridique
Loi (Espagne) 34/2002 sur les services de la société de l'information (LSSI).	Conseil juridique
Loi (Espagne) 2/1996, du 12/04/1996, approuvant le texte révisé de la loi sur la propriété intellectuelle, régularisant, clarifiant et harmonisant les dispositions légales en vigueur en la matière.	Conseil juridique
Loi (Espagne) 17/2001, du 7 décembre, sur les marques.	Conseil juridique
Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.	Conseil juridique
Loi (Espagne) 6/2020, du 11 novembre, réglementant certains aspects des services de confiance électroniques.	Conseil juridique