tinsa

POLITIQUE DE SÉCURITÉ ET DE CONFIDENTIALITÉ DES DONNÉES

TABLE DES MATIÈRES

Feuille de suivi des modifications
Classification : Interne

Version	**Date**	**Mis à jour par (révisé par)**	**Notes et détails de la modification**
1	21/04/2022	Manuel Pantoja (Responsable SGSI)	Version initiale
1.2	27/12/2022	Manuel Pantoja (Responsable SGSI)	La section 4.5.1 « Identification et authentification des utilisateurs » est mise à jour ; le nombre minimum de caractères est porté de neuf (9) à douze (12).
1.3	11/10/2023	Manuel Pantoja (Responsable SGSIP)	Mise à jour selon la norme ISO 27701

DÉCLARATION DE POLITIQUE DE SÉCURITÉ ET DE CONFIDENTIALITÉ DES INFORMATIONS

La Politique de sécurité et de confidentialité établit les lignes directrices et les principes définis par TINSA TASACIONES INMOBILIARIAS, S.A.U., ci-après dénommée **TINSA**, qui s'étend à toutes les entreprises faisant partie du groupe **TINSA**, conformément aux dispositions de la déclaration d'applicabilité, afin de garantir la protection de l'information, la confidentialité et la protection des données à caractère personnel faisant l'objet d'un traitement, ainsi que le respect des objectifs de sécurité définis, assurant ainsi la confidentialité, l'intégrité et la disponibilité des systèmes d'information et, bien entendu, garantissant le respect de toutes les obligations légales applicables.

La direction de **TINSA**, consciente de l'importance de la sécurité de l'information dans le cadre professionnel, assume et prend les engagements suivants concernant le Système de gestion de la sécurité de l'information et de la confidentialité (SGSIP) :

a) Veiller à ce que des objectifs en matière de sécurité de l'information et de protection de la vie privée soient fixés, toujours en accord avec la stratégie de l'entreprise.
b) Veiller à ce que les exigences en matière de sécurité soient intégrées dans les processus de l'organisation.
c) Garantir les ressources nécessaires au système de gestion.
d) Communiquer l'importance d'une gestion efficace de la sécurité de l'information, conforme aux exigences du système de gestion de la sécurité de l'information.
e) S'assurer que le système de gestion de la sécurité de l'information et de la confidentialité atteint les résultats escomptés.
f) Diriger et soutenir les collaborateurs afin de contribuer à l'efficacité du système de gestion de la sécurité de l'information et de la confidentialité.
g) Promouvoir l'amélioration continue du système de gestion.
h) Soutenir les rôles concernés afin qu'ils puissent faire preuve de leadership dans leurs domaines de responsabilité.
i) Veiller au respect de la législation et/ou de la réglementation applicable en matière de protection des données à caractère personnel, notamment, à titre indicatif et non limitatif, les principes et dispositions établis dans le Règlement général sur la protection des données (RGPD) et la Loi organique sur la protection des données et la garantie des droits numériques (LOPDGDD).
j) Garantir le respect des clauses contractuelles convenues entre l'organisation et ses partenaires, ses sous-traitants et les tiers concernés, tels que les clients, en veillant à ce que l'obligation d'information soit respectée et que les responsabilités incombant à chaque partie soient clairement attribuées.

À cette fin, la direction veillera à ce que le personnel de **TINSA** respecte les réglementations, politiques, procédures et instructions relatives à la sécurité de l'information et à la confidentialité.

Grâce à la mise en place de son système de gestion de la sécurité de l'information et de la confidentialité, **TINSA** vise à garantir les objectifs suivants en matière de sécurité et de confidentialité :

1. Garantir la confidentialité, l'intégrité et la disponibilité des informations.

2. Garantir la confidentialité et la protection des données à caractère personnel traitées dans le cadre des processus et des traitements de données à caractère personnel effectués.

3. Respecter toutes les exigences légales applicables.

4. Disposer d'un plan de continuité permettant de rétablir les processus et les activités en cas d'incident, dans les plus brefs délais.

5. Former et sensibiliser l'ensemble des employés aux questions de sécurité de l'information et de confidentialité.

6. Répondre aux attentes et aux besoins en matière de sécurité des clients, des employés, des fournisseurs et des autres parties prenantes.

7. Gérer correctement tous les incidents survenus.

8. Tous les employés seront informés de leurs fonctions et obligations en matière de sécurité et de confidentialité et sont tenus de les respecter.

9. Améliorer en permanence le SGSIP et, par conséquent, la sécurité de l'information et la confidentialité de l'organisation.

Afin de garantir le bon fonctionnement du système de gestion et de respecter les objectifs et les exigences fixés, la direction de TINSA a désigné un responsable du SGSIP qui veillera au respect des directives définies par la présente politique.

1. OBJECTIF

L'objet de la présente politique est d'établir les lignes directrices générales et l'engagement de la direction afin que l'entreprise gère de manière adéquate la sécurité de l'information et la confidentialité des données qu'elle traite.

Cette politique constitue le cadre de référence du Système de gestion de la sécurité de l'information et de la confidentialité (SGSIP), basé sur la norme ISO 27001, en vigueur chez **TINSA**, ainsi que sur la norme ISO 27701.

2. RÉVISION DE LA POLITIQUE DE SÉCURITÉ ET DE CONFIDENTIALITÉ DE L'INFORMATION

La politique de sécurité et de confidentialité des informations, tout comme les processus du système de gestion, sont révisés régulièrement à intervalles planifiés ou en cas de changements significatifs afin d'assurer leur adéquation, leur efficacité et leur efficience continues. De manière générale, ils sont révisés chaque année dans le cadre du processus d'audit interne du système de gestion.

Il existe des procédures de suivi qui fournissent des informations sur le bon fonctionnement du SGSIP.

La direction joue également un rôle important dans la révision du système, en procédant à une analyse approfondie de celui-ci et en identifiant les améliorations possibles ainsi que les lacunes.

3. COMMUNICATION DE LA POLITIQUE DE SÉCURITÉ ET DE LA CONFIDENTIALITÉ DES DONNÉES

La politique du système de gestion est communiquée en interne par courrier électronique et sera disponible sur le portail des employés.

La déclaration relative à la présente politique sera mise à la disposition des parties prenantes externes à **TINSA** via le site web de l'entreprise.

4. ASPECTS SPÉCIFIQUES DE LA SÉCURITÉ ET DE LA CONFIDENTIALITÉ DES INFORMATIONS

Vous trouverez ci-dessous les exigences générales et les directives relatives aux aspects concrets de la sécurité et de la confidentialité des informations.

Ces exigences doivent être connues et respectées par tous les employés de **TINSA**.

En cas de doute, la personne concernée peut s'adresser directement au responsable du SGSIP pour obtenir une réponse.

4.1 Appareils mobiles

Chaque utilisateur est responsable de l'utilisation et de l'entretien appropriés des appareils dont il a la charge. Il doit prévenir tout vol ou détournement lorsqu'il se trouve en dehors des locaux de l'organisation.

L'utilisateur ne doit en aucun cas modifier les mesures de sécurité configurées, telles que le cryptage ou le mot de passe de verrouillage.

Il existe une politique relative aux appareils des utilisateurs que tous les employés doivent connaître : **« SGSIP_SOA_A06-Politique relative aux appareils des utilisateurs _v1.2 ».**

4.2 Télétravail

En cas de télétravail, l'employé veillera à disposer d'un environnement de travail adapté et à protéger les équipements, supports, systèmes et autres ressources dont il est responsable.

L'employé ne doit permettre l'accès à ces derniers à aucune autre personne extérieure à **TINSA**.

4.3 Sécurité relative aux ressources humaines

Il veillera à ce que tous les employés, sous-traitants et tiers comprennent leurs responsabilités et soient aptes à exercer les fonctions qui leur incombent, ainsi qu'à réduire le risque de vol, de fraude ou d'utilisation abusive des ressources mises à leur disposition.

Il veillera à ce que tous les employés, sous-traitants et tiers soient conscients des menaces et des problèmes qui affectent la sécurité de l'information, ainsi que de leurs responsabilités et obligations, et à ce qu'ils soient prêts à respecter la politique de sécurité de l'organisation dans le cadre de leurs activités professionnelles quotidiennes, afin de réduire le risque d'erreur humaine.

Il veillera à ce que tous les employés, sous-traitants et tiers quittent l'organisation ou changent de poste de manière ordonnée et sans compromettre la sécurité de celle-ci.

4.4 Gestion des actifs

L'utilisation des systèmes de **TINSA** sera réservée aux activités propres à leur poste de travail.

L'utilisation responsable des équipements, supports, réseau et autres ressources internes de l'organisation sera encouragée.

Il incombe aux utilisateurs eux-mêmes de veiller à la bonne conservation des actifs dont ils ont la garde pour l'exercice de leurs fonctions contractuelles.

De même, il existe une politique d'utilisation acceptable au sein de l'organisation qui doit être connue de tous les employés et qui peut être consultée sur le Portail des employés.

4.5 Contrôle d'accès

L'accès aux systèmes d'information de **TINSA** sera contrôlé afin qu'il ne soit accordé qu'au personnel autorisé et dans le respect des conditions de sécurité définies par l'organisation.

L'accès des utilisateurs autorisés sera garanti et l'accès des utilisateurs non autorisés aux systèmes d'information de **TINSA** sera empêché.

4.5.1 Identification et authentification des utilisateurs

Dans les cas où il incombe à l'utilisateur de garantir un mot de passe sécurisé pour accéder à un système d'information, les critères de sécurité minimaux suivants seront respectés :

-L'utilisateur devra modifier son mot de passe lors de sa première connexion au système, car cela lui sera automatiquement demandé ; à défaut, il lui incombera d'effectuer cette modification.

-Il convient d'éviter les noms courants, les numéros d'immatriculation de véhicules, les numéros de téléphone, les noms de membres de la famille, d'amis, etc., ainsi que les dérivés du nom d'utilisateur tels que les permutations ou les changements d'ordre des lettres, les transpositions, les répétitions d'un seul caractère, etc.

-Les mots de passe utilisés dans tout système ou service comporteront au moins douze (12) caractères, en combinant des lettres, des chiffres et des symboles tels que ¡”·$%&/()=?¿.

-Si l'on soupçonne que le mot de passe est connu d'autres utilisateurs, il convient d'en informer l'administrateur système afin qu'il le révoque et le remplace par un nouveau.

-L'ordinateur doit être verrouillé lorsqu'il n'est pas utilisé, ou des mécanismes automatiques doivent être activés, et il ne doit jamais être laissé sans surveillance.

-Une politique de poste de travail rangé et de bureau propre sera appliquée, en veillant à ne pas laisser d'informations confidentielles ou privées à la vue de tous.

Les activités suivantes sont expressément interdites :

-Accéder au système en utilisant l'identifiant et le mot de passe d'un autre utilisateur. La responsabilité de tout accès effectué à l'aide d'un identifiant donné incombe à l'utilisateur auquel cet identifiant a été attribué.

-Partager ou communiquer l'identifiant et le mot de passe permettant d'accéder aux systèmes d'information à une autre personne physique, y compris le personnel de **TINSA**. En cas de non-respect de cette interdiction, l'utilisateur sera seul responsable des actes commis par la personne physique utilisant de manière non autorisée son identifiant.

4.6 Utilisation de contrôles cryptographiques

L'accès non autorisé aux informations sera empêché ; à cette fin, les supports contenant des informations à caractère personnel ou des informations sensibles disposeront d'une partie chiffrée dans laquelle ces données seront stockées.

4.7 Sécurité physique et de l'environnement

Tout type d'accès physique non autorisé, de dommages ou d'intrusions dans les installations et les informations de **TINSA** sera empêché. À cette fin, le document « SGSI-SOA-A11-Sécurité physique et de l'environnement_v1.docx » est disponible et précise les mesures mises en place.

Les mesures de sécurité nécessaires seront prises pour éviter toute perte, tout dommage, tout vol ou toute situation susceptible de mettre en danger les biens ou d'entraîner l'interruption des activités de **TINSA**.

Les clés ne doivent pas être laissées sur les portes, les armoires ou les tiroirs, et les portes ou fenêtres ne doivent pas être laissées ouvertes lorsqu'il n'y a personne au bureau.

Les ordinateurs portables doivent être conservés en permanence par la personne à qui ils sont attribués et ne doivent en aucun cas être laissés au bureau lorsque cette personne s'en absente et que celui-ci se retrouve vide.

4.8 Poste de travail dégagé et écran propre.

Le bureau doit rester exempt de toute information confidentielle lorsque l'utilisateur n'est pas présent. Tout type d'information sur papier ou sur des supports contenant des données confidentielles (données clients, données personnelles, etc.) doit être conservé de manière appropriée afin d'empêcher le vol ou la soustraction de ces informations.

Il ne faut pas tenter de modifier la configuration des équipements afin d'éviter leur mise en veille en cas d'inactivité.

4.9 Utilisation correcte des équipements

Les équipements, téléphones portables, tablettes, supports et autres actifs fournis par **TINSA** doivent être utilisés conformément à leur destination.

La configuration par défaut des actifs fournis ne doit pas être modifiée, sauf indication contraire de la part du responsable du SGSIP.

Il incombe aux utilisateurs eux-mêmes de veiller à la bonne conservation des équipements dont ils ont la garde pour l'exécution de leurs tâches contractuelles.

Il est formellement interdit de remettre à toute personne extérieure à **TINSA** tout support contenant des données auxquelles l'utilisateur a eu accès dans l'exercice de ses fonctions, sans l'autorisation requise.

Les documents sur support papier doivent être conservés et archivés dans les dossiers correspondants. À la fin de la journée de travail, l'utilisateur doit veiller à ne pas laisser de documents sur les bureaux ou en dehors de leurs emplacements d'archivage, qui doivent rester fermés à clé.

De même, il existe une politique d'utilisation acceptable au sein de l'organisation qui doit être connue de tous les employés et qui peut être consultée sur le Portail des employés.

4.10 Opérations

Il est permis d'utiliser les informations auxquelles vous avez accès chez **TINSA** uniquement dans la mesure requise par l'exercice de vos fonctions au sein de l'organisation et vous ne pouvez en disposer d'aucune autre manière ni à d'autres fins.

Les activités suivantes sont expressément interdites :
- Il n'est pas permis d'installer de sa propre initiative un quelconque produit informatique sur le système d'information de **TINSA**. Toutes les applications nécessaires à l'exercice de votre travail seront installées uniquement par le personnel dûment autorisé de l'organisation.

-Tenter de fausser ou d'altérer les journaux (LOG) du système.

- Utiliser le système pour tenter d'accéder à des zones restreintes des systèmes informatiques.

-Tenter d'élever le niveau de privilèges d'un utilisateur dans les systèmes d'information.

-Détruire, altérer, rendre inutilisables ou endommager de toute autre manière les données, programmes ou documents électroniques de **TINSA** ou de tiers.

-Introduire volontairement des programmes, virus, macros, applets, contrôles ActiveX ou tout autre dispositif logique ou séquence de caractères causant ou susceptibles de causer tout type d'altération dans les systèmes informatiques de l'entité ou de tiers.

-L'utilisateur est tenu d'utiliser des programmes antivirus et leurs mises à jour afin d'empêcher l'intrusion dans le système de tout élément destiné à détruire ou à corrompre les données informatiques.

-Introduire, télécharger depuis Internet, reproduire, utiliser ou distribuer des logiciels non expressément autorisés par **TINSA**, ou tout autre type d'œuvre ou de matériel dont les droits de propriété intellectuelle ou industrielle appartiennent à des tiers, sans autorisation préalable.

-Installer des copies illégales de tout programme, y compris les programmes d'entreprise.

-Supprimer sans autorisation l'un des programmes légalement installés par **TINSA**.

-Il est interdit d'utiliser les ressources du système d'information auxquelles vous avez accès à des fins privées ou pour tout autre usage que celui strictement professionnel.

-Il est formellement interdit de fournir à toute personne extérieure à **TINSA** tout support contenant des données auxquelles vous avez eu accès dans l'exercice de vos fonctions, sans l'autorisation requise.

-Il est formellement interdit d'utiliser toute information obtenue en raison de votre statut d'employé de **TINSA** et qui n'est pas nécessaire à l'exercice de vos fonctions.

-Vous ne pouvez divulguer ni utiliser, directement ou par l'intermédiaire de tiers ou d'entreprises, les données, documents, méthodologies, codes d'accès, analyses, programmes et autres informations auxquelles vous avez accès pendant votre relation de travail avec **TINSA**, que ce soit sous support physique que sous forme électronique. Tous les engagements susmentionnés doivent être respectés, même après la cessation de la relation de travail avec **TINSA**.

-En ce qui concerne les documents imprimés, l'utilisateur est responsable de leur récupération, qui doit être effectuée immédiatement, afin d'empêcher tout accès à ces documents par des utilisateurs non autorisés.

-Les documents qui ne sont pas utiles à l'utilisateur doivent être détruits à l'aide des destructeurs de papier disponibles.

4.11 Communications

Les utilisateurs d'Internet doivent s'efforcer de faire et de promouvoir une utilisation efficace des réseaux afin d'éviter tout trafic inutile sur le réseau et toute interférence avec le travail d'autres utilisateurs ou avec d'autres réseaux associés, ainsi qu'avec les services qu'ils offrent.

L'utilisation des systèmes informatiques de **TINSA** pour accéder à des réseaux privés ou publics sera limitée aux sujets directement liés à l'activité et aux missions du poste de travail de l'utilisateur.

Il convient d'utiliser le courrier électronique de manière responsable, ainsi que les informations transmises par ce moyen, en préservant leur confidentialité et leur intégrité.

Tout fichier introduit sur le réseau ou sur le terminal de l'utilisateur par le biais de courriels provenant de réseaux externes doit respecter les exigences énoncées dans le présent règlement, et en particulier celles relatives à la propriété intellectuelle et industrielle ainsi qu'au contrôle des virus ou de tout type de code malveillant.

TINSA se réserve le droit de consulter, après notification préalable, les courriels des utilisateurs du réseau et les fichiers journaux (LOG) du serveur, afin de vérifier le respect des présentes règles et de prévenir toute activité susceptible d'engager la responsabilité civile subsidiaire de l'organisation, en vertu de l'article 20 du Statut des travailleurs qui prévoit l'adoption de mesures de sécurité par l'employeur afin de veiller au respect des obligations professionnelles du salarié.

De même, les activités suivantes sont expressément interdites :

-Tenter de lire, supprimer, copier ou modifier les e-mails ou les fichiers d'autres utilisateurs.
-Entraver volontairement l'accès d'autres utilisateurs au réseau par une utilisation massive des ressources informatiques et télématiques de l'entreprise, ainsi que mener des actions qui endommagent, interrompent ou génèrent des erreurs dans ces systèmes.
-Envoyer des e-mails en masse ou à des fins commerciales ou publicitaires sans le consentement de **TINSA**.
-Utiliser les ressources télématiques de **TINSA**, y compris l'accès à Internet, pour des activités qui ne sont pas directement liées au poste de travail de l'utilisateur.
-Envoyer ou transférer des chaînes de lettres ou des messages de type pyramidal.

4.12 Gestion des incidents

Tout incident en matière de sécurité doit être signalé conformément à la procédure établie. Cette notification sera effectuée via JIRA. Une fois la notification reçue, le responsable de la sécurité sera chargé d'en assurer le suivi, de remplir les notifications prévues par la procédure correspondante, de définir les mesures correctives à prendre et de communiquer à l'utilisateur la résolution ou l'état d'avancement de celle-ci.

4.13 Conformité légale

Toute violation des lois ou des obligations légales, réglementaires ou contractuelles, ainsi que des exigences de sécurité affectant les systèmes d'information de **TINSA**, doit être évitée. L'utilisation de logiciels sans licence correspondante est strictement interdite, de même que l'utilisation, la reproduction, la cession, la transformation ou la communication publique de tout type d'œuvre ou d'invention protégée par la propriété intellectuelle ou industrielle.

Tous les employés concernés doivent connaître et respecter cette réglementation. En cas de détection d'une violation de la sécurité enfreignant la réglementation décrite ici, les sanctions prévues par la loi ou la réglementation applicable seront appliquées.

4.14 Renseignement sur les menaces

La sécurité de l'information et la protection des actifs numériques sont des aspects critiques pour **TINSA.** Dans un environnement de plus en plus complexe et face à des menaces en constante -Retour, il est impératif de mettre en place des mesures efficaces pour réduire les risques et protéger notre infrastructure.

La stratégie de veille des menaces de TINSA a été élaborée dans le but d'établir un cadre solide pour la collecte, l'analyse, la diffusion et l'exploitation des informations relatives aux menaces. Cette stratégie, connue sous le nom de « stratégie de veille des menaces », définit les lignes directrices et les procédures nécessaires pour recueillir des données utiles sur les risques potentiels, évaluer leur pertinence et mettre en œuvre des mesures préventives et correctives appropriées.

4.15 Sécurité de l'information pour les services cloud

TINSA s'engage à garantir la sécurité et la confidentialité des données personnelles que nous gérons via des services cloud. Notre politique d'utilisation responsable des services cloud vise à préserver la confidentialité, l'intégrité, la disponibilité et la protection de ces données, tout en mettant en œuvre des mesures de sécurité rigoureuses.

Pour y parvenir, nous avons mis en place des procédures d'authentification robustes, notamment l'authentification à deux facteurs (2FA), et nous limitons l'accès au personnel autorisé à l'aide de pare-feu et de contrôles d'accès stricts. De plus, nous suivons les meilleures pratiques et les directives recommandées pour configurer correctement les services cloud, en accordant une attention particulière à la protection des données personnelles.

Une séparation effective entre les environnements de développement et de production est essentielle pour minimiser les risques ; c'est pourquoi nous appliquons des contrôles d'accès rigoureux et suivons une politique de gestion des accès clairement définie. De plus, nous effectuons régulièrement des évaluations de vulnérabilité de notre infrastructure cloud à l'aide d'outils à jour, ce qui nous permet d'identifier et de traiter en temps opportun les éventuelles failles en matière de sécurité et de confidentialité des données.

Chez TINSA, nous nous engageons à maintenir un environnement cloud sécurisé et respectueux de la confidentialité des données, et nous continuerons à améliorer nos pratiques et nos mesures de sécurité afin de respecter cet engagement.