Sinari

PSSI – Politique Sécurité

Référence du document : SINARI_PSSI_POLITIQUE_SECURITE V2

Ce document exprime la politique sécurité mise en place au sein des infrastructures SINARI et ses filiales pour garantir un niveau de sécurité convenable à ses clients. Cette politique sécurité est appliquée sur le système d'information interne mais ne représente pas un recueil des mesures mises en place sur les plateformes clientes.

Table des matières

Niveau de confidentialité

☑ Public ☐ Interne ☐ Confidentiel ☐ Restreint

CARTOUCHE DE SUIVI							
Version	Rédacteur	Date	Objet	Date de transmission	Vérificateur	Date de transmission	Approbateur
V01	Alan LE MEUR	07/02/2023	Création d'une politique sécurité	xx/03/2023	Mattis PEPIN	xx/03/2023	Fabien GRELLIER
VO2	DPO 101	07/04/2023	Intégration de dispositions en matière de protection des données personnelles	xx/03/2023	Mattis PEPIN	xx/03/2023	Alan LE MEUR
V03	Mattis PEPIN	14/11/2023	Adaptation du document à la charte graphique SINARI et complétion de parties	14/11/2023	Alan LE MEUR	22/11/2023	DPO101

1 Les grands principes

1.1 Contexte de la sécurité du système d'information chez SINARI

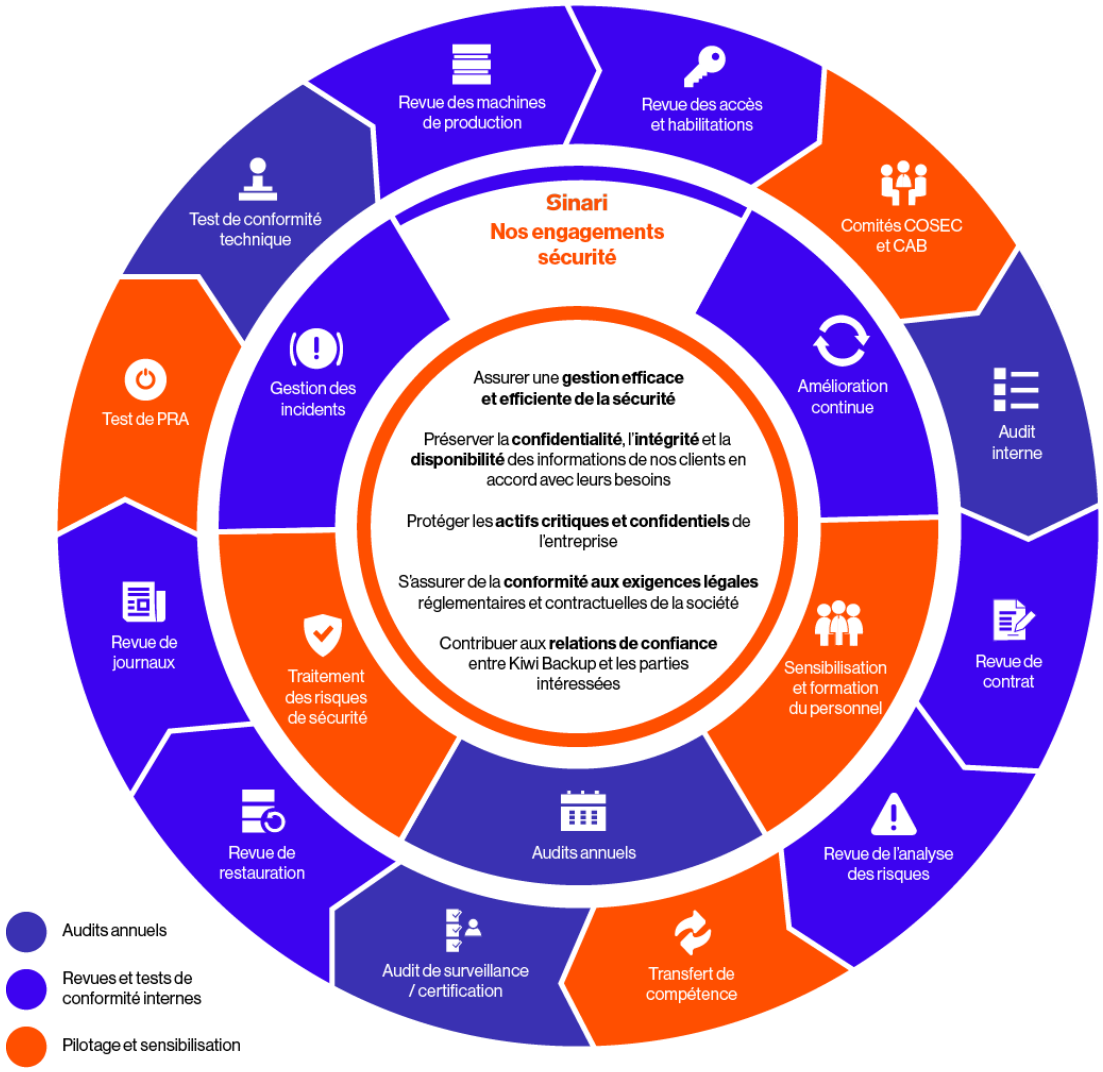
Face à la montée des cyberattaques, de l'utilisation du Cloud (Public ou privé) ou encore des demandes de transformation digitale, nous plaçons la sécurité des données et des infrastructures IT au cœur des enjeux stratégiques de SINARI, notamment pour répondre aux besoins de protection des entreprises sur leur système d'information dans des secteurs très exigeants comme le transport. Ainsi, la préservation de la sécurité informatique de nos clients et donc de leur image et notoriété est un enjeu stratégique capital pour SINARI.

En cohérence avec ses ambitions et celles de nos clients, SINARI a déployé une Politique de Sécurité de son Système d'Information (PSSI) répondant à nos engagements en termes de disponibilité, intégrité, confidentialité et traçabilité.

Notre Système de Management de la Sécurité de l'Information (SMSI), déployé sur nos activités d'hébergement et d'infogérance, nous assure une maîtrise des performances de notre SI tout en satisfaisant aux demandes de nos clients.

L'enjeu de notre SMSI est de nous assurer que nos activités répondent à nos engagements clients en matière de disponibilité, intégrité, confidentialité et traçabilité tout en satisfaisant leurs attentes vis-à-vis de SINARI dans leur développement économique. Notre SMSI atteste également du souhait de SINARI d'être au plus proche de l'ensemble des exigences légales et réglementaires applicables tels que les référentiels ISO 27002, ISO 9001 et 14001.

Par ailleurs, la multiplication des applications et acteurs impose aux hébergeurs infogéreurs une surveillance continue de leur système d'information, en particulier sur des critères tels que la disponibilité, l'intégrité, la confidentialité et la traçabilité (DICT). Nos objectifs fondamentaux sont :



1.2 Revues de la politique de sécurité

La PSSI de SINARI est révisée à minima une fois par an. Elle peut être également révisée en cas de changements significatifs. Dans ce cas-là, la version modifiée sera communiquée à l'ensemble des parties prenantes pertinentes afin de les informer desdits changements.

Les révisions sont à l'initiative du responsable sécurité du système d'information de SINARI, en collaboration avec les propriétaires des actifs identifiés, et sont proposées à la Direction Générale.

La validation d'une nouvelle version, majeure ou mineure, doit être validée par la Direction Générale.

1.3 Domaine d'application du SMSI

Le SMSI de SINARI vise à être en phase avec la certification ISO 27002.

Précisément, le SMSI, applicable au périmètre SINARI, n'exclut aucune clause de la norme ISO : 27002. **Le chapitre développement externalisé de l'ISO 27002 (A.14.2.7), non pratiqué chez SINARI, est lui exclus du périmètre.**

Le périmètre du SMSI inclus également la protection des données à caractère personnel dans le cadre de l'activité d'hébergement et ce en tenant compte de notre obligation de respect du RGPD. Ces prestations d'hébergement comprennent le cas échéant des prestations permettant l'accès direct aux serveurs du client, aux applications et à ses données à caractère personnel.

Dans le cadre de l'activité d'hébergement intégrant par nature des données à caractère personnel, les activités suivantes sont garanties :

1. La mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données à caractère personnel.
2. La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données à caractère personnel
3. La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information
4. La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données à caractère personnel.
5. La sauvegarde des données à caractère personnel.

1.4 Protection des données à caractère personnel

1.4.1 Les grands principes de la protection des données personnelles

La protection des données confiées par les clients, prospects et/ou personnels de SINARI doit être placée au centre des préoccupations de chacun des membres du personnel de SINARI. La PSSI reflète les objectifs de SINARI en matière de sécurité tant de notre système d'information que des données que nous sommes amenés à collecter et traiter.

SINARI traitant des données personnelles au sens du Règlement UE 2016/679 (« Règlement Général sur la Protection des Données » ou « RGPD »), le système d'information garantit la confidentialité de celles-ci de manière à ce que seul le personnel habilité y ait accès.

En matière de protection des données personnelles, les textes suivants s'imposent à SINARI :

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, abrogeant la directive 95/46/CE (règlement général sur la protection des données).
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Code civil et code pénal
- Règlementation CNIL (ex : lignes directrices)

La sécurité des données est un enjeu de conformité de SINARI à ses obligations légales en matière de protection des données. La présente PSSI s'inscrit dans le cadre de cette conformité et assure aux données personnelles un niveau adéquat de protection, calculé sur la base des risques entraînés par un traitement. Dans le cadre du RGPD, les entités du groupe s'exposent à des sanctions administratives, contractuelles, pénales et réputationnelles si les informations collectées se voyaient compromises, indisponibles, volées, ou encore rendues publiques.

En protégeant l'activité par le maintien de l'intégrité des données traitées, stockées, en transit ou bien archivées, le système d'information participe de façon décisive à la mission de chaque entité du groupe.

La protection des données s'articule autour de ces grands principes :

- Principe de licéité et de limitation des traitements
  - Le principe de licéité signifie que tout traitement doit avoir une base légale conforme. Il existe 6 bases légales :
    - Consentement de la personne concernée (Newsletter)
    - Exécution d'un contrat (client)
    - Respect d'une obligation légale (comptabilité, fiche de paie…)
    - Sauvegarde des intérêts vitaux de la personne concernée (Urgence)
    - Mission d'intérêt public
    - Nécessaire aux fins des intérêts légitimes poursuivis du Responsable de traitement
  - Le principe de limitation des traitements signifie que les finalités des traitements doivent être déterminées, explicites et légitimes. Les informations ne doivent pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

  Lorsque SINARI agit en tant que Responsable de traitement, SINARI doit identifier une base légale et une finalité pour chaque traitement de données personnelles mis en œuvre. Lorsque SINARI agit en tant que sous-traitant, ces règles s'appliquent aux clients de SINARI, agissant en tant que Responsables de traitement. SINARI doit également s'assurer

que ses clients ont défini des bases légales et des finalités pour les traitements qu'ils effectuent.

- Principe de minimisation des données : le principe de minimisation des données implique de comprendre ce que l'entreprise collecte pour en assurer son contrôle en s'assurant que ses données sont toutes nécessaires pour assurer l'objectif poursuivi. Les données collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (lien entre finalité et minimisation).

  Le principe de minimisation vise spécifiquement à prévenir la collecte de données non nécessaires au traitement envisagé. Le responsable de traitement doit être en mesure de justifier du caractère nécessaire et proportionné des données effectivement collectées.

- Durée de conservation limitée : Les données personnelles doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.
- Privacy by design et by default : le principe de privacy by default consiste à ne traiter, par défaut, que les données personnelles strictement nécessaires à la finalité poursuivie. Le principe de privacy by design signifie que les entités Sinari doivent mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles dès la conception de leurs solutions.
- Sécurité : les données doivent être traitées de façon à leur garantir une sécurité appropriée, elles doivent être protégées, à l'aide de mesures techniques organisationnelles appropriées, contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle. L'application du principe d'intégrité doit conduire un organisme à garantir que les données personnelles collectées ne seront ni endommagées ni détruites non seulement de son fait mais aussi du fait d'un tiers. Le principe d'intégrité et de confidentialité se traduit par une obligation de sécurité de moyens renforcée à la charge du responsable de traitement (article 32 du RGPD). Ces mesures de sécurité sont d'ailleurs décrites au sein de cette PSSI.

1.4.2 Responsabilités au regard du RGPD

Dans le cadre de son activité, les entités SINARI peuvent être qualifiées de deux façons différentes au sens du RGPD :

- **Les entités SINARI peuvent être sous-traitant :** dans le cadre de ses relations contractuelles, les entités SINARI concluent des contrats avec leurs clients afin de leur fournir des solutions de Transport et Logistique.

  Dans le cadre de la fourniture de ces solutions, les entités SINARI agissent en tant que sous-traitant au sens du RGPD. En effet, les entités SINARI traitent les données de leurs

clients pour le compte de ceux-ci dans le cadre de la fourniture de ces solutions. Le client est alors Responsable de traitement au sens du RGPD et l'entité SINARI est sous-traitant.

- **Les entités SINARI peuvent être responsables de traitement :** dans leur activité, les entités SINARI peuvent aussi agir en tant que Responsables de traitement au regard des traitements effectués pour leur propre activité. Cela concerne par exemple les traitements effectués en matière de gestion du personnel, de gestion des fournisseurs ou de gestion des finances.

Lorsqu'un traitement de données personnelles doit être effectué pour le compte d'un responsable de traitement, certaines obligations s'imposent au sous-traitant et au responsable de traitement. Les entités de SINARI sont soumises à ces obligations, qu'elles agissent en tant que sous-traitants ou en tant que responsables de traitement. Ces obligations s'articulent notamment autour de ces grands principes :

La gestion des demandes de droits des personnes concernées

Les personnes concernées peuvent demander d'exercer leurs droits vis-à-vis de leurs données personnelles, que ce soit au sous-traitant ou au responsable de traitement. Le responsable de traitement facilite l'exercice des droits conférés à la personne concernée. Le sous-traitant, lui, tient compte de la nature du traitement et aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits.

Les utilisateurs finaux des solutions proposées par les entités SINARI peuvent exercer auprès du Responsable de traitement, le client, ou auprès du sous-traitant, l'entité SINARI, leurs droits sur leurs données personnelles. Dans la mesure du possible, des fonctionnalités doivent être mises en œuvre dans les solutions SINARI pour permettre aux clients des entités SINARI de gérer les demandes d'exercice de droits en matière de protection des données personnelles, à savoir la possibilité de supprimer / modifier / anonymiser une ou plusieurs données d'un individu dans le respect des durées règlementaires de conservation du client. Dans la mesure du possible, les entités SINARI doivent tenir compte dans leurs solutions des principes de protection de la vie privée dès la conception et par défaut afin de permettre à leurs clients de gérer les demandes d'exercice de droits en matière de protection des données personnelles.

Les entités SINARI peuvent également agir en tant que Responsables de traitement dans le cadre de leur propre activité. Les personnes concernées par les traitements de données personnelles opérés par les entités SINARI agissant en tant que responsables de traitement peuvent demander d'exercer leurs droits vis-à-vis de leurs données personnelles en adressant un mail à l'adresse : dpo@sinari.fr.

Les durées de conservation des données

Selon le choix du Responsable du traitement, le sous-traitant supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel. Le Responsable de traitement définit des durées de conservation des données pour chaque traitement et s'assure que ces durées sont mises en œuvre.

Les données personnelles ne sont conservées que pour la durée de traitement demandée par le Responsable de traitement, le client de l'entité SINARI. En tant que Responsable de traitement, le client de l'entité SINARI doit définir les durées de conservation des données et l'entité SINARI conserve les données selon les instructions du client. Les entités SINARI doivent s'assurer que les durées de conservation des données sont mises en œuvre pour chaque Responsable de traitement. Le client doit donc donner des instructions à l'entité SINARI concernant les périodes de conservation des données.

Les entités SINARI peuvent également agir en tant que Responsables de traitement dans le cadre de leur propre activité. Dans le cadre de leur activité de Responsable de traitement, les entités SINARI définissent les durées de conservation des données personnelles et le sous-traitant, agissant pour le compte de l'entité SINARI conserve le cas échéant les données selon les instructions de l'entité SINARI.

Notification en cas de violation de données personnelles

En cas de violation de données personnelles, le responsable de traitement doit notifier la violation à l'autorité de contrôle compétente, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. Le sous-traitant, lui, notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

Les entités SINARI agissant en tant que sous-traitant, s'engagent à informer leurs clients, agissant en tant que responsables du traitement, de toute violation de Données à caractère personnel dans le cadre de la fourniture des solutions, dès que possible après avoir pris connaissance de cet événement.

En cas de violation de données à caractère personnel, les entités SINARI coopèrent avec leurs clients, responsables du traitement, et leur prêtent assistance aux fins de la mise en conformité avec les obligations qui incombent au Responsable de traitement en vertu des articles 33 et 34 du RGPD en tenant compte de la nature du traitement et des informations dont disposent les entités SINARI, agissant en tant que sous-traitant. Les entités SINARI doivent assister leurs clients afin rassembler les informations nécessaires pour leur permettre de notifier, le cas échéant, l'incident à une autorité de contrôle et de remédier à l'incident.

Les entités SINARI peuvent également agir en tant que Responsables de traitement dans le cadre de leur propre activité. En cas de violation de données à caractère personnel, les entités SINARI en notifient la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. Les sous-traitants des entités SINARI, eux, notifient au responsable du traitement, l'entité SINARI,

toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

Sous-traitance

Afin de faire appel à un sous-traitant, le responsable de traitement doit s'assurer que celui-ci présente des garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences de la règlementation en matière de protection des données personnelles et garantisse la protection des droits de la personne concernée.

Les solutions des entités SINARI impliquent de faire appel à des sous-traitants et les entités SINARI, en proposant leurs solutions à leurs clients, agissent en tant que sous-traitant. Lorsque l'entité SINARI agit en tant que responsable de traitement, celle-ci met en place des contrats avec ses sous-traitants afin d'encadrer les transferts de données personnel vers ceux-ci. A l'inverse, lorsque l'entité SINARI agit en tant que sous-traitant, des contrats sont également mis en place avec ses clients, agissant en tant que responsable de traitement, afin d'encadrer ces transferts.

Une partie de la PSSI est consacrée à l'encadrement des relations contractuelles avec les tiers et à la sécurisation des transferts de données personnelles, cf. point VI. La gestion des tiers.

2 S’engager : le maitre mot

Basée sur le respect de l’ISO 27002, l’appréciation des risques en matière de sécurité de l’information se déroule à minima annuellement et est pilotée par le Responsable Sécurité des Systèmes d’Informations (RSSI). Cette analyse peut également être déclenchée en cas de changements impactant, tant organisationnels que techniques.

Les résultats sont présentés en revue de direction et la décision quant au seuil d’acceptabilité des risques est décidée puis annoncée dans la lettre d’engagement rédigée par le dirigeant, à l’attention de toutes les parties prenantes.

En découlent des actions qui sont identifiées et validées dans le Plan de Traitement des Risques (PTR) garant du suivi et du déroulement des initiatives en matière de réponse à l’appréciation des risques.

Une veille réglementaire et technologique précise assurée par la DSI groupe ainsi que notre collaboration avec des organismes tels que l’Agence Nationale de la Sécurité Informatique, des entreprises privées nous permettent de mettre en œuvre des actions supplémentaires, de les piloter et de les contrôler dans le temps.

Ainsi, les mesures instaurées sont applicables à différentes activités :

Accès logiques et physiques

- Charte informatique
- Classification et transmission de la donnée
- Contrôle des accès aux données
- Identifiant unique, gestion des privilèges
- Implication du personnel
- Management des actifs
- Usage réseau

La force de notre engagement réside dans la globalisation des pratiques sécurité, quel que soit le périmètre.

2.1 Gouvernance du SMSI

Afin de maintenir un suivi des performances du SMSI de SINARI et alimenter la démarche d’amélioration continue, plusieurs comités ont été instaurés à fréquence planifiée avec des objectifs différents comme présentés dans le tableau ci-dessous.

	Revue de direction 27002	Comité SMSI	Revue de Processus	Audit Interne	Audit Externe
Objectifs	Validation Appréciation des risques Revue stratégique de l'orientation de la politique sécurité et de la pertinence du SMSI	Suivi des Actions du SMSI Suivi des indicateurs Mise à jour documentaire	Evaluation du système de management vis-à-vis des exigences réglementaires	Identifier les écarts, points d'amélioration et opportunités afin d'améliorer les process	Evaluation du système de management en vue du respect de l'ISO 27002
Période	Mois X	Mois X	Mois X	Mois X	Mois X
Fréquence	Annuelle	Trimestrielle	Annuelle	Annuelle	Annuelle
Durée	2h	1h	1h / processus	2h	3h
Eléments d'entrée	CR d'audit interne et externe Appréciation des risques PTR	Suivi avancements des plans d'actions Revue KPI Remontée des disfonctionnements	KPI Processus Procédures Plans d'action	Référentiel ISO 9001 et 27002 Revue de Direction Processus	Périmètre de la certification ISO 27002 Programme d'audit Documents internes
Eléments de sortie	Revue des actions / KPI Définition des objectifs PTR actualisé Evolutions du SMSI	Mise à jour documentaire Plans d'actions Retour aux réclamations	Plan d'action pour mise en conformité éventuelle	Axes d'amélioration définie	CR Préconisations d'amélioration Actions correctives
Pilote	CTO / DSI	Qualité	Auditeur SINARI	ROC / CTO / DSI	Auditeur Externe

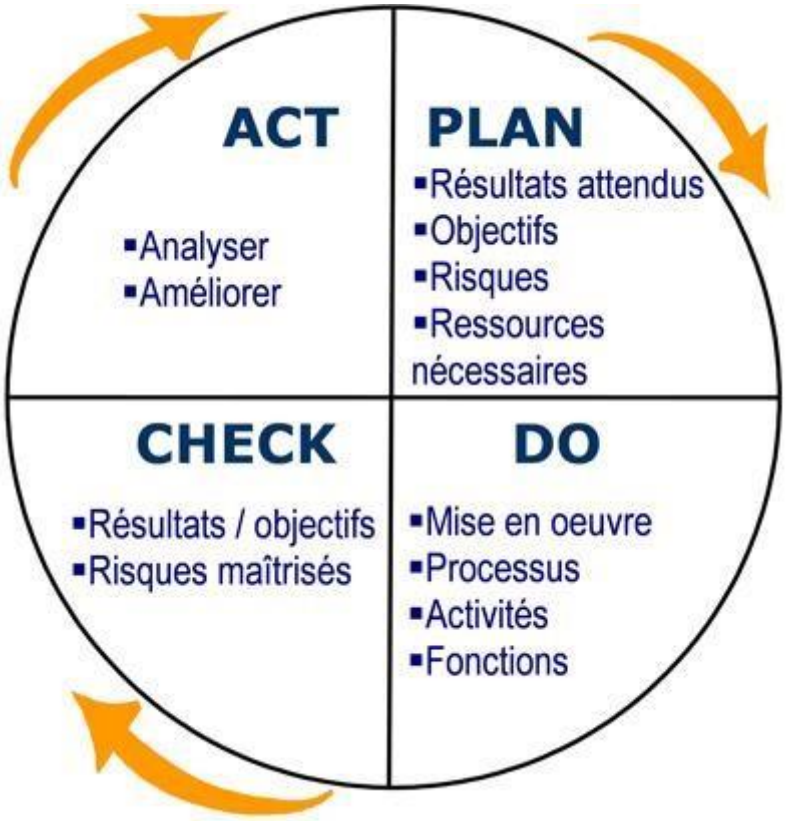
2.2 Amélioration continue

Les Systèmes d'Informations de SINARI font l'objet d'une analyse de risques permettant entre autres, une prise en compte préventive de sa sécurité, adaptée aux enjeux du système considéré. Cette analyse s'inscrit dans une démarche d'amélioration continue et permet de maintenir une maîtrise des risques identifiés.

Les éléments constitutifs du SMSI (processus, procédures…) sont appelés à évoluer dans l'optique d'une amélioration continue.

La pertinence, l'adéquation et l'efficacité du SMSI dans le contexte de l'entreprise sont évalués à fréquence planifiée par le biais notamment d'une gouvernance en matière de sécurité de l'information décrite dans le sous-chapitre précédent.

Ainsi, la démarche d'amélioration continue du SMSI de SINARI s'articule de la manière suivante :



2.3 Rôles et responsabilités et autorités au sein de l'organisation

La direction de SINARI a nommé un RSSI pour s'assurer de la conformité du SMSI aux exigences de la norme ISO 27001 :2013.

Le RSSI s'appuie sur des instances internes pour l'assister dans ses missions. Les rôles et responsabilités ont été définis et communiqués au sein de l'organisation.

Le RSSI rend régulièrement compte à la direction de la performance du SMSI.

Le tableau ci-dessous illustre les différents rôles et responsabilités au sein du SMSI de SINARI.

Direction Générale	▪ Porte la responsabilité de la sécurité des SI SINARI ▪ S'engage sur la disponibilité des ressources et des moyens à mobiliser sur la SSI ▪ Propriétaire de l'ensemble des actifs du SI
CTO	▪ Etablir, mettre en œuvre le PTR ▪ Animer la gouvernance SSI ▪ S'assurer du bon déploiement de la PSSI - Vérifier que les règles soient bien appliquées ▪ Mettre en place les programmes de formation / sensibilisation SSI - Réaliser les revues du plan d'action ▪ Mettre en œuvre les axes d'amélioration ▪ Anime les revues d'analyse de risque
DSI	▪ Se tenir informé de la réglementation ▪ Se tenir informé des failles de sécurité ▪ Être garant de la gestion documentaire liée à la SSI ▪ Soutenir les équipes IT ▪ Gestion des IN / OUT
Équipe IT	▪ Déployer les mesures de ▪ sécurité dans ▪ leurs domaines respectifs
DPO	▪ Assister et conseiller SINARI et ses entités dans leur conformité à la Règlementation en matière de protection des données à caractère personnel ▪ Définir et mettre en place une stratégie de conformité au niveau du groupe et mettre en œuvre des processus internes ▪ Assister et conseiller SINARI et ses entités dans les projets internes et la gestion des relations contractuelles avec leurs clients et prestataires ▪ Former les collaborateurs ▪ Conseiller SINARI et ses entités dans leur gestion des incidents de sécurité impliquant des données personnelles
Référents DPO	▪ Collaborer avec le DPO concernant la conformité des entités SINARI à la Règlementation applicable en matière de protection des données à caractère personnel ▪ Être le point de contact des collaborateurs de chaque entité SINARI en matière de protection des données à caractère personnel

3 Systématiser la sécurité auprès de tous

Les différentes campagnes de sensibilisations, la charte IT, ainsi que l'engagement de confidentialité, permettent au groupe SINARI d'impliquer les collaborateurs dans la démarche de sécurité de l'information globale. Au-delà du périmètre contractuel, SINARI fait le choix également de diffuser les bonnes pratiques à l'ensemble de ses collaborateurs.

La charte informatique constitue un élément d'engagement et de responsabilisation des salariés. Ce document garantit que le collaborateur connait les règles générales à appliquer, afin de protéger l'accès aux données à travers le matériel qui lui est confié, mais aussi afin de garantir la préservation des dispositifs de sécurité en place et la valeur de la confidentialité de l'information

L'engagement de confidentialité, comme la charte informatique, est présenté lors de la signature du contrat de travail, en annexe. L'engagement de confidentialité peut être transmis sur demande aux clients lors des audits.

Par ailleurs, les collaborateurs sont régulièrement conviés à des ateliers (ou webinar) dans le but de les informer et de les sensibiliser aux nouveaux outils de sécurité, à l'évolution des exigences réglementaires et aux bonnes pratiques. Les collaborateurs sont également conviés à des ateliers de formation afin de les sensibiliser à la protection des données personnelles. La sensibilisation des collaborateurs de SINARI à la sécurisation des données personnelles est un enjeu primordial du fait des risques potentiels de violations de données au sein d'une entreprise.

La newsletter interne est également un support essentiel de la communication sur les aspects sécurité. Enfin, le plan de formation annuel permet de répondre aux besoins des collaborateurs en termes de compétences, et d'anticiper les évolutions de l'environnement.

4 Maintenir une architecture résiliente

Lors de l'appréciation des risques, une liste des actifs est dressée selon le périmètre technique certifié. Il est précisé pour chaque actif son propriétaire, et la politique applicable à son utilisation.

De plus, chaque donnée est soumise à une classification, qui a pour but de définir les conditions de manipulation, de criticité, selon les exigences légales. Pour les données contenues dans des supports amovibles, tels que les ordinateurs portables, une procédure est mise en place afin de déterminer précisément les conditions de mise à disposition, et de transfert.

Les politiques essentielles de sécurité sont :

- Patch management
- Endpoint Protection
- Sauvegardes
- Gestion des traces
- Gestion maintenance matériel
- Gestion du réseau
- Contrôles accès aux données
- Contrôles accès logiques
- Contrôles accès physiques
- Normes de développement
- Gestion des incidents

4.1 Politique de Patch Management

SINARI procède à la mise à jour complète des systèmes. Cela regroupe les mises à jour de sécurité et les mises à jour d'applications (correction de bugs). Les mises à jour sont effectuées de façon automatique au rythme suivant :

Type	Catégorie	Fréquence	Mode
Poste de travail	Lot 1	S1 et S3 11h	Auto
	Lot 2	S2 et S4 11h	Auto
Serveurs Windows	Lot 1	S1 mardi 6h	Auto
	Lot 2	S2 mardi 6h	Auto
	Lot 3	S3 mardi 12h	Auto
	Lot 4	S3 lundi 12h	Auto
Serveurs Linux	Tous les serveurs	Quotidien 7h	Auto
Autre OS	Equipements réseaux / sécurité	Bi annuel	Manuel
Applicatif	-	Bi annuel	Manuel

Les systèmes disposent ainsi de l'ensemble des correctifs relatifs aux applications.

Les mises à jour de sécurité nécessitent parfois les redémarrages des machines, des plages de maintenance doivent être prévues (au moins une fois par semaine).

Les mises à jour de sécurité critiques (score CVSS supérieur à 8) font l'objet d'une programmation spécifique :

Type	Catégorie	Fréquence	Mode
Poste de travail	Toutes	24h	Auto
Serveurs Windows	Toutes	24h	Auto
Autre OS	Equipements réseaux / sécurité	ASAP selon l'équipement et la programmation nécessaire (ecab)	Manuel
Applicatif	Exposé sur internet	24h	Manuel
	Non exposé sur internet	ASAP après test et validation	Manuel

Taux moyen de réussite des patchs pour SINARI
Quantité de patchs disponibles
Taux d'équipements compatibles avec la politique de MAJ

4.2 Politique antivirale

Dans le cadre de la lutte antivirale, SINARI met en œuvre les procédures suivantes :

4.2.1 Postes de travail des collaborateurs

L'ensemble des postes de travail des collaborateurs doit disposer d'un logiciel antivirus avec des mises à jour régulières. L'arrêt de la protection des Endpoint est restreinte par un mot de passe inconnu de l'utilisateur.

Les postes doivent procéder à une mise à jour quotidienne de la base de signatures antivirus et effectuer au moins une fois par semaine un scan complet de façon automatique.

En cas de détection d'un fichier malveillant, les actions suivantes sont réalisées de façon automatique, dans l'ordre :

- Tentative de réparation du fichier
- Tentative de mise en quarantaine du fichier
- Tentative de suppression du fichier

En cas d'échec des différentes actions automatiques, l'équipe sécurité prend en charge le nettoyage du poste.

Les postes de travail Windows étant fortement exposés, il est procédé de façon annuelle à un scan complet avec un outil tiers. Celui-ci est réalisé avec un outil en ligne ou sur le réseau local afin de garantir son intégrité vis-à-vis de la machine.

Le CTO définit les périodes où seront réalisés les tests complémentaires ainsi que la procédure.

Le résultat des tests complémentaires est consigné sur l'outil de GED.

4.2.2 Serveurs

Les différents outils doivent être configurés afin d'envoyer des alertes par mail au service sécurité.

Le bon fonctionnement de la mise à jour des analyses comportementales est surveillé en temps réel par l'outil de monitoring.

Une alerte visuelle est levée dans la console de monitoring si la date de la dernière mise à jour des bases comportementales est supérieure à 3 jours.

Taux d'agent EDR à jour

4.3 Politique de sauvegardes

SINARI applique en interne une sauvegarde de ses données sur son architecture de sauvegarde mutualisée, selon les modalités de notre politique de sauvegarde 'standard', précisées dans le tableau suivant :

Périmètre de sauvegarde	Type	Fréquence	Rétention	Fenêtre
Ensemble des composants du SI (système, configuration, données applicatives, traces de sécurité)	Incrémental	Quotidienne	Deux semaines	De minuit à 9 heures
	Complète	Hebdomadaire	Deux mois	Dimanche, début à minuit

Pilotés depuis un réseau d'administration dédié, les backups sont répliqués sur le data center distant (celui n'hébergeant pas les serveurs en question) via le réseau MAN 10Gb/s redondé en fibre noire reliant les Datacenters Nominaux et de secours. La réplication utilise un transfert disque à disque, le flux est protégé par un chiffrement SSL.

Un chiffrement des sauvegardes est réalisé par défaut via l'algorithme AES 256 bits au niveau disque. Le pilotage des tâches de sauvegarde est réalisé grâce à la solution Comvault.

Lors de l'installation des systèmes, des tests de sauvegarde et de restauration sont réalisés automatiquement afin de valider le processus complet. Des tests de restaurations réguliers sont ensuite effectués durant le cycle de vie du système de façon aléatoire de telle sorte que chaque client final soit testé une fois par an à minima et ce afin de garantir nos engagements contractuels vis-à-vis de ces derniers.

Les tests de restauration sont réalisés uniquement par des administrateurs de la solution de sauvegardes. En cas de découverte d'une anomalie, un plan d'action spécifique est mis en œuvre afin de la corriger. Un nouveau test est alors programmé pour valider le correctif. Le cycle est perpétué tant que le résultat du test n'est pas satisfaisant.

Taux de réussite des sauvegardes

Taux de réussite des tests de restauration

4.4 Gestion des traces

4.4.1 Généralités

L'ensemble des équipements SINARI ainsi que les équipements administrés par sa filiale SINARI transfère leurs traces techniques en temps réel sur des serveurs dédiés à cette tâche :

- Applications conformément aux contrats et demandes des clients
- Bases de données
- Certains composants logiciels standards (serveurs web, java, middleware, EAI, ETL...)
- Outil de gestion des sauvegardes
- Outils d'administration (notamment bastion d'administration et stockage)
- Réseaux (tout dispositif de filtrage et notamment pare-feu de cloisonnement)
- Systèmes (physiques et virtuels)

Sont également tracés par notre hébergeur, toutes intrusions physiques par le biais de caméras et de cahier de visites permettant la journalisation des passages.

4.4.2 Génération des traces

Les évènements de sécurité à tracer sont les suivants :

- Opération sur les habilitations
- La création/suppression/modification/désactivation d'un compte
- L'attribution/suppression/modification de droits
- Opération pouvant avoir un impact sur la sécurité du SI
- L'accès aux interfaces d'administration (ajout, modification, suppression)
- L'accès technique ou applicatif à des données de santé (lecture, ajout, modification, suppression)
- L'accès technique ou applicatif à des données personnelles (lecture, ajout, modification, suppression)
- Les modifications de configuration
- L'accès au système de gestion des évènements lui-même
- Accès client
    - Connexions à l'infrastructure d'hébergement
    - Une fois connecté, toute opération, en traçant les mêmes évènements de sécurité que pour le personnel interne
    - Accès physique (sur demande formalisée)

Les traces permettent une surveillance des opérations et d'investiguer dans le cas d'un incident de sécurité. Elles permettent d'identifier :

- L'action journalisée
- Tentative d'authentification (succès et échec)
- Connexion à un environnement/déconnexion
- Création/suppression/modification/activation/désactivation d'un compte
- Attribution/suppression/modification droits
- Action technique (ajout d'une règle pare-feu…)
- Motif de la visite, date, heures et intervenants pour un accès physique
- La source de l'action
- Identifiant de la personne
- Equipement (IP, hostname)
- La date et l'heure de l'action, provenant d'une source de temps unique
- Le statut de l'action
- Réussite/échec
- Alerte
- Erreur
- NA si impossible

Les traces applicatives sont générées conformément aux exigences spécifiées dans les contrats avec les clients.

Les traces applicatives ne peuvent contenir de données à caractère personnel, sans quoi les traces elles-mêmes seront soumises à une analyse d'impact afin de se conformer au RGPD. A cet effet, les traces sont générées de façon à être strictement dissociables des données de l'application.

S'il est spécifié dans le contrat avec un client que les traces applicatives sont collectées par SINARI, alors les traces sont générées dans un format communément admis de gestion des traces. Ainsi les traces seront compatibles avec le système de centralisation, et seront exploitables si nécessaire. Ces formats sont les suivants : Syslog, fichiers csv ou texte.

4.4.3 Collecte des traces

Les traces de sécurité générées sont centralisées de façon à garantir qu'elles ne peuvent être supprimées ou modifiées. Si des traces ne peuvent être centralisées, l'exception est validée par le CTO.

Les traces de sécurité doivent être centralisées de façon synchrone (temps réel) afin qu'une analyse puisse être réalisée. La mise en œuvre de cette centralisation est supervisée.

Les traces sont horodatées et la source de temps de tous les équipements générant des traces est unique. Le service de temps retenu est le service NTP fourni par SINARI ou un serveur global (Ex : pool.ntp.org).

Les traces sont conservées pour une durée de 1 an et uniquement 1 an sauf en cas de nécessité (procédure judiciaire). Au-delà de cette durée définie, les traces sont supprimées définitivement.

L'accès aux traces s'effectue à distance à travers une connexion sécurisée et une authentification nominative par identifiant / Mot de passe.

L'accès en lecture seule est possible à l'ensemble des collaborateurs du pôle technique dans le cadre de leur travail.

L'accès en écriture aux serveurs de centralisation des traces est restreint à la direction sécurité afin d'empêcher :

- La modification des types de messages
- La modification ou la suppression des fichiers de traces

De plus, une surveillance active est positionnée dans l'outil de supervision afin d'éviter une saturation de la partition qui bloquerait l'écriture des traces et donc la récolte de celles-ci.

Toutes les traces collectées sont sauvegardées de façon à garantir que celles-ci sont disponibles, même en cas de destruction du support physique.

Les sauvegardes qui garantissent la complétude, l'intégrité et la confidentialité des traces sont réalisées et sont externalisées.

Les traces récoltées font l'objet d'une analyse afin de détecter toutes défaillances ou tentatives d'intrusions. Cette analyse a pour objectif le déclenchement d'alerte en cas de comportement suspect.

Pour les traces d'accès physiques, celles-ci sont gérées par le fournisseur de Datacenter.

4.4.4 Hébergement de données à caractère personnel

Dans le cadre de l'hébergement de données à caractère personnel, en plus des dispositions habituelles, la solution Wallix Admin Bastion est systématiquement mise en œuvre. Cette solution permet une traçabilité complète des actions des administrateurs systèmes, qu'ils soient Linux ou Windows. Elle permet d'enregistrer les sessions d'administration et de les visionner ultérieurement en cas de besoin (audit, incident, forensics, ...). Elle permet également de garantir à la fois l'imputabilité des connexions et l'imputabilité des actions.

Dans l'architecture d'Hébergement groupe, cette solution de traçabilité est placée dans la DMZ d'administration réservée à SINARI.

Taux de déploiement du Syslog

4.5 Gestion du temps

Chaque serveur et chaque équipement réseaux ou sécurité doivent synchroniser leurs horloges sur une source de temps stable et redondée. Cette source doit se synchroniser elle-même sur au minimum 2 sources de strate 1 sur Internet.

Un potentiel décalage horaire sur les équipements doit être supervisé pour permettre une correction rapide.

4.6 Gestion de la maintenance du matériel

Lors de l'achat de nouveau matériel, une garantie initiale auprès du constructeur est systématiquement souscrite. Celle-ci est généralement de 3 ou 5 ans. Pour les équipements dits sensibles et si cela est possible, un support en 24/7 avec intervention en 4h est souscrit. Pour les autres équipements, le support reste en heures ouvrées et le remplacement est fait en J+1.

Le renouvellement du support à la fin de la période initiale est réalisé uniquement sur les équipements sensibles.

4.7 Sécurité des serveurs

4.7.1 Sécurisation des serveurs LINUX

La sécurité des serveurs Linux au sein de SINARI s'applique en deux temps :

- Application d'un script de post installation lors de l'installation automatique du serveur
- Application des classes Puppet.

Les points suivants sont mis en œuvre dans le cadre de leur sécurisation :

- Arrêt des services inutiles
- Suppression des packages systèmes inutiles
- Création de comptes locaux de secours
- Intégration de la machine dans l'authentification Azure Active Directory
- Configuration de l'externalisation des logs
- Configuration des sauvegardes
- Configuration du monitoring
- Configuration de l'agent Puppet permettant un maintien de conformité
- Configuration de l'inventaire automatique
- Configuration de la synchronisation temporelle
- Configuration de la politique de mise à jour
- Configuration de la politique de mot de passe
- Configuration des accès distants
- Mise en place de droits spécifiques sur l'arborescence.

Par la suite, des scripts de sécurisation standards sont mis en œuvre en fonction du rôle du serveur (serveur Web, serveur BDD, serveur applicatif).

4.7.2 Sécurisation des serveurs Windows

La sécurité des serveurs Windows au sein de SINARI s'applique en deux temps :

- Application d'un script de post installation lors de l'installation du serveur
- Application des stratégies de groupe lors de l'intégration au sein d'un domaine AD.

Les points suivants sont mis en œuvre dans le cadre de la sécurisation des serveurs Windows :

- Arrêt des services inutiles
- Suppression des packages systèmes inutiles
- Création de comptes locaux de secours et renommage du compte Administrateur
- Intégration de la machine dans l'authentification Active Directory
- Configuration de l'externalisation des logs
- Configuration des sauvegardes
- Configuration du monitoring
- Configuration de l'inventaire automatique
- Configuration de la synchronisation temporelle
- Configuration de la politique de mise à jour
- Configuration de la stratégie de mot de passe
- Configuration des accès distants
- Mise en place de droits spécifique sur l'arborescence.

Par la suite, des scripts de sécurisation standards sont mises en œuvre en fonction du rôle du serveur (serveur Web, serveur BDD, serveur applicatif).

Taux de serveurs intégrés dans l'AD

4.8 Les mesures du réseau

De nombreuses mesures afin de sécuriser les réseaux de l'entreprise sont mises en œuvre et répondent à l'annexe 27002 dans le document de déclaration d'applicabilité.

Les utilisateurs doivent avoir uniquement accès aux services pour lesquels ils ont spécifiquement reçu une autorisation. Dans ce cadre, différentes mesures sont en place au niveau réseau et applications.

Les services dédiés à l'administration des systèmes et l'exécution du métier de SINARI sont réservés à la population technique de l'entreprise.

Dans le cas où de tels services doivent être accessibles par une population non technique, des profils utilisateurs doivent être en place afin d'interdire toutes modifications des données.

4.8.1 Isolation réseau

L'isolation des plateformes de chacun des clients est obligatoire et il peut exister, pour une même plateforme, plusieurs types de sous-réseaux. Les différents sous réseaux sont tous isolés les uns des autres par des firewalls qui font soit partie de la production, soit du réseau d'administration SINARI. Cela assure une étanchéité et un contrôle minutieux des différents flux de données.

Les différents sous-réseaux sont les suivants :

- **ITC :** Le réseau ITC est de coloration jaune et représente le réseau d'administration, de supervision et de sauvegarde. Son accès est réservé aux administrateurs SINARI et sa configuration est en PVLAN
- **PROD :** Le réseau PROD est de coloration verte et représente le réseau de production pour les accès des utilisateurs. Son accès est réservé aux utilisateurs et sa configuration peut être en PVLAN ou en VLAN en fonction de la conception de la plateforme
- **BKE :** Le réseau BKE est de coloration bleue et représente le réseau d'interconnexion entre les serveurs d'une même plateforme. Son accès est restreint aux uniques serveurs connectés sur ce réseau, il ne contient pas de GW (sauf exception avec une isolation de niveau 3 entre différents réseau BKE) et sa configuration est en VLAN
- **STO :** Le réseau STO est de coloration rouge et représente le réseau dédié d'interconnexion entre les serveurs et l'équipement de stockage en réseau (ISCSI, NFS, CIFS). Son accès est restreint aux uniques serveurs connectés sur ce réseau, il ne contient pas de GW et sa configuration est en VLAN
- **DRAC :** Le réseau DRAC est de coloration blanche et représente le réseau d'accès aux consoles de managements des équipements (ILO, DRAC, MM etc.). Son accès est réservé aux administrateurs SINARI et sa configuration est en VLAN.

4.8.2 DDOS

SINARI a choisi une solution Anti-DDOS pour sa future application SaaS, Cette solution globale permet de surveiller et de sécuriser infrastructures et trafics.

L'ensemble des services fournis sur internet doivent bénéficier de la protection Anti-DDOS afin de garantir la disponibilité et la visibilité de nos infrastructures.

4.8.3 Protection des applications publiques

Les différentes applications publiques (sites web, portail client, évènementiel) doivent faire l'objet d'une attention particulière. En effet, celles-ci sont plus largement exposées aux risques externes. De fait, les différents services disponibles sur Internet doivent être protégés par un firewall applicatif (WAF) permettant de bloquer les attaques.

4.9 Accès à la donnée

4.9.1 Politique de filtrage firewall

Par défaut, l'ensemble des flux réseau est bloqué au niveau des différents firewalls. Pour faire transiter un nouveau flux, il est nécessaire d'en faire la demande au service sécurité qui effectue certains contrôles puis procède à l'ouverture en suivant scrupuleusement la procédure décrite dans le Wiki.

Dans le cadre d'une demande d'ouverture firewall concernant un flux sensible, l'équipe sécurité doit obtenir l'approbation du CTO avant de réaliser l'ouverture.

4.9.2 Règles de constitution des identifiants

Les identifiants de connexion sont normés de la forme :

- pnom (première lettre du prénom suivi du nom complet) pour les collaborateurs internes.
- pnom-adm pour les comptes administrateur du domaine.
- pnom-ext pour les prestataires externes à l'entité.

Exemple : Michel Nom - mnom

Deux cas particuliers sont à prendre en compte :

- Dans le cas de prénoms composés, les premières lettres de chacun des prénoms suivis du nom sont utilisées

  Exemple : Jean-Pierre Nom - jpnom

- Dans le cas de noms composés, il faut les concaténer en un seul nom.

  Exemple : Jean-Pierre du Nom - JPdunom

4.9.3 Règles de constitution de mot de passe

La constitution d'un mot de passe doit respecter les règles suivantes, à savoir il :

- Doit être composé d'une longueur supérieure ou égale à 14 caractères
- Doit avoir obligatoirement une durée de vie maximale de 180 jours
- Ne doit pas être composé d'aucun terme propre à l'utilisateur ou à l'entreprise
- Ne doit pas être enregistré en clair (au sein d'un fichier), ni pouvoir être déduit par une fonction quelconque ou d'une chaîne de caractères
- Doit être différent des 6 derniers mots de passe
- Doit être construit d'au moins une minuscule, une majuscule, un chiffre.
- Doit être unique et non partagé entre 2 comptes (exemple compte adm et compte classique).

Info : Un générateur de mots de passe est disponible ici.

4.9.4 Stratégie de verrouillage de compte

Afin de limiter les risques d'attaque par brute force, la stratégie de verrouillage de compte suivante est en place :

- Verrouillage du compte après 10 tentatives de connexions infructueuses,
- Déverrouillage du compte après 30 minutes.

L'authentification forte de SINARI

4.9.5 Authentification

AUTHENTIFICATION FORTE

L'authentification forte s'effectue à travers deux voies différentes, et est basée sur un certificat et un mot de passe. Les certificats électroniques sont uniques et personnels, ils attestent de l'identité de l'administrateur. Le mot de passe de l'administrateur est stocké sur l'annuaire de l'entreprise et est associé à son login personnel. Pour s'authentifier, il est indispensable d'être en possession du certificat et du mot de passe. Cette authentification forte correspond à une première authentification obligatoire pour l'ensemble des collaborateurs.

Les certificats sont attribués personnellement pour un membre de l'équipe Sécurité, lors de la procédure INOUT. Chaque demande de nouveau certificat doit être validée par un manager. Seuls les membres de l'équipe sécurité peuvent attribuer et révoquer un certificat.

AUTHENTIFICATION SIMPLE

L'authentification simple est gérée par un unique facteur :

- Par mot de passe : politique des mots de passe présentée au paragraphe précédent
- Par SSO : basée sur les principes de Kerberos, cette authentification permet aux administrateurs de se connecter aux architectures clients. Cette technologie permet d'éviter la transmission de mots de passe sur le réseau en privilégiant l'utilisation de jetons.

AUTHENTIFICATION DES COMPOSANTS

Les postes des utilisateurs SINARI sont authentifiés avec l'adresse MAC de leur ordinateur. Le service DHCP est configuré pour attribuer une adresse IP fixe spécifique en fonction de l'adresse MAC de l'ordinateur (Principe des baux DHCP).

Les authentifications mises en œuvre sont réparties de la façon suivante :

Composants	Type d'authentification	Architecture
Système d'exploitation	Identifiant / Mot de passe	Authentification centralisée
Bases de données	Identifiant / Mot de passe	Authentification locale
Applications	Identifiant / Mot de passe	Authentification locale ou centralisée
Composants réseaux	Identifiant / Mot de passe	Authentification centralisée
Composants de sécurité	Authentification forte	Authentification centralisée
Composants de sauvegarde	Identifiant / Mot de passe	Authentification centralisée
Composants de supervision	Identifiant / Mot de passe	Authentification centralisée
Composants d'exploitation ou d'administration	Identifiant / Mot de passe	Authentification centralisée
Accès distants	Authentification forte	Authentification centralisée

CONTRÔLE DE L'AUTHENTIFICATION

Un contrôle des authentifications Identifiant / Mot de passe est réalisé annuellement. Lors de ce contrôle, des tests de complexité de mot de passe sont réalisés sur quelques comptes aléatoirement.

4.9.6 Transmission des données

La transmission de données doit respecter la politique de classification des documents.

- Transmission de mots de passe : La transmission de mots de passe doit être faite via 2 canaux différents (téléphone, SMS, mail, Signal).
- Transmission de documents numériques : La transmission de documents numérique doit respecter les règles suivantes :
- Respecter les règles de classification de l'information
- Privilégier le partage Sharepoint (Le Wetransfer est à proscrire)
- Être réalisée dans un format non modifiable, il faut privilégier le format PDF plutôt que Word, Excel, etc ...
- Transmission électronique : Les courriels émis par la société doivent contenir la signature numérique qui est fournie au collaborateur. En cas de transmission de données sensibles via courriel, il peut être nécessaire de chiffrer celui-ci à l'aide du certificat, en accord avec la politique de classification des documents.

4.9.7 Expiration de compte

Un processus d'expiration des comptes est en place au niveau de l'annuaire centralisée Active Directory.

Tous comptes inactifs depuis plus de 30 jours sont automatiquement verrouillés. Cette mesure concerne aussi bien les comptes utilisateurs que les comptes de machines.

Taux de mots de passe avec expiration

4.9.8 Réutilisation de comptes

La réutilisation de comptes et identifiants désactivés ou expirés est strictement interdite.

4.9.9 BYOD

La pratique du BYOD (Bring Your Own Device) qui consiste à utiliser du matériel personnel pour se connecter au réseau de l'entreprise est strictement interdit. Seul le matériel fournit par l'entreprise est autorisé à se connecter au VPN.

Dans certains cas particuliers (prestataires / tiers mainteneurs), des équipements n'appartenant pas à l'entreprise peuvent nécessiter un accès au SI. Dans ce cas l'utilisation d'un bastion de rebond en coupure est obligatoire.

4.9.10 Principes sécurité bureautique

4.9.10.1 Pratique du bureau vide

La pratique du bureau vide est applicable sur l'ensemble des collaborateurs. Cette pratique consiste à ne laisser aucuns documents ou informations sur le bureau en dehors des heures de présence. Des caissons et armoires sont à disposition pour mettre sous clefs les documents papiers.

4.9.10.2 Impression

Il est recommandé d'utiliser l'impression sécurisé lors de l'impression sur des équipements non individuels (photocopieurs). L'opération consiste à définir un code au moment de lancer l'impression.

Ce code doit être saisi sur le copieur afin de lancer l'impression. Ce type de précaution permet de garantir que personne ne pourra récupérer le document à votre place lors de son impression.

Pour les autres cas d'impression, il est demandé de récupérer rapidement son document pour éviter toutes fuites d'informations.

Dans un souci environnemental et afin de limiter la reproduction d'information, il est préférable de limiter les impressions autant que faire se peut.

4.9.10.3 Sécurisation du BIOS

Sur l'ensemble des postes bureautiques, un mot de passe de protection BIOS est positionné afin de prévenir une modification de celui-ci. La protection concerne la modification du BIOS est non le démarrage du poste.

4.9.10.4 Gestion des clefs USB

Par défaut, l'utilisation de stockage de masse (USB) est interdite et verrouillée au niveau système sur les postes bureautiques. Pour les métiers justifiant l'utilisation de clefs USB, les mesures suivantes sont appliquées :

- Désactivation de l'autorun
- Utilisation des seules clefs de l'entreprise qui font l'objet d'un marquage d'identification.

4.9.10.5 Droits administrateurs

En dehors des cas particuliers que sont les comptes de la DSI et les administrateurs du domaine (compte –adm), les utilisateurs ne disposent pas des droits d'administration local de leurs postes.

4.10 Gestion de la sécurité logique

4.10.1 Gestion des privilèges

Toutes applications ou systèmes au sein de SINARI doivent disposer d'une gestion des privilèges. Pour les applications, les privilèges doivent définir au moins 2 profils. Un en lecture seule et un en lecture/écriture.

Les privilèges sont attribués sur demande du manager et après validation du CTO lors notamment du déroulement de la procédure IN/OUT.

Toujours dans le cadre de cette procédure, les privilèges sont supprimés ou désactivés lors du départ d'un collaborateur. Une désactivation automatique devra être programmée pour les contrats à durée déterminée (CDD, Stage, Prestataire).

4.10.2 Habilitation

4.10.2.1 Principes d'habilitation interne

Chaque utilisateur dispose d'un identifiant unique et personnel lui permettant d'accéder aux ressources de l'entreprise et aux ressources des clients de l'entreprise dans le cas de l'activité d'hébergement.

Les identifiants sont créés selon les règles exposées au paragraphe « Règles de constitutions des identifiants ».

L'utilisation de comptes génériques sur les systèmes, composants, journaux ou applications est strictement interdite. L'identification d'éventuels comptes génériques est réalisée par le biais de la surveillance active des systèmes et par le contrôle des habilitations et des profils présent sur les différentes applications.

Dans le cas d'applications (API par exemple) ou systèmes ne permettant pas l'utilisation de comptes personnels, l'utilisation d'une authentification moderne (Oauth 2.0) sera adressée ou à défaut l'utilisation d'une solution de bastion (Ex : Wallix) si supportée.

Les habilitations sont fournies à durée indéterminée tant que l'utilisateur ne change pas de rôle dans l'entreprise.

La révision des habilitations aura lieu lors de l'émission d'un changement au niveau de la fiche IN/OUT (changement de service, départ, absence).

L'attribution d'un utilisateur à un groupe est donc réalisée via la procédure IN/OUT sous contrôle du CTO (contrôles trimestriels aléatoires).

Par précaution, les utilisateurs ne peuvent accéder qu'aux applications dont ils ont besoin pour travailler, ni plus, ni moins.

En cas d'absence exceptionnelle de plus de 30 jours (maladie, vacances), les différents accès du collaborateur peuvent être suspendus jusqu'à son retour afin d'éviter tout acte d'usurpation d'identité sur son compte.

4.10.2.2 Principes d'attribution des groupes

D'une façon générale, il existe plusieurs profils d'utilisateurs. Les groupes utilisateurs correspondent à divers profils d'accès tant au niveau système qu'au niveau applicatif.

Les groupes sont créés selon la convention de nommage des groupes AD.

Au sein du groupe SINARI, cinq grands profils d'utilisateurs sont utilisés :

- N1-Public : Accès utilisateurs sans accès administrateur aux serveurs, il dispose néanmoins d'accès sur des applicatifs. Ce profil est attribué aux utilisateurs standards (Ex : Commerciaux / Administratifs / Développeurs / ...).
- N2-Interne : Accès administrateur aux systèmes clients autorisant l'intervention de sous-traitants ou des chefs de projets. Profil lié et attribué à la mission chez le client final. - N3-Restreint : Accès administrateur aux systèmes internes de la société. Profil attribué au cas par cas en fonction des besoins.
- N4-Complet : Accès administrateur aux systèmes internes sensibles de la société (Rôle administrateur global / gestionnaire de coffre-fort numérique / ...). Ce profil est attribué à un nombre très limité de collaborateurs de forte confiance.

On retrouve ensuite des profils d'habilitation liés aux compétences de l'individu et de sa fonction, par exemple :

- Accès sur les équipements réseaux et les équipements de sécurité (Firewall, IDS, etc.)
- Accès à la gestion du stockage
- Accès administrateur virtualisation (ESX, Vcenter)
- Accès aux équipements de sauvegarde Etc ...

La liste exhaustive des différents groupes de sécurité est maintenue par le CTO qui valide en concertation avec les managers l'affectation du personnel dans les différents groupes d'utilisateurs.

4.10.3 Réexamen des droits d'accès

Un réexamen semestriel est réalisé afin d'identifier tout écart dans les droits d'accès ou des accès qui ne sont plus pertinents. Le réexamen est réalisé par le CTO accompagné de la DSI groupe et sont étudiés lors d'un point sécurité dédié aux droits d'accès.

Le réexamen a lieu sur l'ensemble des applications et dans la gestion des identités SINARI (Active directory).

Sont étudiés :

- La liste des comptes actifs
- L'appartenance aux groupes
- Les profils associés aux groupes

A l'issu du réexamen, les actions correctives sont consignées dans le rapport d'audit et la correction des droits est réalisée dans les plus brefs délais. Si nécessaire, une vérification auprès du manager peut être effectuée.

Lors du réexamen des droits d'accès, il est contrôlé par la même occasion la présence de comptes illégitimes sur les différents équipements. Si des comptes illégaux sont découverts, leur désactivation est immédiate.

4.10.4 Stockage des mots de passe

L'ensemble des mots de passe doit être stocké dans un environnement sécurisé, à savoir :

- Gestionnaire de mot de passe pour l'usage personnel
- Un partage de dossiers dans un gestionnaire de mot de passe pour les besoins collaboratifs (Ex : Support / Chef de projets)

L'écriture d'un mot de passe au sein d'un script ou d'une application doit être faite dans un format non réversible (qui ne permet pas de le restituer).

Attention : Le stockage de mots de passe, sans exception, est strictement interdit sur les postes utilisateurs.

4.10.5 Transmission des identifiants et mots de passe

En interne, les identifiants et mots de passe sont transmis par le biais des coffres forts numériques (cf stockage des mots de passe).

La transmission des accès à un client doit être réalisée par le biais de 2 canaux différents, 3 possibilités existent :

- Transmission de l'identifiant par mail et du mot de passe par SMS (Idéalement par SIGNAL)
- Transmission de l'identifiant par mail et du mot de passe par téléphone
- Transmission de l'identifiant par mail et du mot de passe par appel Teams

4.10.6 Déconnexion automatique des sessions inactives

Les sessions utilisateurs sur les serveurs Microsoft et Linux sont déconnectées automatiquement après **2 heures** d'inactivité.

4.10.7 Verrouillage automatique des sessions utilisateurs

Les sessions graphiques sont configurées pour se verrouiller automatiquement après **15 minutes** d'inactivité.

4.10.8 Accès console

Les accès console sont réalisés à distance au travers des cartes de contrôle à distance (iDRAC, ILO, UCS, etc...). Cet accès console est systématiquement protégé par utilisateur / mot de passe. Dans la mesure du possible, l'accès utilise l'authentification nominative centralisée. Les mots de passe par défaut des constructeurs sont systématiquement modifiés.

4.10.9 Accès VPN

Au sein de la filiale SINARI, l'utilisation d'un accès VPN est obligatoire sur l'ensemble des postes quel que soit leur emplacement physique ou leur type (fixe et portable). L'accès VPN est nécessaire aussi bien depuis les locaux de SINARI qu'en situation de nomadisme, seule la typologie de VPN diffère à savoir IPSEC pour les locaux SINARI, SSL en mode nomade.

Cet accès est réalisé à l'aide d'une authentification forte multifacteurs MFA composée d'un couple identifiant / mot de passe et d'un complément pouvant être un SMS, un appel ou un authentificator.

Il existe 3 types de VPN donnant accès à des ressources différentes (segmentation au niveau réseau) :

- Accès Administratif permettant l'accès aux outils internes uniquement
- Accès Technique permettant l'accès aux outils internes et à l'ensemble des serveurs hébergés et infogérés pour les administrateurs
- Accès Prestataire permettant d'accéder à des ressources prédéfinies en fonction du besoin en garantissant un accès sécurisé point à point ouvrable à la demande ou permanent.

Taux d'écarts lors de la revue des droits

4.10.10 Accès en cas de maintenance

Les opérations de maintenance du SI sont enregistrées dans une main courante.

Le suivi des opérations de maintenance doit s'appliquer à tous les acteurs de cette maintenance, dans et en dehors des entités SINARI (employés et prestataires externes). Il implique l'ouverture d'un registre détaillé sur les interventions subies par les composants du SI.

Les interventions de prestataires tiers sont encadrées par le RSSI ou un employé désigné des entités SINARI.

Les entités SINARI concluent des contrats spécifiques avec tout prestataire de maintenance externe.

Ces contrats devraient prendre en compte les éléments suivants : (i) la responsabilité de l'entité SINARI et du prestataire externe, (ii) les moyens mis en œuvre sur les SI du prestataire pour s'interfacer avec le SI de l'entité SINARI, (iii) les possibilités et modalités de contrôle et d'audit de l'entité SINARI chez le prestataire, (iv) l'identification des personnes intervenant et manipulant les composants du SI de l'entité SINARI et (v) les privilèges accordés au prestataire pour la réalisation de ses missions.

4.11 Politique appareils mobiles

Une politique en matière d'appareils mobiles est mise en œuvre sur le périmètre SINARI par le biais d'un outil de MDM (Mobile Device Management).

L'accès aux ressources de l'entreprise (email, annuaire, agenda) est conditionné à la configuration des points suivants sur le périphérique mobile :

- Verrouillage automatique de l'écran **après 5 minutes**
- Présence d'un code de verrouillage de l'écran (minimum 4 chiffres)
- Présence d'un code PIN obligatoire sur la carte SIM (autre que 0000 et 1234)
- Politique de durcissement du code PIN
- Chiffrement du téléphone

Il est également demandé aux collaborateurs de ne pas laisser sans surveillance leur téléphone portable afin de limiter les vols et fuites de données.

4.12 Gestion de la sécurité physique

SINARI gère la sécurité physique de ses locaux au niveau du siège et des agences. L'accès physique aux datacenters est garanti par des fournisseurs de colocation spécialisés certifiés notamment ISO 27001. Une procédure d'accès physique est disponible pour chaque Datacenter.

- Datacenter de DIGITAL REALTY PAR5
- Datacenters de DIGITAL REALTY MRS7
- Siège social de Cesson-Sevigné

Les accès sont essentiellement contrôlés par code au siège de SINARI à Cesson-Sévigné, et par badge personnel et incessible aux datacenters (Sur demande formelle pour le personnel SINARI).

4.12.1 Datacenter

Les bâtiments type Datacenter doivent répondre à minima aux protections suivantes :

- Détection et extinction incendies automatisés
- Environnement climatique redondé
- Environnement électrique double alimenté et secouru (onduleurs et générateurs)
- L'accès à un serveur nécessite un contrôle d'accès à minimum 4 niveaux (exemple : parking, PC sécurité, zone technique, suite, baie)
- Murs renforcés
- Portes et issues de secours sous alarme
- Présence d'une équipe sécurité 24/7/365
- Présence de vidéo surveillance
- Procédure d'accès sur accréditations.

Les datacenters hébergeant les données du groupe SINARI seront à minima Tier IV pour le nominal et Tier III pour le secours.

Les datacenters hébergeant les données du groupe SINARI seront certifiés ISO 27001.

L'ensemble des datacenters sont situés en France.

4.12.2 Agences

Les bâtiments type bureaux, également nommé « Agences » doivent disposer à minima des protections suivantes :

- Alarme intrusion
- Contrôle d'accès par code aux bâtiments
- Contrôle d'accès par badge aux salles informatiques
- Détection incendie automatisée
- Existence d'une procédure d'accès visiteur
- Murs en dur

4.13 Exigences de sécurité pour les nouveaux équipements et nouveaux services

4.13.1 Exigences liés aux matériels

Lors de l'acquisition de matériel physique destiné à un environnement datacenter, il est nécessaire de respecter les exigences suivantes :

- Présence d'une double alimentation électrique (ou possibilité de mise en place d'ATS le cas échéant),
- Présence d'une carte de contrôle à distance type iDrac ou ILO pour les serveurs
- Présence d'une redondance matérielle au niveau du stockage de la donnée (raid)
- Présence à minima de 2 cartes réseaux pour la séparation des flux.

4.13.2 Exigences liés aux logiciels

Lors de l'acquisition de nouveaux logiciels ou lors de la modification de logiciels, il est important de tenir compte des exigences de sécurité en termes de Disponibilité, Intégrité, Confidentialité et Traçabilité.

Il est également demandé, qu'une analyse de conformité au RGPD de ces nouveaux logiciels soit réalisée afin d'éviter tout écart au processus d'accountability.

Ces phases d'identification et d'analyse sont faites lors de la phase projet, c'est à dire avant l'acquisition ou le changement.

CRITÈRES DE DISPONIBILITÉ

Le système hébergeant l'application doit être suffisamment dimensionné pour que l'application puisse fonctionner normalement en incluant une marge de manœuvre raisonnable afin d'éviter tout déclenchement d'alarme dans l'outil de supervision.

Dans le cas d'applications liées aux systèmes sensibles, celles-ci doivent permettre la mise en place d'une redondance.

Il est également important d'étudier la possibilité de souscrire à un support auprès de l'éditeur ou de l'infogéreur.

CRITÈRES D'INTÉGRITÉ

Les solutions doivent pouvoir gérer plusieurs paramètres :

- Les communications doivent pouvoir être chiffrées par SSL (ldaps, https, etc).
- L'application doit pouvoir gérer une historisation des accès.
- Dans le cas d'une application publique, un WAF (Web Application Firewall) doit être mis en place.

CRITÈRES DE CONFIDENTIALITÉ

Les solutions retenues doivent à minima permettre la mise en place des exigences suivantes :

- Gérer une authentification forte (MFA)
- Permettre une authentification sur le système de gestion d'identité (si possible SSO)
- Pouvoir gérer des profils utilisateurs avec restrictions de droits (profils admin et profils lecteur).
- Personnaliser les éléments de configuration par défaut, particulièrement les secrets d'authentification.

CRITÈRES DE TRAÇABILITÉ

La preuve au sein de l'application doit permettre à minima de :

- Historiser les authentifications (Date/Heures IP sources, login, Succès/Echec)
- Historiser les accès (log web par exemple)
- Exporter les logs (au travers du système si l'application ne le gère pas nativement)
- Non répudiation.

CRITÈRES D'ACCEPTATION D'EXPLOITATION

Les points additionnels suivants doivent être couverts pour qu'une application ou un nouveau service soit éligibles à la mise en production :

- Sauvegardes en place et fonctionnelles
- Supervision complète (système, applicatif, service final)
- Existence d'un Dossier d'Architecture Technique (DAT)
- Présence d'un support de formation (Physique ou Numérique)
- Contrôle qualité, validé
- PV de recette SSI validé

4.14 Norme de développement

4.14.1 Jeu d'essai

Sur la plateforme de test, aucune donnée de production n'est exploitée. Pour effectuer des développements ou faire des recettes d'applications, SINARI crée un jeu d'essai avec des données anonymisées sauf dans le cas où le client demanderait à utiliser ses propres données pour former ses collaborateurs. Ainsi les jeux d'essais ne contiennent jamais d'information de production identifiables sauf demande explicite du client pour des besoins de formation interne à l'entreprise.

4.14.2 Mesures cryptographiques

SINARI met en œuvre différentes mesures cryptographiques afin de protéger les données sensibles de l'entreprise.

Le besoin de chiffrement des documents est défini par les exigences du tableau de classification.

Les mesures cryptographiques sont également utilisées dans les cas suivants :

- Chiffrement AES-256 et hachage des postes nomades bureautique (Ex : Bitlocker)
- Chiffrement des communications mails au niveau contenu avec des certificats X509
- Chiffrement des communications SSL (OAUTH/HTTP/LDAPS TLS 1.2 minimum).
- Création de conteneurs sécurisés avec chiffrement AES-256.
- Chiffrement des smartphones (voir politique appareils mobiles et MDM).

Des moyens de recouvrement sont mis en œuvre avec le stockage des clefs au niveau du coffre-fort numérique.

4.14.3 Modification des logiciels

SINARI ne modifie pas les logiciels propriétaires. Si par nécessité, SINARI a besoin d'effectuer une modification, celle-ci est étudiée par le pôle développement et sécurité. Si elle est retenue, elle sera mise en œuvre en partenariat avec le fournisseur de façon à veiller au bon déroulement de cette modification sans altération du niveau des performances, de la sécurité et du contrat de service du fournisseur (notamment garanties).

Une phase de recette avec le fournisseur permettra la meilleure exécution.

4.15 Gestion des incidents de sécurité

4.15.1 Définition

Un incident SSI est un évènement, potentiel ou avéré, indésirable et/ou inattendu, impactant ou présentant une probabilité forte d'impacter la sécurité de l'information dans les critères de Disponibilité, de Confidentialité, d'Intégrité ou de Traçabilité.

Il correspond à une action malveillante délibérée ou d'une manière générale à toute atteinte aux informations, toute augmentation des menaces sur la sécurité des informations ou toute augmentation de la probabilité de compromission des opérations liées à l'activité.

4.15.2 Traitement et résolution

Tout incident de sécurité observé ou suspecté doit être signalé à l'équipe sécurité dans les plus brefs délais par les collaborateurs. Les prestataires sont également tenus à cette obligation. La suite à donner est définie à partir des critères d'évaluation d'impacts, qui permettent la détermination du niveau de l'incident : mineur, sévère, majeur, critique.

À la suite de cette qualification, des mesures d'urgence peuvent être prises pour limiter les impacts et préserver les traces, tels qu'un confinement, une isolation, une communication ciblée.

Une investigation est ensuite effectuée afin de préciser les caractéristiques de l'incident, et peut conduire au déclenchement d'une cellule de crise. L'incident est enfin résolu, soit par le biais d'une solution de contournement, soit par l'application d'un correctif.

Une revue mensuelle des incidents de sécurité est effectuée par l'équipe sécurité, afin de dégager et globaliser des plans d'action correctifs pérennes.

Temps moyen de résolution des incidents de sécurité

Quantité d'incidents SWAT

4.16 Gestion des audits sécurité

Des audits de sécurité récurrents sont réalisés sur le périmètre du SMSI SINARI. Ils permettent de contrôler la conformité entre les politiques validées par la direction et la réalité.

Les audits portent sur :

- Habilitations et accréditations des utilisateurs : Semestriellement
- Politique d'authentification : Semestriellement
- Sauvegardes : Quotidiennement (Reporting automatique)
- Sécurité périmétrique logique : Mensuellement

A cela s'ajoute des tests de redondances sur les équipements les plus critiques comme les core services (DNS / NTP / Mail) ou le service d'authentifications. Les tests de redondance sont réalisés à minima 1 fois par an.

Les potentiels écarts détectés font l'objet de corrections dans les plus brefs délais.

4.17 Mise au rebut de matériel

4.17.1 Serveurs

Effacement des données en 3 passes à l'aide d'un logiciel de Zeroing :

- Un premier écrasement par des bits à 1
- Un second écrasement par des bits à 0
- Une passe aléatoire

4.17.2 Equipements réseau et sécurité

Effacement des données en 2 étapes :

- Effacement de la mémoire flash
- Réinitialisation de l'équipement avec les paramètres d'usine

4.17.3 Equipements physiques

Pour les équipements physiques, 2 solutions possibles :

- Pour les disques durs physiques, utilisation d'un logiciel de Zeroing
- Pour les supports type CD/DVD, utilisation d'un broyeur

4.17.4 PV de destruction

Des PV de destruction sont émis lors de la mise au rebut d'un équipement, et plus particulièrement pour les équipements ayant contenus des données sensibles (Au titre du RGPD).

Les PV de destruction contiennent les informations suivantes :

- Identification du matériel (numéro de série, adresse mac, ...)
- Ancien propriétaire (entité, ou à défaut identité personne physique)
- Nouveau propriétaire (entité, identité personne physique)
- Date de transfert de l'équipement
- Date et nature de l'intervention d'effacement ou de destruction effectuée
- Statut des opérations réalisées (opérateur, date, type d'effacement, contrôle de l'effacement, ...)

5 Garantir notre continuité de service

Conformément aux exigences ISO 27002 et aux besoins internes, SINARI procède régulièrement à la revue et à l'audit technique de son infrastructure. Ces contrôles permettent de maîtriser au mieux la conformité avec ce qui a été défini et est connu de tous notamment dans le cadre du Plan de Continuité d'Activité (PCA).

Pour ce faire, SINARI a défini une organisation et des modes opératoires associés ayant pour but de garantir la survie de l'entreprise lors un sinistre important. Il s'agit ici de faire perdurer les activités essentielles (sans interruption des services vitaux) et de redémarrer les activités moins critiques le plus rapidement possible avec le minimum de perte de données.

5.1 Périmètre

Lors de l'appréciation des risques réalisée dans le cadre de la norme ISO 27002, il a été identifié trois types de risques nécessitant la mise en place du plan de continuité.

LA PERTE OU L'INDISPONIBILITE D'UN SITE PHYSIQUE

Ce risque regroupe l'ensemble des problèmes liés aux bâtiments. Le risque peut être temporaire (perte de sources d'énergie) ou définitif dans le cas d'une destruction du bâtiment. On distingue également 2 types de bâtiments : les datacenters d'une part et les bureaux d'autre part.

L'INDISPONIBILITE D'UN NOMBRE IMPORTANT DE SALARIES

Il s'agit de l'indisponibilité d'un nombre important de salariés ou dans l'incapacité de se rendre au travail. Cette indisponibilité pourrait avoir des origines diverses comme des grèves massives, une pandémie virale...

LA PERTE OU LA CORRUPTION D'UN SERVICE VITAL (CORE SERVICE)

Le bon fonctionnement des services de cœurs de réseaux étant vital, ils entrent dans le

afin que des mesures de redondance adéquates soient mises en place.

5.2 Indisponibilité d'un site physique

5.2.1 Indisponibilité temporaire

5.2.1.1 Sites de bureaux ou agences

L'indisponibilité temporaire indique que le site est toujours existant mais ne permet plus de travailler ou d'accueillir les collaborateurs. L'indisponibilité est relativement courte et ne dépasse généralement pas 24 heures. Ce cas peut se présenter lors de la perte des sources d'énergie, la perte des moyens de communications ou un besoin d'évacuation.

Cette indisponibilité n'a aucun impact sur les services proposés par SINARI, les collaborateurs étant équipés pour télétravailler sur l'ensemble du groupe.

5.2.1.2 Sites datacenter

Les sites de datacenters étant pleinement redondés ceux-ci ne subissent pas de coupures temporaires ou alors très courtes, la résolution est traitée comme un incident classique à la charge de l'hébergeur.

5.2.2 Indisponibilité permanente

5.2.2.1 Sites de bureaux

L'indisponibilité permanente d'un site hébergeant des bureaux est déclarée en cas de destruction du site. La destruction indique que le site sera indisponible pendant une longue durée.

Cette indisponibilité ne déclenche pas de PRA, elle impose cependant de trouver de nouveaux locaux afin de conserver un niveau acceptable dans le travail collaboratif des équipes.

5.2.2.2 Sites de datacenter

L'indisponibilité permanente d'un datacenter est la situation la plus critique possible pour SINARI. Ce cas peut se présenter en cas de catastrophe naturelle, d'attentats, incendie.

Cette indisponibilité déclenche immédiatement l'ensemble des PRA Clients pour ceux n'ayant pas souscrits à l'offre de PCA (PRA et Standalone). L'ordre de déclenchement des PRA clients est défini en fonction de 2 critères :

- Le RTO (Recovery Time Objective) qui correspond au temps maximum de coupure admissible selon l'engagement de service contractualisé avec le client
- Le volume financier du client

Concernant les clients ayant souscrit à l'offre Standalone, conformément aux contrats clients, une mise à disposition des données externalisées sera réalisée à partir des sauvegardes.

5.3 Indisponibilité humaine

L'indisponibilité massive d'employés lors d'épisodes viraux sévères (grippe saisonnière, grippe aviaire) représente un risque pour SINARI. Il peut être nécessaire de mettre en place des mesures de sauvegarde du personnel. Selon le niveau d'alerte virale et en accord avec les autorités sanitaires, les mesures suivantes peuvent être prises :

- Actions de communication interne spécifiques
- Mise à disposition d'un gel désinfectant et/ou masque de protection
- Remplacement des essuies mains en tissu par du papier jetable
- Confinement en télétravail

En cas de dépassement d'un taux d'absentéisme de **30%**, le confinement en télétravail est mis en place pour les utilisateurs vitaux.

5.4 La cellule de crise PCA

Si un des incidents couverts par le périmètre du PCA se présente, une cellule de crise est immédiatement mise en place.

5.4.1 Composition

La cellule de crise PCA est composée de :

- La direction générale
- La direction financière
- La direction technique
- Les directeurs de services opérationnels
- L'équipe DPO

5.4.2 Mission de la cellule de crise

La cellule de crise PCA est chargée des missions suivantes :

- Validation du déclenchement du PCA
- Prise de décision et ajustement sur l'orchestration des PRA
- Prise de décision sur les mesures et investissements immédiats
- Communication auprès des clients impactés

5.4.3 Principe de réunion

La cellule de crise se concerte en réunion à toutes les étapes clés du PCA (déclenchement / PRA vitaux / fin) et à minima 2 fois par jour.

Pour ce faire, la grande salle de réunion au RDC des locaux de Cesson-Sévigné est réquisitionnée d'office.

5.4.4 Test de constitution de la cellule de crise

Des tests de constitution de la cellule de crise sont réalisés une fois par an. Il s'agit d'un exercice assurant que l'ensemble des acteurs peuvent être joint rapidement.

Taux de tests PRA effectués

6 La gestion des tiers

Les solutions proposées par les entités SINARI impliquent de faire appel à des sous-traitants et les entités SINARI, en proposant leurs solutions à leurs clients, agissent en tant que sous-traitant.

Lorsque les entités SINARI font appel à des sous-traitants, les transferts de données à caractère personnel sont encadrés par la signature de contrats avec ces sous-traitants. Au sein de ces contrats, le traitement de données personnelles est encadré. Notamment, en cas de transferts des données personnelles en dehors de l'Union Européenne, des mécanismes de transfert sont mis en place afin d'assurer un niveau de protection des données suffisant et approprié.

Ces mécanismes de transferts sont :

- une décision d'adéquation de la Commission européenne concernant certains pays assurant un niveau de protection adéquat permettant de transférer des données personnelles vers ces pays sans mécanisme supplémentaire ;
- des clauses contractuelles types (CCT) de la Commission européenne signées avec le sous-traitant ;
- des règles internes d'entreprises (BCR)

Lorsque les entités SINARI agissent en tant que sous-traitant, celles-ci encadrent également les transferts de données personnelles par la signature de contrats avec leurs clients, agissant en tant que responsables de traitement.

Ces contrats visent à :

- encadrer les activités de traitement de données personnelles au titre du contrat
- lister les sous-traitants ultérieurs de l'entité SINARI (nom de l'entité, localisation, description du traitement, mécanismes de transferts mis en place en cas de transfert hors UE)
- décrire les mesures techniques et organisationnelles de sécurité mises en place par l'entité SINARI en tant que sous-traitant visant à garantir un niveau de sécurité approprié, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

De plus, les entités SINARI, en tant que responsables de traitement, peuvent auditer leurs sous-traitants et les entités SINARI, en tant que sous-traitant peuvent également être audités par leurs clients. Les conditions de mise en œuvre d'un tel audit sont encadrées par le contrat entre le sous-traitant et le responsable de traitement. Cet audit sera réalisé afin de vérifier que le sous-traitant respecte ses obligations au titre du contrat de traitement entre lui et le responsable de traitement.

7 Annexe 1 : Indicateurs SSI

Thème	Nom de l'indicateur	Référentiel	Formule de calcul	Fréquence	Objectif
Patch Management	Taux moyen de réussite des patchs	Outil Patch management Windows et linux	Nb patch OK / Nb patch lancé x 100	**Mensuelle**	**95%**
	Taux d'équipements compatible avec la politique de MAJ	Outil Patch management Windows et linux	Nb poste config OK / Nb poste Total x 100	**Mensuelle**	**100%**
Code Malveillant	Taux d'agent antivirus à jour	Logiciel antivirus	Nb agent à jour / Nb agent total x 100 MAJ inférieure à 3 jours entre la date de dernière connexion et la date de définition de virus	**Mensuelle**	**95%**
Sauvegardes	Taux de réussite des sauvegardes	Logiciel de sauvegarde	Nb job OK / Nb job Total x 100	**Mensuelle**	**95%**
	Taux de réussite des tests de restauration	Tableau de suivi des tests	Nb de restauration OK / Nb de restauration Total x 100	**Mensuelle**	**100%**
Gestion des traces	Taux de déploiement du Syslog	Serveurs Syslog	Nb test OK / Nb test Total x 100 Nb asset Syslog / Nb asset Total x 100	**Trimestrielle**	**95%**
Durcissement	Taux de serveurs intégrés dans l'AD	Inventaire	Nb poste dans l'AD / Nb poste Total x 100	**Trimestrielle**	**100%**
Anti-DDoS	Taux de services configurés en protection DDOS	Solution de protection anti DDOS	Nb service configuré / Nb service Total x 100	**Trimestrielle**	**100%**
Comptes logiques	Taux de mots de passe avec expiration	Active Directory	Nb compte avec expiration / Nb compte Total x 100	**Trimestrielle**	**100%**
	Taux d'écarts lors de la revue des droits	Tableau de suivi des revus des droits	Nb compte en erreur / Nb compte controlé x 100	**Trimestrielle**	**<2%**
Gestion des incidents	Temps moyen de résolution des incidents de sécurité	Outil de ticketing	Somme des temps de résolution / Nb d'incident fermé	**Mensuelle**	
PRA	Taux de tests PRA effectués	Tableau de suivi des PRA	Nb PRA testé / Nb PRA Total x 100 PRA testé = PRA testé au cours des 365 jours précédents	**Trimestrielle**	