Envoyé en préfecture le 12/12/2024
Reçu en préfecture le 12/12/2024
Publié le
ID : 069-256910183-20241206-CS_2024_12_3-DE

POLITIQUE DE SÉCURITÉ DU SYSTÈME D'INFORMATION DU SITIV

VERSION 2.0

Version 2022-04

Table des matières

I. Préambule

Le SITIV est un Syndicat Intercommunal qui a pour objectif la mise à disposition de ressources informatiques mutualisées et d'œuvrer à la modernisation numérique des communes membres.

La *politique de sécurité du système d'information mutualisée du SITIV* (PSSI-S) contribue à :

- Définir et expliquer la vision stratégique des Directions Générales des Services du SITIV et des Villes en matière de sécurité du SI ;
- Définir les objectifs de sécurité à atteindre, les acteurs associés ainsi que les moyens accordés ;
- Démontrer la volonté du SITIV d'impliquer les collectivités membres dans un front commun pour l'atteinte d'un niveau de sécurité cible.
-

La PSSI-S s'adresse à l'ensemble des services constituant le SITIV ainsi qu'aux services des villes membres pour leur usage du système d'information mutualisé, elle énonce des mesures organisationnelles, de mise en œuvre et techniques qui établissent des règles de sécurité souhaitées par la Direction Générale des Services.

La PSSI-S repose sur des référentiels de sécurité reconnus, notamment le Référentiel Général de Sécurité (RGS), le guide d'hygiène des bonnes pratiques de l'ANSSI, ainsi que la norme ISO 27001 – Annexe A (ISO 27002). En complément, cette politique intègre les directives du référentiel NIS2, visant à renforcer la résilience des systèmes d'information face aux menaces cyber et à assurer une conformité accrue aux exigences de sécurité au niveau européen. Ces bases fournissent un cadre robuste pour établir des pratiques de sécurité alignées sur les standards et les meilleures pratiques internationales.

2. Eléments stratégiques

2.1. Périmètre de la PSSI-S

La PSSI-S couvre l'ensemble du système d'information (SI) du catalogue des services du SITIV, y compris les plateformes applicatives et les plateformes d'hébergement qui lui sont associées.

Cette politique s'applique à toutes les personnes physiques et morales impliquées dans ce SI : les agents du SITIV, les représentants des villes membres, ainsi que les prestataires externes et sous-traitants, ainsi que leurs collaborateurs. Dans ce document, l'ensemble de ces éléments sera désigné par le terme « actifs ».

Le périmètre de la PSSI-S inclut, de manière non exhaustive, les sous-ensembles suivants :

- **Les actifs nécessaires à la gestion interne du syndicat** : systèmes de gestion financière, ressources humaines, marchés publics, institutions, etc.
- **Les actifs des services numériques mis à disposition des villes membres** : messagerie, applications métiers, sites internet, espaces de stockage, sauvegardes, dans le cadre du plan de service du système d'information.
- **Les plateformes d'hébergement et les réseaux d'interconnexion** : incluant les réseaux reliant les villes membres et le datacenter.
- **Les données gérées par les différents systèmes d'information**.

Les règles de sécurité définies dans cette PSSI-S forment un socle de bonnes pratiques communes, à appliquer par le SITIV et ses membres pour une protection cohérente et mutualisée des actifs numériques.

2.2. Date d'entrée en vigueur

La PSSI-S prend effet à compter de sa date d'approbation par le comité syndical.

2.3. Dispositions transitoires

La mise en application de la PSSI-S se déroule selon les principes suivants :

Plan d'action d'amélioration continue et de remédiation : Le SITIV et ses collectivités adhérentes mettent en œuvre un plan d'action triennal visant à atteindre les objectifs définis par la PSSI-S. Ce plan fait l'objet d'un suivi annuel, au minimum, par la gouvernance du SITIV.

Engagement des Villes membres : Les Villes membres participent activement au processus de mise en conformité de leur système d'information et appliquent les actions décidées par le groupe de travail SSI.

Plan de service SSI : Un plan de service SSI, annexé à la PSSI-S, définit le socle minimal et commun des règles de sécurité auquel chaque membre s'engage à adhérer, contribuant ainsi à la sécurité globale des systèmes d'information.

Commenté [sH1]: L'ecrire SV va ddm

2.4. Pilotage et évolutions de la PSSI-S

La PSSI-S, ainsi que son annexe *Plan de Service*, sont conçus pour évoluer dans le temps. Ils peuvent être révisés pour intégrer :

- Les nouvelles menaces identifiées et les retours d'expérience des traitements d'incidents ;
- Les résultats des analyses de risques ainsi que les actions issues d'audits ou de contrôles d'inspection ;
- Les évolutions des contextes organisationnel, juridique, réglementaire et technologique ;
- L'élévation progressive du niveau de sécurité cible.

Le suivi de ces évolutions est assuré par un comité de pilotage, coordonné par le SITIV et composé des membres suivants : le Directeur Général des Services, le RSSI mutualisé, les DSI des villes membres, les responsables de l'application de la PSSI-S chez les adhérents, ainsi que le service Hébergement et Sécurité du SITIV. Les principales missions de ce comité sont :

- Suivre la mise en œuvre de la PSSI-S ;
- Proposer des mises à jour de la PSSI-S ;
- Élaborer des documents complémentaires et des directives pour faciliter et clarifier l'application de la PSSI-S ;
- Suivre les mises à jour des documents techniques associés.

La PSSI-S mutualisée du SITIV est soumise à l'approbation du Comité Syndical du SITIV après validation par le comité de pilotage des Directeurs Généraux des Villes.

2.5. Enjeux et orientations stratégiques

D'une part, le SITIV entend mobiliser des ressources humaines, techniques et organisationnelles pour renforcer la sécurité de ses services et contribuer activement à la politique de sécurité de l'État en matière de cyberdéfense. Dans cette optique, les enjeux et orientations stratégiques globaux suivants sont définis :

- **Contribuer à la cybersécurité nationale** : Participer activement à la lutte contre les menaces cyber et les attaques visant les collectivités et les données des citoyens.
- **Mettre en œuvre le volet cyber du plan de relance** : Appliquer rapidement les mesures de cybersécurité prévues dans le cadre du plan France Relance.
-

D'autre part, en tant que politique mutualisée, la PSSI-S s'inscrit dans une stratégie locale visant à :

- **Sensibiliser les communes membres** : Impliquer les communes dans une démarche de prise de conscience des enjeux de sécurité du SI.
- **Élever le niveau global de sécurité** : Renforcer la sécurité du SITIV et de ses membres pour une résilience accrue face aux cybermenaces.
- **Renforcer la confiance des usagers** : Assurer aux usagers la fiabilité et la sécurité des services numériques proposés.
- **Protéger les données personnelles et les infrastructures** : Garantir la sécurité des données personnelles et la robustesse des infrastructures qui les hébergent.
- **Optimiser les ressources au service des membres** : Servir d'appui efficace pour l'exploitation des services mutualisés.

- **Soutenir le déploiement technique** : Accompagner les membres dans la mise en place des projets techniques.
- **Assurer la disponibilité et la sécurité de l'infrastructure** : Adapter et faire évoluer les services pour garantir une infrastructure mutualisée sécurisée et disponible.

2.6. Expression des objectifs de sécurité

Dans sa volonté de renforcer la sécurité de son système d'information et en accord avec son conseil syndical, le SITIV définit ses objectifs de sécurité conformément à la norme NIS2, entrée en vigueur en octobre 2024. Cette norme impose des exigences spécifiques en matière de cybersécurité pour garantir la résilience des infrastructures critiques. Les objectifs de sécurité sont établis en fonction des risques identifiés et sont complétés par les éléments suivants :

- **Une auto-évaluation de la sécurité du SI** : Conformément aux règles d'hygiène informatique de l'ANSSI et aux exigences de la norme NIS2.
- **Un socle de sécurité** : Basé sur les référentiels de l'ANSSI, la norme ISO 27001 – Annexe A et les exigences spécifiques de la norme NIS2.
- **Une Prospective Pluriannuelle d'Investissement (PPI)** : Élaborée par le SITIV et diffusée auprès des collectivités membres, pour planifier et prioriser les investissements en cybersécurité selon les nouveaux standards imposés par la norme NIS2.

Commenté [sH2]: Proposer ca

Le SITIV et les villes membres, décident pour leur PSSI-S mutualisée de se donner les objectifs de sécurité suivants :

Durcir l'authentification et protéger les données du matériel nomade	Appliquer les mises à jour sécurité sur le SIE	Sensibiliser et former les équipes à la sécurité (numérique & physique)	Définir une procédure de gestion des incidents de sécurité	Intégrer la sécurité dans projets applicatifs et SI
Garantir la sécurité dans la relation avec les fournisseurs	Identifier les actifs de l'organisation et définir les responsabilités pour une protection appropriée	Se protéger des logiciels malveillants, de la perte de données et organiser une journalisation efficiente	Limiter l'accès à l'information et aux moyens de traitement de l'information	Documenter une politique de Maintien en Conditions de Sécurité (MCS)
Améliorer la sécurisation des postes de travail	Maîtriser les risques de l'infogérance et sécuriser les accès à privilèges	Se conformer aux obligations légales et réglementaires	Etablir un inventaire technique du SIE et utiliser uniquement des équipements maîtrisés	Appliquer et suivre une politique de gestion des mots de passe sur les équipements et services

SIE : Système d'Information Essentiel

3. Principes & règles de sécurité

L'élaboration des principes et des règles de sécurité de la PSSI-S a pour objectif de répondre aux objectifs de sécurité définis dans la première partie. Ces principes ont été sélectionnés en se basant sur le référentiel de sécurité de l'ANSSI, la norme NIS2, et la norme ISO 27001.

Cette section de la PSSI-S est destinée à évoluer avec le temps et est structurée en trois grands domaines :

- **Principes organisationnels** : Définissent les structures et les processus nécessaires pour assurer la gestion de la sécurité au sein du système d'information.
- **Principes de mise en œuvre** : Portent sur les méthodes et les pratiques à adopter pour garantir la conformité aux principes de sécurité dans les activités quotidiennes.
- **Principes techniques** : Couvrent les aspects techniques relatifs à la protection des systèmes, des données et des infrastructures.

Chaque principe inclut une ou plusieurs règles d'application, visant à garantir leur mise en œuvre effective.

3.1. PRINCIPES ORGANISATIONNELS

ORGANISATION DE LA SECURITÉ

Politique de sécurité

Commenté [sH3]: A faire

EXEMPLE

Organisation de la sécurité de l'organisme

Le SITIV définit, met en œuvre et assure la mise à jour continue des procédures visant à garantir le maintien en conditions opérationnelles et de sécurité des ressources matérielles et logicielles de ses systèmes d'information réglementés.

Commenté [sH4]: SV

L'entité veille à la mise à jour des bases de connaissances concernant les outils de protection contre les logiciels malveillants. Cela inclut, entre autres, la mise à jour des bases antivirales de l'antivirus ainsi que des signatures utilisées par la solution d'EDR. La solution d'EDR est mise en place via Harfang Lab, avec une couverture assurée par un SOC externalisé fonctionnant 24h/24 et 7j/7 pour les serveurs dits "premium". Pour les serveurs qualifiés d'"essentiels", opérés par le SITIV, la surveillance est assurée pendant les jours ouvrés et durant les heures ouvrées.

Elle met également en place une veille continue sur les vulnérabilités, les correctifs de sécurité, ainsi que les mesures d'atténuation recommandées pour ses ressources de systèmes d'information réglementés (SIR). Ces informations proviennent notamment des fournisseurs, des fabricants des ressources, des prestataires mandatés ou encore des centres de veille et d'alerte en cybersécurité, tels que le CERT-FR ou les CSIRT.

Tous les serveurs doivent être enregistrés et suivis dans l'outil de gestion de vulnérabilités Cyberwatch, afin de garantir un suivi centralisé et un traitement rapide des alertes de vulnérabilités.

Le SITIV déploie sans délai les correctifs de sécurité nécessaires sur les ressources exposées à des réseaux externes (par exemple, serveurs Web, pare-feu exposés sur Internet, serveurs de messagerie) ainsi que sur les postes de travail des utilisateurs.

L'entité planifie et installe régulièrement les correctifs de sécurité sur l'ensemble de ses ressources.

Elle installe et maintient à jour les logiciels de ses SIR, y compris les logiciels embarqués, en veillant à ce qu'ils soient dans des versions supportées par leurs éditeurs ou fabricants et qu'ils intègrent les mises à jour de sécurité requises.

L'entité s'assure que toutes les nouvelles versions sont téléchargées à partir des ressources officielles mises à disposition par les éditeurs ou fournisseurs.

Lorsque des contraintes techniques ou opérationnelles empêchent l'installation d'une version supportée par le fournisseur, l'entité met en place des mesures pour limiter les risques liés à l'utilisation de versions obsolètes.

Enfin, elle garantit la mise en œuvre d'une procédure permettant de traiter ces alertes et, le cas échéant, d'appliquer les mesures de sécurité recommandées.

3.2. Sécurité et cycle de vie

3.2.1. Revue de configuration des ressources de ses SIR

L'entité réalise chaque année une revue de configuration des ressources de ses SIR afin de vérifier que les mesures de sécurité et de conformité définies ont bien été appliquées. La revue pourrait être organisée en plusieurs étapes, incluant une analyse des écarts, une validation des configurations, et une mise à jour des bonnes pratiques.

Il est recommandé d'utiliser des outils automatisés pour effectuer cette revue, afin de garantir une couverture complète et de réduire le risque d'erreurs humaines.

Lorsque des contraintes techniques ou opérationnelles empêchent la désactivation ou la désinstallation d'une ressource logicielle, l'entité prend des mesures compensatoires pour atténuer les risques associés. Ces mesures peuvent inclure, par exemple, la limitation de l'accès à cette ressource ou l'augmentation de la fréquence des contrôles de sécurité.

3.2.2. Contrôle d'application de la PSSI-S

La PSSI-S impose la mise en place de procédures et de mécanismes de contrôle interne afin de garantir une application efficace et conforme des mesures de sécurité. Le SITIV, en collaboration avec les collectivités membres, devra compléter ces actions par des audits externes pour s'assurer de la conformité et de l'efficacité des dispositifs en place. Le SITIV pourra également être sollicité par ses membres pour fournir un soutien, qu'il soit organisationnel ou opérationnel. Un rapport annuel sur la « sécurité » sera présenté lors du Comité Syndical afin de faire le point sur l'état de la sécurité et des actions mises en œuvre.

3.2.3. Protection des informations confiées à l'organisme

Le SITIV s'engage, conformément au Règlement Général sur la Protection des Données (Règlement UE n°2016/679 et loi n°78-17 du 6 janvier 1978, modifiée par la loi n°2018-493), à mettre en place les mesures techniques et organisationnelles nécessaires pour répondre aux exigences de ce règlement.

Chaque ville adhérente désigne un Délégué à la Protection des Données (DPD), et la liste des DPD est mise à jour annuellement. Un bilan RGPD, couvrant à la fois le SITIV et les villes membres, est annexé au compte rendu « sécurité » annuel.

3.2.4. Organiser la sécurité par la nomination d'un RSSI mutualisé

La nomination d'un responsable de la sécurité des systèmes d'information (RSSI) mutualisé est indispensable pour garantir la responsabilité globale de l'élaboration, de la mise en œuvre et du bon fonctionnement de la gestion de la SSI au sein du SITIV et de ses membres. Ce RSSI veille à l'application de la PSSI à tous les niveaux et dans tous les domaines de l'organisme.

3.2.5. Responsabiliser la gestion de la PSSI

Le SITIV met en place un comité de pilotage de la SSI, chargé de l'élaboration, de la mise en œuvre et de l'évolution de la PSSI. Ce comité se réunit au moins deux fois par an et est animé par le RSSI mutualisé.

3.2.6. Les responsabilités du Système de Management de la Sécurité de l'Information (SMSI)

Le **Système de Management de la Sécurité de l'Information (SMSI)** désigne le système mutualisé mis en place par le SITIV et les villes membres pour assurer la sécurité des données traitées. Conformément au principe général de sensibilisation de l'OCDE, les attributions et responsabilités des acteurs impliqués dans la sécurité du système d'information doivent être clairement définies.

Pour piloter la politique de sécurité des systèmes d'information et en faciliter la mise en œuvre, le SITIV, sous l'autorité de son directeur, s'appuie sur une chaîne fonctionnelle intersyndicale composée comme suit :

Le comité de pilotage des Directeurs Généraux des Villes, chargé de :

- Protéger le patrimoine informationnel des villes membres,
- Préparer les mesures de défense, de vigilance et de prévention en cas de crise,
- Gérer les situations d'urgence,
- Exécuter les plans de défense et de sécurité.

Le Directeur Général des Services du SITIV, chargé de :

- Traduire la PSSI mutualisée dans la Prospective Pluriannuelle d'Investissement,
- Garantir la cohérence de la mutualisation de la PSSI.

Le responsable de la sécurité des systèmes d'information (RSSI) mutualisé, nommé par le directeur général du SITIV, assure le lien avec les villes membres. Il contribue à l'élaboration et à la mise en œuvre d'une PSSI cohérente et en assure le suivi. Ses missions incluent :

- Suivre la mise en œuvre des dispositions SSI,
- Établir la PSSI mutualisée,

- Relayer les informations de sécurité provenant des centres d'alerte et de réaction aux attaques informatiques,
- Valider les projets en termes de sécurité,
- Remonter les dysfonctionnements à l'équipe de réaction aux incidents de sécurité,
- Rappeler les règles de sécurité à respecter (chartes informatiques et de sécurité des villes et du SITIV),
- Rédiger les documents relatifs à la SSI, tels que la PSSI-S et la charte informatique et de sécurité,
- Analyser les bilans et audits de sécurité et évaluer les besoins,
- Mettre en place des actions de prévention, de formation et de conseil pour les villes membres,

Les correspondants à la sécurité des systèmes d'information (CSSI), désignés par chaque ville adhérente, assistent le RSSI dans l'exercice de sa mission de SSI. La fonction de CSSI peut être partagée avec d'autres missions d'exploitation du SI et, dans le cadre d'un plan de service proximité, être assurée par le SITIV. Les missions du CSSI incluent :

- Promouvoir l'application de la PSSI,
- Veiller à la mise en place des mesures de sécurité nécessaires,
- Appliquer les instructions et recommandations en matière de sécurité,
- Sensibiliser les utilisateurs à la sécurité dans leur environnement SI,
- Mettre en place des opérations de prévention,
- Prendre les mesures appropriées en cas d'incident (ou s'assurer qu'elles soient prises),
- Appliquer les directives de la chaîne fonctionnelle SSI,
- Assurer la veille en matière de SSI.

Les responsables de traitement au sein du SITIV et des villes membres, conformément à l'article 24 du RGPD, sont responsables de la mise en œuvre des mesures techniques et organisationnelles permettant de garantir la conformité des traitements. Le SMSI assure ces garanties grâce à la politique validée par les responsables de traitement, au programme d'audit interne et aux mécanismes d'enregistrement des preuves.

L'organisation de ces responsabilités est simplifiée par fonction dans la matrice RACI ci-dessous :

	Comité Syndical du SITIV	Comité de pilotage des Directeurs Généraux	DGS du SITIV	RSSI Mutualisé	Comité de pilotage SSI	Responsable de traitement (RGPD)
Management de la SSI	A	A	A	R	C	I
Mise en œuvre	A	A	A	A/R	R	-
Contrôle interne et indicateurs	I	I	I	R	C	C

R – Responsable, A – Autorité approbatrice, C – Consulté, I – Informé

3.2.7. Assurer la sécurité dans les relations avec des tiers

Il est primordial pour le SITIV de maîtriser les accès, tant au système d'information qu'aux informations sensibles relatives à ce dernier et à sa sécurité. Lorsqu'il est nécessaire que des tiers accèdent à ces informations dans le cadre de la prestation de services, il est essentiel de s'assurer que les mêmes règles de sécurité s'appliquent à ces intervenants qu'aux personnels internes. Cela inclut la mise en place de documentation appropriée et d'accords contractuels, ainsi que la vérification de leur application par les parties concernées.

Voici la liste des organismes impliqués dans la gestion de la SSI du SITIV et des villes membres :

ORGANISMES	Type de relation	Consignes SSI	Contacts utiles
ATHEO	Prestataire Sécurité	A contacter sur le thème SSI	Yann BOBBA yann.bobba@cheops.fr 04 72 59 29 29
ADISTA (Vaulx-en-Velin)	Prestataire Opérateur de solutions télécoms	A contacter : pare-feu, DMZ, interconnexion VPN MPLS	Support One Adista supportone@adista.fr
LINKT	Prestataire opérateur de solutions télécoms	A contacter sur le sujet Interconnexion	Fabien ROGER fabien.roger@linkt.fr 07 70 24 64 74
ANSSI	Partenaire Sécurité	A contacter en cas de détection d'acte malveillant	Mathieu Delaplace mathieu.delaplace@ssi.gouv.fr 06 07 30 85 07
Jaguar	Prestataire Hébergement/Cloud	A contacter en cas d'indisponibilité	
CNIL	Autorité administrative	A notifier en cas de violation	116006 ou téléservice en ligne

Commenté [sH5]: check

Commenté [sH6]: Check

3.2.8. Cadre contractuel pour les échanges de données sécurisées

Afin de prévenir les risques liés à la perte, à la modification ou à la mauvaise utilisation des données lors des échanges avec les prestataires, les villes ou le SI de l'État, il est essentiel que les acteurs de la SSI (SITIV et villes membres) définissent clairement les responsabilités et obligations contractuelles des différents intervenants, tant pour les transmissions de données que pour les applications les intégrant.

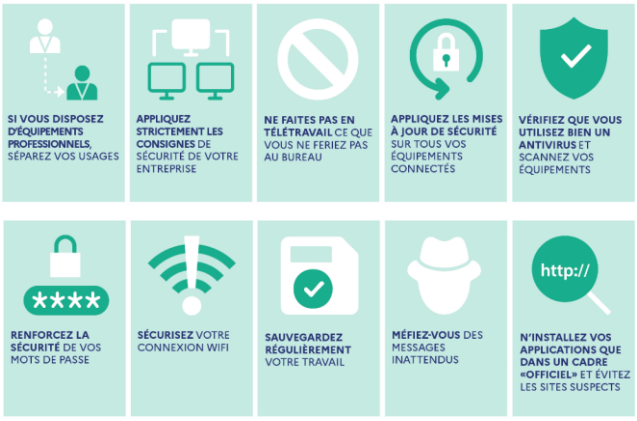
Une clause type sur la confidentialité et l'intégrité des flux peut être incluse dans les contrats avec des tiers :

« Tous les flux d'administration doivent être chiffrés à l'aide de procédés fiables (SSH, SSL, IPsec, etc.), garantissant ainsi la confidentialité et l'intégrité des données. De manière générale, tous les flux contenant des informations sensibles et circulant sur un réseau public doivent être chiffrés avec des méthodes assurant ces mêmes garanties. Le choix et le dimensionnement des algorithmes cryptographiques doivent être conformes aux règles et recommandations du RGS (Référentiel Général de Sécurité). Le prestataire devra préciser l'ensemble des mécanismes et mesures mis en place pour garantir la confidentialité et l'intégrité des flux d'administration. »

3.2.9. Télétravail

Le personnel du SITIV ou des villes membres travaillant depuis leur domicile évolue dans un environnement privé, sur lequel l'organisme concerné n'a aucun contrôle. Il est donc essentiel d'établir des règles techniques spécifiques concernant les droits d'accès. L'utilisateur doit être sensibilisé à la protection de son poste de travail et informé de ses responsabilités quant aux informations traitées dans ce contexte particulier.

Ce personnel doit utiliser uniquement l'ordinateur mis à disposition à cet effet et se connecter en VPN exclusivement avec les outils fournis et mis à jour (FortiEMS, double authentification, etc.). Il doit également respecter les règles définies dans la charte de la collectivité. À défaut, il devra suivre les bonnes pratiques en matière de travail à distance, telles que l'hygiène numérique, et utiliser les outils de sécurisation mis à disposition.



3.2.10. Les moyens cryptographiques

Il est essentiel d'élaborer et de mettre en œuvre une politique de mesures cryptographiques pour protéger l'information. Le SITIV et ses membres peuvent recourir à des techniques cryptographiques pour répondre à plusieurs objectifs de sécurité des informations qualifiées de sensibles, tels que :

- **La confidentialité** : via le chiffrement lors du stockage ou de la transmission des données.
- **L'intégrité et l'authenticité** : par l'utilisation de signatures électroniques.

- **La non-répudiation** : permettant de prouver qu'une action ou un événement a bien eu lieu.
- **L'authentification** : grâce à des techniques cryptographiques permettant de vérifier l'identité des utilisateurs et des systèmes sollicitant un accès.

Afin d'éviter une utilisation erratique ou inappropriée de ces outils cryptographiques, le choix des technologies sera mutualisé et appliqué de manière uniforme, optimisant ainsi les avantages du chiffrement et minimisant les risques associés.

Un inventaire des clés cryptographiques (SSH) et des certificats présents dans le périmètre du SITIV et des villes membres devra être créé et mis à jour régulièrement.

3.2.11. Organisation d'une cellule de crise mutualisée

La gestion de crise est une démarche structurée, impliquant des ressources humaines, techniques, juridiques et matérielles adaptées pour permettre au SITIV et à ses membres de se préparer aux risques et de gérer efficacement les impacts pouvant affecter leur fonctionnement. Pour une gestion optimale, il est essentiel de définir de manière précise les rôles et responsabilités des différents acteurs impliqués dans la crise, en scindant les tâches entre deux cellules complémentaires : **la cellule de direction de crise** et **la cellule opérationnelle de crise**.

3.2.11.1. Cellule de direction de crise (pilotage stratégique)

Cette cellule est constituée des décideurs principaux, responsables du pilotage global de la gestion de crise. Elle se réunit en permanence ou à intervalles réguliers pour prendre les décisions stratégiques, suivre l'évolution de la crise, et définir les grandes lignes de la réponse à apporter. Elle est chargée des aspects décisionnels et communicationnels de la crise.

Missions principales :

- **Déclaration officielle de la crise** : Dès qu'une situation est identifiée comme une crise, la cellule évalue la situation et procède à la déclaration officielle, en précisant la nature, l'étendue et l'urgence de la crise.
- **Prise de décisions stratégiques** : La cellule prend toutes les décisions nécessaires pour contenir et résoudre la crise, en fonction de l'évolution de la situation. Cela comprend la définition des priorités et l'allocation des ressources nécessaires.
- **Recours aux expertises internes et externes** : Selon les besoins, la cellule fait appel à des experts internes (RSSI, DSI, responsables juridiques) et externes (consultants spécialisés, autorités compétentes) pour analyser les enjeux techniques et sécuritaires de la crise.
- **Gestion de la communication** : La cellule définit les messages à transmettre aux parties prenantes (internes, externes, autorités, médias), coordonne les actions de communication et supervise le respect des protocoles de confidentialité.
- **Décision de fin de crise** : La cellule évalue la situation et, une fois les mesures correctives et préventives mises en place, prononce la fin de l'état de crise. Elle définit également les étapes post-crise pour rétablir un fonctionnement normal et effectuer un bilan détaillé.

Composition de la cellule :

- **Directeur Général des Services du SITIV**
- **Responsable Sécurité des Systèmes d'Information (RSSI)**
- **Responsable Juridique**
- **Responsable Communication**
- **Directeurs des collectivités membres concernés**
- **Experts externes (en fonction de la nature de la crise)**

3.2.11.2. Cellule opérationnelle de crise

La cellule opérationnelle de crise est responsable de la mise en œuvre des décisions prises par la cellule de direction. Elle est composée des acteurs impliqués dans la gestion quotidienne de la crise et se charge de la coordination des actions sur le terrain, de la mise en œuvre du Plan de Continuité d'Activité (PCA), et du suivi des processus de rétablissement.

Missions principales :

- **Activation de la cellule opérationnelle** : La cellule est activée immédiatement après la déclaration de la crise. Elle mobilise les ressources nécessaires, répartit les tâches et assure l'animation de l'équipe en charge de l'exécution.
- **Coordination des actions de crise** : La cellule coordonne toutes les actions nécessaires à la gestion de la crise, y compris l'activation du PCA et l'intervention des différents services internes (ex. : support technique, services de sécurité, maintenance). Elle ajuste les priorités en fonction de l'évolution de la situation.
- **Suivi de l'état de remise en service** : La cellule suit en temps réel la reprise des activités normales et assure une surveillance continue des systèmes et processus pour détecter les éventuelles failles.
- **Communication avec tous les acteurs** : La cellule informe régulièrement tous les intervenants (internes, externes, parties prenantes) sur l'état de la crise, les actions entreprises et les décisions prises. Elle gère les canaux de communication et s'assure de la diffusion correcte des informations.
- **Application des procédures de crise et fiches réflexes** : La cellule suit strictement les procédures d'urgence et les fiches réflexes établies pour chaque type de crise (pannes systèmes, cyberattaque, crise sanitaire, etc.). Elle s'assure que toutes les étapes sont respectées pour limiter l'impact et optimiser la réponse.

Composition de la cellule :

- **Chef de cellule opérationnelle** : Responsable de la coordination des actions
- **Responsable technique (DSI, RSSI)** : En charge de la gestion des systèmes d'information et de la sécurité
- **Responsable des ressources humaines** : Gestion des équipes et du bien-être des collaborateurs
- **Responsable logistique** : Coordination des moyens matériels et de la gestion des ressources physiques
- **Responsable communication** : Assure la communication interne et externe
- **Représentants des différents services (juridique, support, etc.)**

3.2.11.3. Procédures de collaboration entre les cellules :

- **Flux d'information clair et rapide** : Les deux cellules doivent établir des canaux de communication directs et rapides. Les informations transmises par la cellule opérationnelle doivent être synthétisées et transmises immédiatement à la cellule de direction pour prise de décision.
- **Réunions de coordination** : Des réunions régulières (quotidiennes, selon l'évolution de la crise) doivent être organisées pour permettre à la cellule de direction d'être informée en temps réel de la situation et pour ajuster les décisions prises.

- **Évaluations et ajustements continus** : La cellule opérationnelle doit régulièrement évaluer l'état de la crise et des mesures mises en place, et ajuster les actions en fonction de l'évolution de la situation. Ces retours sont transmis à la cellule de direction pour valider les stratégies à adopter.

Pour garantir une gestion de crise efficace, le SITIV et ses villes membres doivent mettre en place une série de mesures préparatoires essentielles :

- Fiche de contacts « Gestion de crise » : Il est impératif de préparer une fiche de contacts dédiée à la gestion de crise pour le SITIV ainsi qu'une fiche équivalente pour chaque ville adhérente. Ces fiches doivent comporter les informations actualisées de tous les acteurs clés de la cellule de crise, y compris les responsables, leurs suppléants, ainsi que les contacts externes (experts, prestataires, autorités locales). Ces fiches doivent être accessibles et régulièrement mises à jour pour garantir leur efficacité en cas d'urgence.
- Formation et préparation des personnes impliquées : Toutes les personnes qui auront un rôle à jouer en cas de crise doivent être formées et informées des procédures à suivre. Cela inclut le personnel de la cellule de direction de crise, la cellule opérationnelle, ainsi que tous les acteurs opérationnels et de soutien. Cette préparation doit inclure des formations régulières, des simulations de crise et des mises à jour sur les meilleures pratiques en matière de gestion de crise.
- Accessibilité en tout temps : Il est crucial que chaque membre de la cellule de crise soit joignable à tout moment, qu'il soit en période de travail ou en dehors des heures ouvrées. Des moyens de communication adaptés, comme des téléphones portables, des messageries sécurisées et des plateformes de communication de crise, doivent être mis en place pour garantir cette disponibilité.
- Désignation de suppléants : Afin d'assurer la continuité de la gestion de crise même en cas d'absence d'un membre de la cellule, il est nécessaire de désigner, en amont, au moins un suppléant pour chaque rôle clé. Ces suppléants doivent être formés aux mêmes tâches et procédures que les titulaires, afin d'assurer une transition fluide et une gestion de crise sans interruption.
- Réalisation d'exercices de crise : Des exercices réguliers doivent être organisés pour tester les réactions de la cellule de crise et vérifier l'efficacité des procédures en place. Ces exercices permettent non seulement de renforcer la préparation des équipes, mais aussi d'identifier d'éventuelles faiblesses dans l'organisation, la communication et l'exécution des actions de crise. Des simulations réalistes, incluant des scénarios de crises variées, sont essentielles pour s'assurer que tous les membres de la cellule aient les bons réflexes et soient capables de réagir de manière appropriée et coordonnée en situation réelle.

Commenté [sH7]: SV

3.3. Gestion des risques SSI

Dans le cadre de la mise en conformité avec la Directive NIS2, le SITIV ainsi que ses villes membres, s'engagent à réaliser et maintenir une analyse régulière de la conformité des Systèmes d'Information Réglementés (SIR) vis-à-vis des exigences de cette directive. Cette analyse constitue un processus clé pour garantir que les mesures de sécurité et de gestion des risques mises en place répondent aux exigences légales et aux objectifs de sécurité définis par la NIS2. En complément, un processus d'audit continu est mis en place pour évaluer régulièrement l'alignement des systèmes d'information avec les exigences NIS2, assurant ainsi une amélioration continue de la sécurité et de la conformité.

L'analyse de conformité a pour objectif de vérifier si les pratiques de sécurité de l'entité, ainsi que les infrastructures et services associés, respectent pleinement les obligations prévues par la directive

NIS2. Elle permet ainsi de mesurer l'alignement des processus internes avec les critères de sécurité, de gestion des risques, de gouvernance, et de protection des infrastructures critiques. Pour chaque Système d'Information Réglementé (SIR), l'entité doit procéder à une analyse de conformité qui identifie les éventuels écarts entre les mesures mises en œuvre et les exigences légales de la NIS2. Ces écarts peuvent concerner des domaines variés tels que la gestion des risques, la prévention des incidents de cybersécurité, la continuité d'activité, la gouvernance de la sécurité, ou encore les aspects de notification et de transparence des incidents de sécurité.

- Les étapes de l'analyse de conformité :

- Identification des exigences spécifiques de la NIS2 : Une première étape consiste à bien cerner les exigences réglementaires précises de la directive NIS2, notamment celles relatives à la gestion des risques de cybersécurité, la protection des infrastructures critiques et la capacité de résilience des systèmes d'information. Ces exigences couvrent un large éventail de domaines, y compris la protection contre les menaces, la gestion des incidents, la continuité des services et l'échange d'informations avec les autorités compétentes.

- Cartographie et évaluation des SIR : Chaque système d'information réglementé doit être cartographié pour identifier les différents composants techniques et les processus associés. Une évaluation approfondie est réalisée pour s'assurer que chaque élément du système respecte les exigences de sécurité, tant au niveau des technologies employées que des processus de gestion associés.

- Identification des écarts : L'analyse compare les pratiques actuelles de l'entité avec les exigences de la NIS2. Cette comparaison permet d'identifier les écarts entre les mesures de sécurité existantes et celles requises par la réglementation. Les écarts peuvent être relatifs à des domaines comme l'authentification des utilisateurs, le chiffrement des données, la mise en place de mécanismes de détection des incidents de cybersécurité, ou encore la gestion des vulnérabilités.

- Plan d'action correctif : Une fois les écarts identifiés, un plan d'action est établi pour corriger ces anomalies et renforcer la conformité avec la directive NIS2. Ce plan précise les actions concrètes à mener, les responsables de leur mise en œuvre, ainsi que les délais de réalisation. Il peut inclure des mesures techniques (mises à jour de logiciels, renforcement des protocoles de sécurité, etc.) ainsi que des mesures organisationnelles (formation des équipes, révision des processus de gestion des incidents, etc.).

- Suivi et mise à jour régulière : L'analyse de conformité n'est pas un processus ponctuel, mais doit être réalisée de manière continue pour s'assurer que le SIR reste conforme aux exigences de la NIS2 au fur et à mesure de l'évolution des systèmes, des menaces et des réglementations. Des revues périodiques sont nécessaires pour évaluer l'état de conformité et apporter les ajustements nécessaires à la stratégie de cybersécurité en place.

3.3.1. Maîtriser et contrôler les flux spécifiques

Afin de garantir une sécurité optimale des systèmes d'information, le SITIV et ses villes membres recommandent fortement la mise en place d'un serveur proxy dédié à la gestion et au filtrage des flux sortants.

Ce serveur proxy joue un rôle crucial en améliorant l'accès au web tout en protégeant les utilisateurs contre les risques liés à l'accès à des sites web dangereux ou malveillants. En filtrant les sites et les contenus accessibles, il permet de sécuriser les échanges tout en optimisant la performance de l'accès internet.

Dans le cadre de l'utilisation du pare-feu mutualisé, il est important que ce dernier soit configuré pour effectuer un filtrage complet des flux sortants. Cela inclut le contrôle applicatif, l'antivirus, l'anti-spam, ainsi que le filtrage web.

L'objectif est de s'assurer que tout trafic sortant soit conforme aux règles de sécurité définies et qu'aucune donnée sensible ou malveillante ne soit envoyée à l'extérieur du réseau. Le suivi et la gestion de ces flux doivent être organisés de manière rigoureuse afin de garantir la conformité et la sécurité des échanges.

3.3.1.1. Gestion du Pare-feu Mutualisé :

La gestion de ce pare-feu et des règles associées doit suivre un cadre strict et des procédures clairement définies, comprenant les points suivants :

- **Accès par des comptes nominatifs** :
  Chaque entité (SITIV et villes membres) devra se voir attribuer un compte nominatif d'accès au système de gestion du pare-feu. Cette approche permet de garantir une traçabilité des actions et de maintenir un contrôle sur les personnes ayant la capacité de modifier les règles de filtrage.

- **Création de tickets GLPI pour toute modification** :
  Toute modification apportée aux règles de filtrage (que ce soit pour le filtrage des flux, la redirection de ports ou autres ajustements) devra être formalisée par la création d'un ticket dans l'outil de gestion GLPI. Cela permettra au SITIV de suivre précisément les modifications effectuées, d'assurer une bonne gestion des changements et de conserver un historique des actions réalisées. Cette procédure garantit également que toutes les modifications sont validées et suivies correctement.

- **Sensibilisation et formation sur la gestion des règles de filtrage** :
  Des actions de sensibilisation et de formation doivent être proposées aux responsables des entités sur la gestion des règles du pare-feu. L'objectif est de garantir que les personnes en charge de la configuration et de l'administration du pare-feu comprennent bien les principes de base de sécurité et de filtrage. La formation permettra également de réduire les risques liés à des erreurs humaines dans la gestion des règles de sécurité.

- **Journalisation des accès** :
  Tous les accès et toutes les modifications doivent être soigneusement journalisés. Les logs doivent être consultables et analysables afin de détecter toute activité suspecte ou toute tentative d'accès non autorisé. Une gestion centralisée et sécurisée des journaux est

essentielle pour garantir la traçabilité des actions et faciliter les investigations en cas d'incident.

Le détail complet de la gestion du pare-feu mutualisé, comprenant une matrice des responsabilités, des règles d'utilisation précises et des informations techniques nécessaires à la configuration, est disponible en annexe. Cette documentation assure une meilleure compréhension des responsabilités et des processus à suivre pour maintenir un haut niveau de sécurité du réseau.

3.3.1.2. Flux de messagerie

Les échanges de courriels avec l'extérieur constituent un vecteur essentiel pour la communication professionnelle. Cependant, ils comportent également des risques, notamment en matière de sécurité des données et de conformité aux réglementations telles que le RGPD. Pour garantir la sécurité et la conformité des échanges par messagerie électronique, il est crucial de mettre en place des règles strictes encadrant la taille des messages, la gestion des pièces jointes, le contrôle anti-virus et la protection contre les codes malicieux.

Le RGPD permet la conservation des données de messagerie personnelle, sous condition que celles-ci soient traitées à des fins d'archivage. L'une des meilleures pratiques pour protéger les données contenues dans les e-mails est d'utiliser le chiffrement des messages et de stocker les e-mails dans un environnement sécurisé. Le SITIV et les villes membres doivent donc appliquer un ensemble de règles de sécurité pour garantir la protection des informations sensibles échangées par mail.

3.3.1.2.1. Règles de sécurité appliquées au SITIV et aux villes membres :

- **Identification des messages personnels** :
  Les utilisateurs doivent clairement identifier les messages personnels en les signalant dans l'objet de l'e-mail par la mention « PERSONNEL » ou « PRIVÉ ». Cette pratique permettra de différencier les messages professionnels des messages personnels et d'appliquer des règles de conservation et de gestion distinctes.
- **Durée de conservation des e-mails** :
  La durée maximale de conservation des messages électroniques est fixée à 5 ans avant archivage. Au-delà de cette période, les messages doivent être déplacés dans un dossier d'archivage. Cette règle garantit la conformité avec les exigences légales et permet de gérer efficacement les informations tout en limitant les risques liés à une conservation excessive des données.
- **Limitation de la taille des messages** :
  Pour garantir une gestion optimale de l'infrastructure de messagerie, la taille maximale des messages (texte + pièces jointes) est limitée à 10 Mo. Cette restriction vise à réduire les risques d'encombrement du système de messagerie et à améliorer la performance du réseau. Pour l'envoi de fichiers volumineux excédant cette limite, il est recommandé d'utiliser des solutions alternatives, telles que des outils de transfert de fichiers sécurisés.
- **Limitation de la taille des boîtes aux lettres** :
  La taille totale d'une boîte aux lettres est limitée à 4 Go, sauf pour les utilisateurs bénéficiant de privilèges particuliers. Cette mesure permet d'assurer un usage optimal des ressources du système de messagerie tout en garantissant que les données ne soient pas stockées de manière excessive sur les serveurs.

Commenté [sH8]: A valider avec anasse

Commenté [sH9]: A valider avec anasse

3.3.1.2.2. Dispositifs de sécurité et gestion des pièces jointes :

- **Contrôles antivirus et de sécurité** :
  Tous les messages et pièces jointes entrants et sortants seront soumis à un contrôle antivirus et un filtrage contre les codes malicieux. Ce dispositif garantit que les menaces potentielles, telles que les virus et les logiciels malveillants, soient détectées et neutralisées avant qu'elles n'atteignent les utilisateurs.

- **Chiffrement des e-mails** :
  Le chiffrement des messages est essentiel pour protéger la confidentialité des données transmises par messagerie électronique. Tous les messages contenant des informations sensibles doivent être systématiquement chiffrés avant envoi. Cette pratique assure que seuls les destinataires autorisés peuvent accéder au contenu des messages.

- **Archivage des e-mails dans un environnement sécurisé** :
  Les e-mails doivent être archivés dans un environnement sécurisé qui garantit la protection des données, notamment en termes de confidentialité, d'intégrité et de disponibilité. Des solutions d'archivage adaptées et sécurisées seront mises en place pour répondre à ces exigences.

Commenté [sH10]: Valider avec anasse

3.3.1.3. Mise à disposition des règles de gestion des e-mails :

Un ensemble de règles et de procédures détaillées sera mis à disposition des utilisateurs pour améliorer la gestion des e-mails professionnels, en particulier concernant l'envoi de pièces jointes volumineuses et la sécurité des messages. Ces règles permettront de garantir un niveau de sécurité optimal pour l'architecture de messagerie et d'assurer la conformité avec les exigences réglementaires.

3.3.2. Identification des services et moyens justifiant l'utilisation de la cryptographie

Application/Service	Type d'information	Cadre réglementaire	Moyen cryptographique possible*
Communications avec les services de l'État TDT S2LOW	Actes administratifs, financiers	RGS	Certificat RGS
Application eParapheur	Documents officiels	RGS	Certificat RGS Certificat SSL (en fonction de l'enjeu)

Application métier publiée sans DP	Bases de données	RGS	HTTPS, certificat serveur
Application métier publiée avec DP	Bases de données	RGS, RGPD	HTTPS, certificat serveur
Service d'authentification LemonLDAPNG	Identité numérique agent	RGS, agentConnect territoires	HTTPS, TOTP, France Connect

** Certificats RGS, signatures électroniques, LemonLDAP, certificats serveurs. Possibilités multiples de chiffrement en application des moyens « ouverts » du RGS.*

Commenté [sH11]: Valider avec anasse

3.4. Sécurité et cycle de vie

3.4.1. Intégration de la SSI dans les projets

L'intégration de la sécurité des systèmes d'information (SSI) dès les premières étapes des projets est cruciale pour garantir la protection des données, des infrastructures et des processus au sein du SITIV et des villes membres. La PSSI-S (Politique de Sécurité des Systèmes d'Information - Sécurisation) prévoit une organisation qui veille à ce que les aspects liés à la sécurité soient pris en compte tout au long du cycle de vie des projets. Bien que chaque projet puisse être autonome dans son organisation, il est impératif que ces projets soient en lien étroit avec les responsables de la SSI globale, qu'ils soient issus du SITIV ou des collectivités concernées. Cette démarche permet de garantir que tous les enjeux de sécurité sont correctement identifiés, évalués et gérés.

3.4.2. Organisation et responsabilités

L'intégration de la SSI dans les projets repose sur une collaboration efficace entre les équipes projets et le service Hébergement et Proximité, qui est le garant de la SSI. Ce service doit être sollicité dès la phase de conception des projets et accompagner les équipes tout au long de leur mise en œuvre pour s'assurer que les principes de sécurité sont bien intégrés. De cette manière, la SSI devient un élément fondamental de la planification, de la gestion des risques et de l'exécution des projets.
Les projets concernés par cette démarche d'intégration de la SSI sont multiples et couvrent un large éventail de domaines. Voici quelques-uns des projets dans lesquels le service Hébergement et Proximité doit intervenir ou être sollicité pour garantir un niveau de sécurité optimal :

3.4.2.1. Projets SI - Applications métiers

Les projets liés aux systèmes d'information (SI) et aux applications métiers sont parmi les plus stratégiques pour le SITIV et ses villes membres. L'intégration de la SSI dans ces projets permet de garantir que les données sensibles et critiques des applications sont protégées tout au long de leur cycle de vie. Le service Hébergement et Proximité doit être impliqué dès la phase de spécification des besoins, notamment pour :

- L'analyse des risques associés aux nouvelles applications.
- La mise en place de mesures de protection adaptées (cryptage, contrôle d'accès, surveillance, etc.).
- L'intégration de solutions de gestion des vulnérabilités.

- La formation des utilisateurs sur les bonnes pratiques de sécurité liées à l'utilisation des applications.

3.4.2.2. Flux d'échanges internes/externes

Les projets qui impliquent des flux d'échanges de données, que ce soit à l'intérieur ou à l'extérieur de l'organisation, doivent également prendre en compte les aspects de sécurité. Les échanges de données entre systèmes, entités ou avec des partenaires externes exposent l'organisation à des risques importants en matière de confidentialité, d'intégrité et de disponibilité des informations. Le service Hébergement et Proximité doit intervenir pour garantir la sécurité de ces flux en :

- Définissant les normes de sécurité pour les échanges de données, y compris le chiffrement, la signature électronique, et l'authentification des parties prenantes.
- Mettant en place des mécanismes de contrôle des flux entrants et sortants, comme des proxy, des pare-feu ou des outils de détection d'intrusions.
- Assurant la conformité avec la réglementation (RGPD, NIS2) concernant les échanges transfrontaliers de données.
- Effectuant des audits réguliers pour vérifier que les mécanismes de sécurité des flux sont correctement appliqués.

3.4.2.3. Processus d'intégration de la SSI

L'intégration de la SSI dans les projets ne doit pas se limiter à une simple vérification des mesures de sécurité en fin de projet. Elle doit être un processus continu et itératif, qui commence dès la phase de conception et se poursuit tout au long de la durée de vie du projet. Le service Hébergement et Proximité doit intervenir à chaque étape clé du cycle de vie du projet, selon le processus suivant :

- **Phase de conception** : Évaluation des risques liés à la sécurité, identification des exigences de sécurité pour le projet, définition des bonnes pratiques et des contrôles à mettre en place.
- **Phase de mise en œuvre** : Vérification de l'intégration des exigences de sécurité dans les systèmes, les outils et les processus. Tests de vulnérabilité et validation des dispositifs de sécurité.
- **Phase de déploiement** : Validation de la mise en production des systèmes sécurisés, formation des utilisateurs, mise en place de mécanismes de surveillance.
- **Phase de maintenance** : Surveillance continue, gestion des incidents de sécurité, mise à jour régulière des systèmes et des outils pour répondre aux nouvelles menaces.

3.4.3. Contrôle permanent des moyens de protection

L'intégrité et la disponibilité des équipements de sécurité tels que les pare-feu, les proxies, les antivirus et les systèmes de mise à jour sont des conditions fondamentales pour assurer l'efficacité de la sécurité des systèmes d'information (SI) au sein du SITIV et des villes membres. En effet, ces équipements jouent un rôle crucial dans la protection contre les cybermenaces, l'analyse des flux, ainsi que la gestion des vulnérabilités. Pour garantir leur bon fonctionnement et minimiser les risques de défaillance, il est essentiel de mettre en œuvre des mesures de supervision appropriées.

La supervision des équipements de sécurité est un pilier majeur de la gestion de la sécurité des systèmes d'information. En raison de la nature dynamique des cybermenaces, ces dispositifs de sécurité doivent être constamment surveillés pour détecter rapidement toute anomalie ou défaillance, qu'il s'agisse

d'une tentative d'attaque, d'une mise à jour échouée, ou d'un dysfonctionnement de l'un de ces systèmes. Cela permet non seulement de maintenir une haute disponibilité des dispositifs, mais aussi d'assurer leur intégrité et leur bon fonctionnement dans la durée.
Les dispositifs critiques, tels que les pare-feu, les proxy, les solutions antivirus et les mécanismes de mise à jour, doivent être surveillés de manière proactive afin de :

- Identifier et corriger les vulnérabilités dès qu'elles sont détectées.
- Maintenir une couverture de sécurité constante.
- Garantir une résilience élevée contre les menaces informatiques.
- Assurer une disponibilité continue des services de sécurité sans interruptions qui pourraient compromettre la protection du SI.

3.4.3.1. Mise en œuvre des mesures de supervision

Pour garantir une gestion optimale de la sécurité, les entités doivent adopter des outils et des méthodes de supervision performants et adaptés à leurs besoins. Un système de supervision centralisé permet de suivre en temps réel l'état de chaque équipement de sécurité, de remonter les alertes et d'assurer un traitement rapide des incidents. Par exemple, un outil comme ServiceNav peut être utilisé pour surveiller de manière centralisée la disponibilité et les performances des équipements critiques.
Les mesures suivantes doivent être mises en œuvre pour garantir une supervision efficace des dispositifs de sécurité :

3.4.3.1.1. Supervision des pare-feu et proxy

- **Surveillance des flux de données entrants et sortants** : Il est essentiel de monitorer les flux pour détecter toute tentative d'intrusion ou de connexion non autorisée. Les pare-feu et les proxies doivent être configurés pour alerter en cas de comportements suspects, de violations des règles de sécurité ou de tentatives d'accès à des sites malveillants.
- **Mise à jour régulière des règles** : La supervision doit également vérifier que les règles de filtrage des pare-feu et des proxies sont régulièrement mises à jour pour répondre aux nouvelles menaces et vulnérabilités.

3.4.3.1.2. Supervision des antivirus et des mises à jour

- **Suivi de la mise à jour des signatures antivirus** : Un mécanisme de supervision doit permettre de vérifier que les bases de données des antivirus sont à jour et que les définitions de virus sont régulièrement mises à jour pour détecter les nouvelles menaces.
- **Vérification des déploiements de correctifs de sécurité** : La supervision des mises à jour doit inclure le suivi du déploiement de patchs de sécurité sur les équipements et les systèmes d'exploitation pour corriger les vulnérabilités connues.

3.4.3.1.3. Gestion des alertes et des incidents

- **Centralisation des alertes** : Un système de supervision centralisé doit être mis en place pour centraliser toutes les alertes provenant des équipements de sécurité. Cela permet aux équipes responsables de la sécurité d'évaluer rapidement la gravité des incidents et de prendre les mesures nécessaires.
- **Plan de réponse aux incidents** : Un plan détaillé de gestion des incidents doit être disponible pour garantir une réponse rapide et efficace face à toute alerte de sécurité.

3.4.3.1.4. Analyse et rapport des données de supervision

- **Rapports réguliers** : Les rapports générés par les outils de supervision doivent être analysés pour identifier les tendances, les anomalies et les zones à risque. Ces rapports doivent être partagés avec les responsables de la sécurité afin qu'ils puissent prendre les mesures nécessaires.
- **Évaluation continue des performances** : La supervision doit permettre d'évaluer l'efficacité des dispositifs de sécurité et de déterminer si des ajustements doivent être apportés pour améliorer leur performance et leur couverture de sécurité.

3.4.4. Autres types de contrôles nécessaires

Afin de garantir la sécurité et la conformité du système d'information (SI) du SITIV et des villes membres, il est impératif de mettre en place une série de contrôles réguliers et d'audits pour vérifier la bonne application des mesures de sécurité et assurer que les processus sont suivis correctement. Ces contrôles doivent couvrir divers aspects du système et des opérations afin de maintenir un environnement sécurisé et conforme aux exigences légales et réglementaires. Ci-dessous sont détaillés les types de contrôles nécessaires pour garantir une gestion efficace de la sécurité du SI :

3.4.4.1.1. Contrôle de la couverture de la PSSI-S par rapport à l'évolution des enjeux du SI

Il est essentiel que la **Politique de Sécurité des Systèmes d'Information (PSSI-S)** soit régulièrement mise à jour pour refléter les évolutions du système d'information et les nouveaux enjeux liés à la cybersécurité. Ce contrôle vise à garantir que la PSSI-S reste alignée avec les objectifs stratégiques du SI, les menaces émergentes et les risques liés aux nouvelles technologies, tout en répondant aux exigences réglementaires. Une révision périodique permet de détecter les lacunes potentielles dans la couverture de la sécurité et d'ajuster les mesures en conséquence.

- **Actions à mener :**
  - Réaliser des revues périodiques de la PSSI-S en fonction des évolutions du SI.
  - Mettre à jour les procédures et les mécanismes de contrôle de la sécurité en fonction des nouvelles menaces.
  - Évaluer l'adéquation de la PSSI-S avec les nouveaux projets et technologies déployées dans l'organisme.
  -

3.4.4.1.2. Contrôle de la bonne application des règles de gestion des accès & habilitations

Le contrôle de la gestion des accès et des habilitations est essentiel pour s'assurer que seules les personnes autorisées accèdent aux ressources sensibles et aux informations critiques du SI. Il s'agit de vérifier que les processus de gestion des utilisateurs (création, modification, suppression des comptes) sont rigoureusement suivis et que les niveaux d'accès sont attribués de manière appropriée en fonction des rôles et responsabilités des utilisateurs.

- **Actions à mener :**
  - Vérifier régulièrement les droits d'accès pour s'assurer qu'ils sont conformes aux principes du moindre privilège.

- Contrôler les processus d'habilitation et de révocation des accès pour s'assurer qu'ils sont réalisés conformément aux règles internes.
- Auditer périodiquement les comptes à privilèges pour s'assurer qu'ils ne sont pas utilisés de manière inappropriée.

3.4.4.1.3. Contrôle du respect des règles de sécurité par les Tiers (prestataires, infogérance)

Les prestataires externes et les services d'infogérance jouent un rôle clé dans la gestion et l'exploitation du SI. Il est donc impératif de s'assurer qu'ils respectent les mêmes normes de sécurité que celles imposées au sein de l'organisation. Cela inclut la validation de la conformité des prestataires aux exigences de sécurité, à travers des audits réguliers et des vérifications des pratiques mises en place.

- **Actions à mener :**
  - Vérifier la présence de clauses contractuelles de sécurité dans tous les contrats avec des prestataires.
  - Réaliser des audits réguliers sur les pratiques de sécurité des prestataires, en particulier ceux ayant accès à des informations sensibles.
  - Évaluer les rapports de conformité des prestataires aux règles de sécurité internes.

3.4.4.1.4. Contrôle de l'exploitation régulière des traces d'activités des comptes à privilèges

Les comptes à privilèges sont des vecteurs potentiels de risques en raison de leur capacité à accéder à des données sensibles et à effectuer des actions critiques. Le contrôle de l'exploitation des traces d'activité de ces comptes permet de détecter rapidement toute utilisation anormale ou abusive de leurs privilèges. Cela garantit que les actions effectuées avec ces comptes sont bien auditées et conformes aux règles de sécurité.

- **Actions à mener :**
  - Mettre en place une surveillance continue des logs générés par les comptes à privilèges.
  - Analyser régulièrement les traces d'activités pour détecter des comportements inhabituels ou suspects.
  - Évaluer les actions de remédiation en cas d'irrégularités détectées.

3.4.4.1.5. Contrôle de la présence de clauses contractuelles de sécurité dans l'ensemble des contrats fournisseurs

Les contrats avec les fournisseurs doivent inclure des clauses spécifiques concernant la sécurité des données, des équipements et des services fournis. Ces clauses doivent être conformes aux exigences réglementaires et aux normes internes du SITIV et des villes membres. Ce contrôle vise à s'assurer que toutes les parties prenantes sont contractuellement obligées de respecter les règles de sécurité.

- **Actions à mener :**
  - Vérifier que chaque contrat avec un fournisseur inclut des clauses spécifiques sur la sécurité des informations.
  - Auditer les contrats existants pour garantir qu'ils sont conformes aux exigences de sécurité actuelles.
  - Mettre en place un processus de révision des contrats de manière régulière.

3.4.4.1.6. Contrôle de l'efficacité des mesures de protection du réseau

Les mesures de protection du réseau, telles que les pare-feu, les systèmes de détection d'intrusion et les protections contre les attaques par déni de service, doivent être régulièrement évaluées pour s'assurer qu'elles sont efficaces face aux nouvelles menaces. Le contrôle de l'efficacité de ces mesures permet de s'assurer que le réseau est bien protégé contre les intrusions et autres attaques.

- **Actions à mener :**
  - Réaliser des tests d'intrusion réguliers pour évaluer la solidité des mesures de sécurité.
  - Analyser les performances des systèmes de protection du réseau et les ajuster si nécessaire.
  - Vérifier que les mises à jour des dispositifs de sécurité sont effectuées régulièrement.

3.4.4.1.7. Contrôle du respect des lois et règlements

Le respect des lois et des règlements en matière de protection des données, de cybersécurité et de gestion des SI est une obligation fondamentale. Ce contrôle a pour objectif de garantir que toutes les actions du SITIV et des villes membres sont conformes aux exigences légales en vigueur, telles que celles imposées par le RGPD, la loi sur la cybersécurité ou les normes sectorielles.

- **Actions à mener :**
  - Vérifier la conformité des systèmes d'information aux lois et règlements en matière de sécurité et de confidentialité des données.
  - Mettre en place un suivi des évolutions législatives et réglementaires et adapter les pratiques en conséquence.
  - Auditer régulièrement les processus internes pour garantir leur conformité aux normes légales.
  -

3.4.5. Réalisation d'audit de sécurité

L'audit de sécurité permet de vérifier la conformité des systèmes d'information (SI) aux exigences réglementaires et d'évaluer l'efficacité des mesures de sécurité mises en place. Ces audits réguliers (tous les 3 ans) assurent la protection des données et la résilience du SI face aux menaces et vulnérabilités identifiées.

- **Réalisation d'audits réguliers**

Un audit de sécurité complet doit être effectué tous les 3 ans pour évaluer la conformité aux mesures de sécurité et identifier les vulnérabilités. Un rapport détaillant la conformité, les failles et les recommandations sera diffusé aux villes membres concernées.

- **Tests intrusifs**

Des tests de pénétration doivent être réalisés tout les trois ans ou sur présentation d'une nouvelle architecture pour simuler des attaques réelles et évaluer la sécurité du SI

- **Rapport d'audit**

Le rapport d'audit présente les résultats, les non-conformités, et les vulnérabilités identifiées. Il fournit également des recommandations pour améliorer la sécurité du SI, avec un suivi des actions correctives mises en place.

3.5. Assurance et certification

3.5.1. Critères d'acquisition et conditions d'usage de progiciels (ACR-06)

Le SITIV et ses membres doivent garantir que la sécurité est un élément clé dans le processus d'acquisition et de mise en place de nouvelles applications, en accord avec la PSSI-S.

- **Intégration de la sécurité dès la conception**

Lors de l'acquisition de progiciels, la sécurité doit être intégrée dès les premières étapes du projet, conformément à la PSSI-S. Cela comprend la vérification de la conformité des applications aux exigences de sécurité avant leur déploiement.

- **Tests de conformité et restrictions d'utilisation**

Avant l'implémentation de toute nouvelle application, des tests de conformité doivent être effectués pour vérifier qu'elles respectent les normes de sécurité définies. De plus, des restrictions d'utilisation peuvent être mises en place pour limiter les risques associés à leur exploitation.

- **Qualifications et certifications**

Le SITIV et ses villes membres s'engagent à suivre des démarches de qualification ou de certification recommandées par l'État. Ces démarches garantiront que la sécurité est prise en compte à chaque étape, depuis la sélection du progiciel jusqu'à son déploiement et son utilisation au sein des infrastructures.

3.5.2. Maintenance de la documentation de sécurité

La documentation de sécurité doit être régulièrement mise à jour pour refléter les modifications apportées aux systèmes, processus ou politiques de sécurité. Chaque changement majeur, qu'il s'agisse de modifications techniques ou organisationnelles, doit entraîner une révision immédiate de la documentation associée.

- **Mise à jour continue de la documentation**

À chaque modification, qu'il s'agisse d'une mise à jour de système, d'une nouvelle procédure de sécurité ou d'une évolution de la réglementation, la documentation de sécurité doit être mise à jour en conséquence pour garantir sa pertinence et son efficacité. Cela inclut tous les documents techniques, opérationnels et stratégiques.

- **Archivage ou mise au rebut des versions précédentes**

Les anciennes versions de la documentation doivent être archivées de manière sécurisée ou détruites selon des procédures bien définies. Cela garantit que seules les versions les plus récentes et conformes sont accessibles, tout en préservant un historique des changements pour des fins de conformité et de traçabilité.

- **Organisation de la gestion documentaire**

Une organisation claire et définie doit être mise en place pour gérer la mise à jour, l'archivage et la destruction de la documentation. Cela comprend la désignation de responsables pour assurer la conformité et l'intégrité des documents tout au long de leur cycle de vie.

3.6. Gestion Humaine

3.6.1. Plan de responsabilité

Le dirigeant exécutif de l'entité désigne un ou plusieurs points de contact spécifiques pour les questions de sécurité numérique. Ces points de contact assurent la liaison directe avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et, le cas échéant, avec d'autres autorités nationales compétentes, et mettent à jour leurs coordonnées en cas de modification.

Une personne est nommée pour conseiller et accompagner le dirigeant dans ses responsabilités en matière de sécurité numérique. Cette personne agit comme interlocuteur privilégié de l'ANSSI sur tous les sujets de sécurité numérique, offrant expertise et continuité dans les échanges avec l'agence.

Le dirigeant exécutif est également chargé d'approuver la Politique de Sécurité des Systèmes d'Information (PSSI) de l'entité, assurant ainsi l'engagement de la direction dans la démarche de sécurité. En tant que responsable de la sécurité numérique, il veille particulièrement à la conformité des systèmes d'information réglementés avec les exigences de sécurité en vigueur.

L'entité consigne les coordonnées d'au moins un point de contact pour chaque élément figurant dans la cartographie de son écosystème, facilitant ainsi une communication structurée et réactive pour chaque acteur impliqué.

3.6.2. Tou les agents sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités

Les contrats de travail des agents rattachés au SITIV et à ses membres doivent inclure une annexe intitulée « Charte Informatique & Sécurité ». Cette charte, à signer par chaque agent, est conservée par les pôles ressources. Elle précise les responsabilités des utilisateurs concernant la sécurité des systèmes d'information ainsi que les règles d'utilisation des équipements mis à leur disposition, établissant ainsi un cadre clair et documenté pour promouvoir la sécurité numérique au sein de l'organisation.

3.6.3. Principe du moindre privilège

Les habilitations sont strictement personnelles et ne peuvent être transférées. La revue des habilitations doit s'effectuer annuellement en respectant le principe du moindre privilège, c'est-à-dire que le SITIV et ses membres attribuent à chaque utilisateur le niveau d'accès minimum nécessaire à l'exercice de ses fonctions. Pour renforcer la sécurité, le mot de passe du compte « administrateur local » doit être modifié périodiquement sur les postes de travail et serveurs, opération facilitée par l'utilisation de l'outil Microsoft LAPS (Local Administrator Password Solution).

3.6.4. Postes de travail sensibles

Les postes de travail de certaines catégories d'utilisateurs sont considérés comme sensibles et font partie intégrante du système d'information essentiel en raison de la nature de leurs fonctions et des responsabilités associées. Ces catégories incluent :

1. **Postes du Maire et des Élus** : ces postes sont stratégiques pour la prise de décisions et nécessitent un niveau de sécurité élevé pour éviter tout risque d'accès non autorisé à des informations sensibles.
2. **Postes du Directeur Général des Services et des Équipes de Direction** : en charge de la gestion et de la coordination des services, ces utilisateurs ont accès à des données et applications critiques pour la continuité des opérations de la collectivité.
3. **Postes des Administrateurs Systèmes** : ces postes disposent de droits d'administration sur le système d'information, ce qui nécessite des contrôles renforcés pour éviter tout risque de compromission de l'infrastructure.
4. **Postes des Agents à Mission Sensible** : certains agents, du fait de leurs missions spécifiques (finances, ressources humaines, sécurité), accèdent à des données confidentielles nécessitant une protection renforcée.

Pour ces postes, une **procédure d'habilitation spécifique** doit être mise en œuvre pour garantir que seuls les utilisateurs autorisés peuvent accéder aux ressources nécessaires, et uniquement dans la mesure de leurs besoins fonctionnels. Cette procédure prévoit une **validation préalable des droits d'accès**, une revue régulière des autorisations, et des contrôles rigoureux pour prévenir les abus. Les accès doivent être attribués selon le principe du **moindre privilège** afin de limiter l'exposition des informations sensibles.

3.7. Planification de la continuité des activités

3.7.1. Élaboration d'un plan de reprise

Le Plan de Reprise d'Activité (PRA) est essentiel pour assurer la continuité des opérations critiques du système d'information (SI) face aux perturbations majeures, qu'elles soient d'origine humaine, naturelle, accidentelle ou délibérée. Son objectif principal est de limiter les conséquences d'un incident majeur et de rétablir le SI dans son état de fonctionnement initial, permettant ainsi une reprise rapide et ordonnée des activités.

Le PRA repose sur une évaluation minutieuse des exigences opérationnelles critiques afin de définir les moyens nécessaires pour retrouver un fonctionnement normal. **Il inclut des procédures spécifiques pour fournir** des solutions temporaires et alternatives en cas de dysfonctionnement ou de défaillance d'un équipement, en garantissant que les services essentiels restent opérationnels jusqu'au retour complet à la normale.

Dans le cadre de son plan de service « Hébergement », le SITIV propose une infrastructure matérielle robuste, comprenant des serveurs, des systèmes de stockage, et des réseaux dédiés à l'hébergement sécurisé des applications métiers du SITIV et de ses collectivités membres. Cette infrastructure est conçue pour résister aux catastrophes naturelles et limiter l'accès aux seuls utilisateurs autorisés. Les serveurs virtualisés, les bases de données (notamment sous Oracle), et la messagerie bénéficient de mécanismes de sauvegarde régulière, garantissant une protection renforcée et un rétablissement rapide en cas d'incident majeur.

3.7.2. Mise en place des procédures de sauvegarde

Un plan de sauvegarde structuré est essentiel pour protéger les données critiques et assurer une reprise rapide des activités en cas de sinistre. Ce plan de sauvegarde doit être conçu en fonction des délais de reconstruction propres à chaque type d'activité et de processus, afin de minimiser les interruptions et pertes de données.

Pour garantir son efficacité, le plan de **sauvegarde doit être testé régulièrement, au minimum** une fois par trimestre. Ces tests permettent de vérifier la capacité de restauration des données et d'assurer que les sauvegardes répondent aux besoins opérationnels.

Afin de prévenir la perte de données en cas de sinistre sur le site principal, un nombre suffisant de copies de sauvegarde doit être stocké dans un emplacement distant et sécurisé. Cet emplacement doit être suffisamment éloigné pour ne pas être impacté par les mêmes risques environnementaux que le site d'origine.

Une revue annuelle du plan de sauvegarde est également indispensable pour s'assurer de sa conformité aux évolutions technologiques et organisationnelles, garantissant ainsi la fiabilité et la réactivité des procédures de restauration.

3.7.3. Test réguliers des plans

Afin de garantir un niveau de confiance élevé et la résilience des systèmes, le plan de continuité ainsi que les plans associés (plan de reprise d'activité, plan de continuité métier, plan de gestion de crise et plan de sauvegarde) doivent faire l'objet de tests réguliers. Ces exercices permettent de vérifier l'efficacité

des plans en conditions réelles et d'identifier d'éventuels dysfonctionnements ou retards dans les processus de reprise.

À l'issue de chaque test, un groupe de Retour d'Expérience (REX) est mis en place. Ce groupe analyse les points faibles ou les lenteurs rencontrés au cours de l'exercice, puis apporte des ajustements aux plans pour renforcer la réactivité et l'efficience des actions de continuité. Ce processus itératif de mise à jour des plans, basé sur des expériences concrètes, assure une amélioration continue et une meilleure préparation face aux crises éventuelles.

3.8. Gestion des incidents

3.8.1. Mise en place d'un réseau de détection et d'alerte des incidents de sécurité

La centralisation et l'analyse des journaux systèmes des équipements critiques (pare-feu, routeurs, serveurs, bases de données, etc.) sont essentielles pour la détection et la gestion proactive des incidents de sécurité. Ces journaux doivent être collectés dans une solution de gestion des informations et des événements de sécurité (SIEM) mutualisée. Cette solution corrèle les événements issus de différents équipements pour identifier des menaces potentielles et les relier à une même cause, offrant ainsi une visibilité accrue sur les incidents et une détection plus rapide.

En cas de détection d'un incident critique susceptible d'impacter significativement les systèmes d'information essentiels, une procédure de notification rapide aux autorités compétentes est mise en place, conformément aux obligations de la directive NIS2. Cette procédure inclut les éléments suivants :

- Identification des incidents critiques :

  Une évaluation immédiate est réalisée pour qualifier l'incident et déterminer s'il doit être classé comme critique. Un incident critique est défini comme ayant un impact majeur sur la disponibilité, l'intégrité ou la confidentialité des systèmes d'information essentiels, ou risquant d'entraîner des perturbations significatives pour les services publics ou les usagers.

- Délais de notification :

  Une fois l'incident identifié comme critique, l'entité est tenue de notifier l'ANSSI (ou toute autre autorité compétente) dans un délai de 24 à 72 heures selon la gravité :

  - Délai de 24 heures :

    Pour les incidents graves ayant un impact direct et immédiat sur les infrastructures critiques ou les services essentiels.

  - Délai de 72 heures :

    Pour les incidents qui nécessitent une surveillance renforcée mais dont l'impact est jugé moins immédiat.

- Contenu de la notification :

  La notification aux autorités doit comporter les informations suivantes, dans la mesure où elles sont disponibles au moment de la transmission :

  - Une description de l'incident, précisant sa nature et l'étendue de son impact.
  - La date et l'heure de détection de l'incident.
  - Les mesures de remédiation immédiates entreprises pour contenir les effets de l'incident.
  - Les coordonnées d'un point de contact responsable de la gestion de l'incident et de la coordination des actions de réponse.

- Suivi et rapports supplémentaires :

Si de nouvelles informations sont découvertes après la notification initiale, elles doivent être transmises aux autorités compétentes sans délai. Cela comprend l'analyse post-incident, les causes identifiées et les actions correctives mises en place pour éviter la récurrence de l'incident.

- Archivage et documentation :

Un registre détaillé des incidents critiques, incluant les notifications envoyées aux autorités, est maintenu pour assurer une traçabilité des actions entreprises. Ce registre comprend les chronologies, les mesures prises, les communications effectuées et les rapports transmis, ce qui permet un suivi rigoureux et peut être consulté lors de contrôles de conformité ou d'audits.

Pour appuyer cette démarche, l'utilisation de GLPI est recommandée pour le suivi des incidents, soutenue par des ressources humaines mutualisées afin d'assurer un niveau de sécurité homogène et optimisé pour toutes les entités impliquées.

Enfin, le RSSI mutualisé est chargé de maintenir et de présenter un tableau de bord des incidents de sécurité aux instances de gouvernance, incluant les Directions Générales, les DSI et les élus, afin de suivre l'évolution de la sécurité des systèmes et de garantir un pilotage éclairé en matière de cybersécurité. Ce tableau de bord inclut également le registre des incidents critiques, garantissant la transparence et facilitant la gestion de la conformité.

3.9. Sensibilisation et formation

La sensibilisation et la formation des utilisateurs, ainsi que des équipes en charge de la gestion des crises cyber, sont essentielles pour renforcer la capacité de l'entité à faire face aux menaces de cybersécurité. Pour cela, un programme structuré de sensibilisation et de formation est mis en place, ciblant tous les utilisateurs des systèmes d'information réglementés, ainsi que les personnels mobilisables en cas d'incident.

Ce programme comprend plusieurs points :

- Formation des équipes de gestion de crise : Les collaborateurs impliqués dans la gestion des crises cyber apprennent les procédures et réflexes nécessaires pour répondre efficacement aux incidents. Des exercices réguliers, qui simulent des scénarios de cyberattaques, permettent de tester les réponses des équipes et d'identifier des axes d'amélioration.

- Sensibilisation de tous les utilisateurs : L'ensemble des utilisateurs des systèmes d'information est régulièrement sensibilisé aux bonnes pratiques de sécurité numérique, comme la gestion des mots de passe, la vigilance face au phishing, et l'utilisation sécurisée des ressources numériques. Ces sessions rappellent à chacun l'importance de la vigilance individuelle et de la responsabilité partagée pour protéger le système d'information.

- Formation périodique obligatoire : En accord avec les exigences de la norme NIS2, tous les utilisateurs doivent suivre une formation obligatoire chaque année. Cette formation permet de maintenir à jour les connaissances de chacun sur les nouvelles menaces cyber et les bonnes pratiques de sécurité. Un suivi des participations est effectué pour garantir que chaque utilisateur est bien formé.

- Parcours de formation adapté aux rôles : Des parcours de formation continue sont proposés selon les niveaux de responsabilité et d'accès aux données. Les utilisateurs ayant accès à des informations sensibles suivent des modules spécifiques, pour une compréhension approfondie des risques et des comportements sécuritaires liés à leur rôle.

Ce programme de sensibilisation et de formation est régulièrement actualisé pour suivre les nouvelles menaces et les évolutions technologiques et réglementaires. En renforçant la culture de sécurité de ses utilisateurs, l'entité se dote d'un environnement où chacun contribue activement à la cybersécurité et à la protection des systèmes d'information.

3.10. Aspects physiques et environnementaux

3.10.1. Accès physique aux locaux, ses salles serveurs et ses locaux techniques

Le SITIV met en œuvre des mesures de sécurité strictes afin de limiter et de contrôler l'accès physique aux locaux sensibles, tels que les salles serveurs et les locaux techniques, dans le but de protéger les infrastructures et les données critiques de l'entité. L'accès à ces zones est réservé aux personnes dûment autorisées, et des contrôles d'accès physiques sont systématiquement appliqués pour empêcher toute intrusion non autorisée.

Le SITIV veille à ce que chaque point d'entrée aux locaux, aux salles serveurs et aux locaux techniques soit protégé par des dispositifs de sécurité appropriés, tels que des systèmes de verrouillage électronique, des contrôles d'accès par badges, ou des dispositifs biométriques. De plus, des contrôles d'identité peuvent être effectués à chaque entrée, avec une vérification rigoureuse des personnes accédant à ces espaces sensibles.

Un autre objectif clé est de garantir la traçabilité des accès physiques. Chaque entrée et sortie de ces zones est enregistrée, et des systèmes de surveillance vidéo (CCTV) peuvent être utilisés pour monitorer les zones à haut risque, assurant ainsi une surveillance continue et la possibilité de réaliser des audits réguliers.

En ce qui concerne l'accès des personnes externes, telles que les prestataires ou les visiteurs, le SITIV impose une procédure stricte. Toute personne externe souhaitant accéder aux locaux techniques ou aux salles serveurs doit être accompagnée en permanence par un membre autorisé du personnel. Cette mesure vise à garantir que toute intervention ou présence dans ces zones sensibles soit supervisée, évitant ainsi tout risque d'accès non autorisé ou de manipulation des équipements.

Enfin, des audits réguliers des dispositifs de contrôle d'accès physique et des procédures associées sont effectués pour s'assurer que les mesures mises en place restent conformes aux standards de sécurité les plus élevés et aux exigences réglementaires en matière de protection des infrastructures critiques.

3.10.2. Chiffrement des équipements

Conformément aux exigences de la directive NIS 2, l'entité a défini et met en œuvre des politiques de sécurité robustes couvrant plusieurs domaines clés afin de protéger les systèmes d'information et les données sensibles. Ces politiques incluent notamment :

1. **L'usage du chiffrement** : L'entité déploie des mécanismes de chiffrement avancés pour garantir la confidentialité et l'intégrité des données sensibles en transit et au repos. Le chiffrement est appliqué sur toutes les communications et supports de données, y compris les mémoires de masse des postes de travail et équipements mobiles.
2. **Le contrôle d'accès physique et logique** : Des mesures strictes sont prises pour contrôler l'accès aux systèmes d'information et aux locaux sensibles, tant sur le plan physique (accès aux locaux, salles serveurs) que logique (contrôle d'accès aux applications et ressources réseau). Ces contrôles permettent de limiter l'accès aux seules personnes autorisées, réduisant ainsi les risques d'accès non autorisé.
3. **La revue de l'application des mesures de sécurité** : L'entité s'assure que les mesures de sécurité mises en place sont régulièrement revues et évaluées pour vérifier leur efficacité. Ces

évaluations permettent de garantir que les politiques et procédures de sécurité sont correctement appliquées et restent adaptées face aux évolutions des menaces et des technologies.

4. **Le maintien en condition de sécurité** : Un processus continu de surveillance et de mise à jour des mesures de sécurité est instauré pour assurer le maintien des systèmes dans un état opérationnel et sécurisé. Cela inclut l'application de correctifs, de mises à jour logicielles et de réévaluations des risques.

En ce qui concerne les équipements mobiles et les postes de travail permettant un accès à distance au Système d'Information Réglementé (SIR) depuis des lieux non maîtrisés par l'entité, des protections renforcées sont mises en place. Les mémoires de masse de ces appareils, tels que les disques durs et les supports amovibles, sont systématiquement protégées par des mécanismes de **chiffrement** et d'**authentification** conformes aux meilleures pratiques et à l'état de l'art, tel que recommandé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Le chiffrement garantit que, même en cas de vol ou de perte de ces dispositifs, les données restent inaccessibles à toute personne non autorisée. Par ailleurs, l'authentification permet de s'assurer que seules les personnes légitimes peuvent accéder aux systèmes et aux ressources du SIR. Ces mesures sont régulièrement réévaluées pour s'assurer qu'elles respectent les normes de sécurité les plus élevées et qu'elles s'adaptent aux nouvelles menaces potentielles.

3.11. Identification et authentification

3.11.1. Gestion de l'identité dans le système d'information

La gestion des secrets d'authentification est essentielle pour garantir l'intégrité et la sécurité des systèmes d'information. Selon la nature des applications et des services, les moyens de protection des secrets d'authentification doivent être adaptés et différenciés en fonction des niveaux de sécurité requis. En effet, un même secret ne doit être utilisé que pour des services ou applications présentant un niveau de sécurité équivalent, afin de ne pas compromettre l'intégrité de l'ensemble du système.

Dans cette optique, le **SITIV** et les collectivités territoriales membres adoptent une **authentification forte**, qui repose sur deux éléments distincts. Chaque utilisateur devra non seulement fournir un mot de passe robuste, mais également un second facteur d'authentification, tel qu'un mot de passe à usage unique (OTP, One-Time Password). Cette double authentification vise à renforcer la sécurité des accès aux ressources critiques et sensibles de l'entité.

Le service de double authentification est déjà mis en œuvre et doit être généralisé sur l'ensemble des systèmes d'information essentiels et/ou sensibles de l'entité. Cette démarche s'inscrit dans une politique de sécurité proactive, visant à se conformer aux bonnes pratiques en matière de cybersécurité, en particulier face aux risques croissants de cyberattaques.

- **Collaboration avec le Projet National AgentConnect Territoires**

Dans un souci d'harmonisation et de sécurisation des identités, le SITIV choisit de collaborer au projet national AgentConnect Territoires. Ce projet vise plusieurs objectifs importants pour les administrations publiques et les acteurs territoriaux :

- **Offrir un référentiel d'identité national** des agents et élus des collectivités territoriales (CT), garantissant une gestion centralisée et sécurisée des identités.
- **Permettre un accès unique** aux services numériques fournis par l'ensemble des acteurs (collectivités, État, fournisseurs de services privés, etc.), simplifiant l'accès tout en renforçant la sécurité.
- **Fournir un haut niveau de qualification et de certification de l'identité**, validée par l'autorité territoriale, afin d'assurer une gestion fiable et sécurisée des identités des agents.
- **Gestion et Contrôle des Identités**

L'identité des utilisateurs doit être gérée sous le contrôle direct de l'autorité territoriale, qui en est le gestionnaire principal. Le SITIV, en tant que fournisseur de services, met à disposition les moyens techniques nécessaires pour assurer un contrôle efficace et sécurisé de cette identité. Cela inclut l'implémentation d'outils d'authentification et de gestion des identités permettant de garantir l'intégrité et la traçabilité des accès aux systèmes.

L'**identification unique et sans équivoque** du propriétaire d'un accès est cruciale pour garantir la traçabilité des opérations et faciliter le diagnostic des anomalies de sécurité (audit et contrôle). Cette approche permet de mieux comprendre les actions effectuées sur les systèmes et de réagir rapidement en cas d'incident de sécurité.

- **Règles et Conditions pour la Délivrance des Moyens d'Authentification**

Dans le cadre de la gestion des moyens d'authentification, plusieurs règles strictes sont appliquées pour assurer la sécurité des accès et protéger l'identité des utilisateurs :

1. **Engagement formel** : Avant la délivrance d'un accès par authentification à un nouvel utilisateur, ce dernier doit s'engager formellement à respecter les règles de protection des moyens d'accès fournis, et à signaler immédiatement en cas de vol ou de perte de ces moyens.
2. **Délivrance des moyens d'accès** : La remise des moyens d'accès, tels que les mots de passe, doit être réalisée de manière exceptionnelle et dans des conditions garantissant que seul le propriétaire du compte en ait connaissance. Ce processus doit être encadré et sécurisé.
3. **Traitement des incidents de sécurité** : En cas de vol ou de perte d'un secret d'authentification, des mesures immédiates doivent être prises pour empêcher toute tentative d'usurpation d'identité, incluant la réinitialisation des accès et l'enquête sur l'incident.
4. **Suppression des accès lors d'un départ** : Le départ d'un agent (qu'il s'agisse d'un licenciement ou d'une mutation) doit systématiquement conduire à la suppression immédiate de tous ses accès aux systèmes d'information, afin de prévenir tout risque d'accès non autorisé après son départ.
5. **Gestion sécurisée des accès** : L'utilisation du gestionnaire d'accès LemonLDAP doit être priorisée pour assurer un niveau d'accès le plus sécurisé possible. Ce gestionnaire permet de centraliser et de sécuriser la gestion des authentifications tout en simplifiant l'accès aux ressources pour les utilisateurs autorisés.

Commenté [sH12]: Verifier avec Anasse cette partie

3.12. Politique des comptes et comptes administrateurs

Une politique de gestion des comptes est essentielle pour garantir la sécurité et l'intégrité des systèmes d'information de l'entité. Elle définit les principes et les procédures qui régissent la création, l'attribution, la gestion, la révision et la suppression des comptes utilisateurs et administrateurs, en veillant à ce que chaque utilisateur ou processus automatisé dispose des droits d'accès nécessaires et proportionnels à ses fonctions. Cette politique repose sur des principes de sécurité clés, tels que le principe du moindre privilège, l'authentification robuste, la traçabilité des actions et la gestion des comptes inactifs. Elle vise à prévenir les risques d'accès non autorisés, à assurer la conformité avec les normes de sécurité en vigueur, et à garantir une gestion transparente et contrôlée des droits d'accès. Pour plus de détails sur les exigences et les pratiques à suivre, veuillez consulter le document complet de la politique de gestion des comptes.

Commenté [sH13]: Dois je mettre la politique la ?

3.13. Contrôle d'accès

3.13.1. Règles d'accès au système d'information

L'accès au système d'information du SITIV et de ses membres doit être rigoureusement contrôlé afin de garantir la confidentialité, l'intégrité et la disponibilité des données. À cet effet, plusieurs dispositifs de sécurité essentiels sont mis en place, parmi lesquels les pare-feu, les systèmes d'authentification, et les mécanismes de contrôle d'accès. Ces dispositifs sont considérés comme des priorités dans la mise en œuvre de la politique de sécurité des systèmes d'information (PSSI).

Les pare-feu servent à filtrer le trafic entrant et sortant des réseaux internes, empêchant les accès non autorisés et les tentatives d'intrusion. Les systèmes d'authentification assurent que seules les

personnes et processus légitimes peuvent accéder aux ressources et services du Système d'Information Réglementé (SIR), tandis que les contrôles d'accès définissent et vérifient les droits des utilisateurs en fonction de leur rôle au sein de l'entité.

- Segmentation du Réseau pour Renforcer la Sécurité

Une autre mesure clé dans la sécurisation des systèmes d'information consiste à mettre en place une segmentation des réseaux (ou cloisonnement), qui doit être réalisée dès que cela est possible. Cette approche permet de diviser le réseau en segments distincts afin de contrôler plus efficacement les accès et d'augmenter la sécurité des données. La segmentation vise plusieurs objectifs spécifiques :

- Contrôle d'accès renforcé : En isolant les différentes parties du réseau, il devient plus facile de limiter l'accès aux ressources critiques et de restreindre la communication entre les segments.
- Protection contre les intrusions : En cas de compromission d'un segment, les attaquants seront limités dans leur capacité à se déplacer latéralement dans le réseau, réduisant ainsi les risques de propagation d'une attaque.
- Prévention des fuites d'information : La segmentation empêche les données sensibles de s'échapper vers des réseaux externes ou de transiter via des techniques d'attaque comme le rebond, où un attaquant tente d'utiliser une machine compromise pour atteindre d'autres ressources.

Cette segmentation peut être réalisée de manière efficace à l'aide de VLANs (Virtual Local Area Networks) configurés sur des switchs. Les VLANs permettent de créer des réseaux virtuels isolés au sein d'un même réseau physique, améliorant ainsi la sécurité en limitant les interactions entre différents segments de réseau.

- Responsabilité du RSSI et Sécurité Mutualisée

Le Responsable de la Sécurité des Systèmes d'Information (RSSI) joue un rôle clé dans l'application de la PSSI mutualisée et dans la gestion des risques au sein des infrastructures mutualisées. Le RSSI est chargé de veiller à l'application des politiques de sécurité, d'assurer la conformité aux normes en vigueur, et de superviser les mesures de sécurité au sein des systèmes d'information de l'entité et de ses membres. Il est également responsable de l'analyse et de la gestion des risques mutualisés qui concernent les ressources partagées au sein du réseau.

Le RSSI doit également intervenir sur la sécurité de l'infrastructure mutualisée, en s'assurant que les processus de sécurisation et les contrôles sont adaptés et appliqués de manière cohérente à l'ensemble des composants de l'infrastructure partagée.

- Sécurisation des Réseaux de Télécommunications

L'utilisation des réseaux de télécommunications pour l'accès des utilisateurs, les connexions des postes de travail isolés, et la segmentation des réseaux ne doit en aucun cas compromettre les mesures de sécurité physiques mises en place. En effet, les réseaux de télécommunications, bien qu'indispensables pour le fonctionnement quotidien des systèmes d'information, doivent être sécurisés de manière complémentaire pour garantir qu'aucune brèche ne soit laissée dans la protection des réseaux physiques.

Cela implique que les mesures de sécurité physiques, telles que le contrôle d'accès aux câblages et équipements réseau, les dispositifs de surveillance, et les mécanismes de prévention des accès non autorisés, doivent être étendues et renforcées pour couvrir tous les éléments d'infrastructure, y compris les composants télécoms utilisés pour les connexions distantes.

3.13.2. Transmission des mots de passe

Dans le **Système d'Information** (SI) du **SITIV** et des systèmes d'information des **villes membres**, la protection des mots de passe constitue une priorité absolue pour assurer la confidentialité et l'intégrité des données. Tous les fichiers contenant des mots de passe, qu'ils soient actifs ou obsolètes, doivent impérativement être soit supprimés, soit chiffrés afin de limiter les risques de fuite ou d'utilisation non autorisée.

Afin de répondre à ces exigences, le SITIV a mis en place des mesures techniques spécifiques pour protéger les mots de passe à différents niveaux du système. Ces mesures se déclinent en deux grands axes selon la nature des comptes concernés.

3.13.2.1.1. Comptes d'utilisateurs nominatifs : Coffre-fort Bitwarden

Pour les comptes d'utilisateurs nominatifs, qui sont attribués à des individus et liés à des accès spécifiques, le SITIV recourt à l'utilisation d'un coffre-fort numérique sécurisé, à savoir Bitwarden. Bitwarden est une solution de gestion de mots de passe robuste et conforme aux bonnes pratiques de sécurité. Elle permet de stocker, gérer et partager des mots de passe de manière sécurisée grâce à un chiffrement de bout en bout.

Ce coffre-fort numérique est particulièrement adapté pour garantir que les mots de passe des utilisateurs ne sont jamais stockés en texte clair. En plus de stocker les mots de passe, Bitwarden permet aussi de générer des mots de passe complexes, uniques et difficiles à deviner, contribuant ainsi à la réduction du risque de compromission lié à l'utilisation de mots de passe faibles ou réutilisés. L'accès au coffre-fort Bitwarden est protégé par une authentification forte et des mécanismes de sécurité supplémentaires (tels que l'authentification multi-facteurs), garantissant ainsi que seuls les utilisateurs autorisés peuvent accéder à leurs mots de passe.

3.13.2.1.2. Comptes d'utilisateurs de service : Solution de Sécurisation des Accès à Privilèges

Pour les comptes d'utilisateurs de service, souvent utilisés dans des contextes techniques tels que la configuration des serveurs ou des processus automatiques, le SITIV met en œuvre des solutions avancées de sécurisation des accès à privilèges. Ces comptes sont souvent associés à des droits d'accès étendus, ce qui en fait un vecteur potentiel d'attaque en cas de mauvaise gestion.

3.13.3. Contrôle global des accès

Dans le cadre de la gestion de la sécurité du Système d'Information (SI) du SITIV et des villes membres, il est impératif d'assurer un contrôle strict des accès, en particulier ceux qui ne sont pas sous contrôle direct ou qui sont susceptibles de présenter un risque pour la sécurité. Les accès non maîtrisés doivent être immédiatement identifiés et bloqués afin de prévenir toute tentative d'intrusion ou de compromission.

3.13.3.1.1. Identification et Blocage des Accès Non Maîtrisés

Les accès non maîtrisés peuvent se manifester de différentes manières, comme par exemple l'utilisation d'un poste de travail connecté à la fois au SI et à une connexion 4G ou la connexion physique non autorisée d'un poste au réseau local. Dans ces situations, l'accès au réseau de l'entité est ouvert à des canaux externes non sécurisés, ce qui expose potentiellement le SI à des risques d'intrusion. Par conséquent, il est impératif que ces accès soient rigoureusement identifiés et immédiatement bloqués. Cela implique une surveillance continue du réseau, ainsi que la mise en place de politiques de segmentation et de contrôles d'accès renforcés, notamment en matière de contrôle des connexions externes et des périphériques non autorisés.

Des outils de surveillance et de détection des accès non autorisés doivent être utilisés pour garantir que toute tentative de connexion par un canal non maîtrisé soit instantanément repérée et bloquée. De plus, des dispositifs de filtrage et de contrôle d'accès doivent être appliqués pour limiter les connexions à distance à des connexions sécurisées et validées par l'entité.

3.13.3.1.2. Traçabilité et Protection Renforcée des Accès de Maintenance à Privilèges Élevés

Les accès de maintenance aux systèmes d'information, notamment pour les prestataires et les fournisseurs, représentent un vecteur de risques important. Ces accès permettent de réaliser des interventions techniques, parfois avec des privilèges élevés, sur des ressources sensibles du SI. Il est donc crucial de mettre en place des moyens de traçabilité rigoureux et des mesures de protection renforcée pour surveiller ces accès.

Pour cela, des outils de gestion des accès à privilèges (PAM – Privileged Access Management) doivent être utilisés pour gérer, contrôler et auditer toutes les actions effectuées par des utilisateurs externes disposant de privilèges élevés. Ces outils permettent non seulement de garantir que les actions sont effectuées par des personnes autorisées, mais aussi d'assurer une traçabilité complète des interventions et des modifications apportées aux systèmes. Les prestataires et fournisseurs doivent être soumis à une authentification forte, et l'accès à certaines zones du système d'information doit être limité au strict nécessaire, avec des enregistrements détaillés de chaque opération réalisée.

3.13.3.1.3. Gestion des Profils d'Utilisateurs Locaux

Les profils d'utilisateurs locaux sont sous la responsabilité et le contrôle de chaque collectivité. Cette gestion décentralisée permet de maintenir un certain degré d'autonomie au sein des différentes entités tout en respectant des normes de sécurité strictes. Le SITIV, quant à lui, assure pour ses collaborateurs la gestion des profils d'utilisateurs locaux de manière centralisée et indépendante.

Cela signifie que, bien que les collectivités aient la liberté de gérer leurs propres profils utilisateurs locaux, le SITIV intervient en tant que garant de la conformité et de la sécurité de cette gestion pour ses employés. Il est essentiel que chaque profil local soit configuré de manière sécurisée, avec des contrôles réguliers sur les accès et les privilèges attribués à chaque utilisateur. La séparation des rôles et la limitation des privilèges sont des principes fondamentaux de cette gestion, afin d'éviter les risques liés à des comptes mal configurés ou abusés.

3.13.4. Environnement du poste de travail

Dans le cadre de la gestion de la sécurité des postes de travail au sein du Système d'Information (SI) du SITIV et des villes membres, des mesures strictes sont mises en place pour prévenir les risques liés à l'usurpation d'identité et limiter l'accès non autorisé aux fonctions sensibles des postes de travail.

3.13.4.1. Mise en Veille Automatique pour Prévenir l'Usurpation d'Identité

Pour éviter toute tentative d'usurpation d'identité ou d'accès non autorisé lorsqu'un utilisateur quitte son poste de travail, celui-ci doit être configuré de manière à se mettre automatiquement en veille après un délai d'inactivité. Cette mesure permet de garantir que, même en l'absence de l'utilisateur, le poste reste inaccessible sans procédure de réauthentification. En effet, lorsqu'un poste est laissé sans surveillance, il devient vulnérable à des accès malveillants. En activant une mise en veille automatique, l'accès au système est restreint et nécessite à chaque reprise une identification claire et sécurisée de l'utilisateur.

Cette fonctionnalité peut être couplée à des politiques de verrouillage automatique de l'écran, renforçant ainsi la sécurité physique des postes de travail, en particulier dans des environnements partagés ou publics. L'objectif est de s'assurer que seuls les utilisateurs autorisés peuvent accéder à leurs ressources personnelles et professionnelles, réduisant ainsi les risques de fuites d'informations ou de modifications non autorisées.

3.13.4.2. Limitation des Droits d'Accès aux Fonctions Sensibles

Les droits d'accès aux fonctions d'administration et de sécurité des postes de travail doivent être strictement limités et réservés uniquement au personnel habilité. Ces droits incluent des accès à des fonctionnalités sensibles, comme les configurations systèmes, les paramètres de sécurité, ou la gestion des applications critiques. Afin de protéger ces fonctions contre les risques d'accès non autorisé, seules les personnes ayant reçu une autorisation spécifique et ayant été formées aux bonnes pratiques de sécurité sont autorisées à y accéder.

Les autres utilisateurs, même s'ils disposent d'un accès au poste de travail, ne doivent pas pouvoir modifier les configurations de sécurité ni intervenir dans les processus administratifs. L'application de ces règles est cruciale pour garantir l'intégrité des systèmes et éviter tout abus ou compromission des données sensibles. Les contrôles d'accès basés sur les rôles (RBAC – Role-Based Access Control) doivent être utilisés pour appliquer cette séparation stricte des fonctions et restreindre l'accès en fonction des responsabilités de chaque utilisateur.

En outre, des journaux d'audit doivent être activés pour enregistrer toutes les actions effectuées sur les fonctionnalités d'administration et de sécurité des postes de travail. Ces logs permettent de garantir une traçabilité complète des modifications effectuées, ce qui est essentiel pour toute analyse post-incident en cas de problème de sécurité.

3.13.5. Journalisation

3.13.5.1. Journalisation des intrusions

Dans le cadre de la gestion de la sécurité des postes de travail au sein du Système d'Information (SI) du SITIV et des villes membres, des mesures strictes sont mises en place pour prévenir les risques liés à l'usurpation d'identité et limiter l'accès non autorisé aux fonctions sensibles des postes de travail.

3.13.5.1. 1. Mise en Veille Automatique pour Prévenir l'Usurpation d'Identité

Pour éviter toute tentative d'usurpation d'identité ou d'accès non autorisé lorsqu'un utilisateur quitte son poste de travail, celui-ci doit être configuré de manière à se mettre automatiquement en veille après un délai d'inactivité. Cette mesure permet de garantir que, même en l'absence de l'utilisateur, le poste reste inaccessible sans procédure de réauthentification. En effet, lorsqu'un poste est laissé sans surveillance, il devient vulnérable à des accès malveillants. En activant une mise en veille automatique, l'accès au système est restreint et nécessite à chaque reprise une identification claire et sécurisée de l'utilisateur.

Cette fonctionnalité peut être couplée à des politiques de verrouillage automatique de l'écran, renforçant ainsi la sécurité physique des postes de travail, en particulier dans des environnements partagés ou publics. L'objectif est de s'assurer que seuls les utilisateurs autorisés peuvent accéder à leurs ressources personnelles et professionnelles, réduisant ainsi les risques de fuites d'informations ou de modifications non autorisées.

3.13.5.2. 2. Limitation des Droits d'Accès aux Fonctions Sensibles

Les droits d'accès aux fonctions d'administration et de sécurité des postes de travail doivent être strictement limités et réservés uniquement au personnel habilité. Ces droits incluent des accès à des fonctionnalités sensibles, comme les configurations systèmes, les paramètres de sécurité, ou la gestion des applications critiques. Afin de protéger ces fonctions contre les risques d'accès non autorisé, seules les personnes ayant reçu une autorisation spécifique et ayant été formées aux bonnes pratiques de sécurité sont autorisées à y accéder.

Les autres utilisateurs, même s'ils disposent d'un accès au poste de travail, ne doivent pas pouvoir modifier les configurations de sécurité ni intervenir dans les processus administratifs. L'application de ces règles est cruciale pour garantir l'intégrité des systèmes et éviter tout abus ou compromission des données sensibles. Les contrôles d'accès basés sur les rôles (RBAC – Role-Based Access Control) doivent être utilisés pour appliquer cette séparation stricte des fonctions et restreindre l'accès en fonction des responsabilités de chaque utilisateur.

En outre, des journaux d'audit doivent être activés pour enregistrer toutes les actions effectuées sur les fonctionnalités d'administration et de sécurité des postes de travail. Ces logs permettent de garantir une traçabilité complète des modifications effectuées, ce qui est essentiel pour toute analyse post-incident en cas de problème de sécurité.

3.13.6. Gestion des traces

Dans le cadre de la gestion de la sécurité du Système d'Information (SI) du SITIV et des villes membres, il est primordial de mettre en place des moyens de journalisation afin de détecter et d'enregistrer toute activité

suspecte ou malveillante au sein des systèmes. La journalisation des événements et des intrusions permet non seulement de renforcer la sécurité mais aussi d'améliorer la capacité de réponse en cas d'incident.

3.13.6.1. Objectifs de la Journalisation

La journalisation des intrusions ou des utilisations malveillantes sert deux objectifs principaux :

Identification des causes et origines de l'intrusion : En cas d'incident de sécurité, la journalisation permet de recueillir des informations détaillées sur les actions suspectes et les événements qui ont mené à l'incident. Cela comprend la collecte de logs de connexions, d'activités sur le réseau, d'accès non autorisés, et d'autres comportements inhabituels. Ces données permettent une analyse approfondie et aident les équipes de sécurité à identifier rapidement les vulnérabilités exploitées et à remédier aux failles.

Preuves de l'intrusion : En plus de la résolution de l'incident, la journalisation permet de disposer de preuves tangibles de l'intrusion ou de l'utilisation malveillante des systèmes. Ces éléments peuvent être cruciaux pour des actions légales, des enquêtes ou des audits de sécurité. Les logs doivent être conservés de manière sécurisée et immuable pour garantir leur intégrité et leur valeur en cas de besoin.

3.13.6.2. Mise en Place de la Journalisation

Afin d'assurer une couverture complète, le SITIV et les villes membres doivent installer des systèmes de journalisation sur tous les composants critiques du SI, incluant les serveurs, postes de travail, réseaux et autres infrastructures sensibles. Ces systèmes doivent être capables de capturer et de stocker les événements dans des journaux sécurisés qui seront utilisés pour analyser les incidents et garantir une traçabilité complète.

Les logs doivent inclure des informations telles que :

- Les tentatives de connexion (réussies et échouées) et les activités suspectes,
- Les modifications de configurations ou d'accès aux ressources sensibles,
- Les anomalies réseau, comme les connexions suspectes ou l'accès à des zones non autorisées,
- Les changements dans les privilèges d'utilisateur, ou les activités liées à des comptes à privilèges élevés.

3.13.6.3. Conservation et Sécurisation des Logs

Les logs doivent être stockés dans un environnement sécurisé, avec des contrôles d'accès stricts pour en garantir l'intégrité. Des mécanismes de chiffrement et de contrôle d'accès doivent être utilisés pour empêcher toute altération des journaux. De plus, un système de gestion centralisée des logs (par exemple, SIEM - Security Information and Event Management) peut être déployé pour faciliter la collecte, l'analyse et la corrélation des événements en temps réel, ce qui permet une réaction rapide face à toute anomalie.

3.13.6.4. Plan de Réponse à l'Incident de Sécurité

La journalisation des intrusions s'inscrit dans une approche globale de gestion des incidents de sécurité. Le SITIV dispose d'un plan de réponse à incident de sécurité (voir annexe), qui définit les actions à entreprendre en cas d'intrusion ou de comportement malveillant. Ce plan inclut des procédures pour l'analyse des logs, l'identification des auteurs potentiels, l'évaluation de l'impact de l'incident, ainsi que les mesures correctives et préventives à mettre en place.

3.13.7. Système d'alerte de sécurité

La gestion des traces (logs et autres données d'activité) doit être rigoureusement encadrée. Cette gestion garantit la traçabilité des actions réalisées, permet de détecter les incidents de sécurité en temps utile et répond aux exigences réglementaires en matière de sécurité. Les traces sont gérées selon des règles strictes, définies par l'entité, afin d'assurer leur intégrité, leur confidentialité et leur conformité aux normes de sécurité applicables.

3.13.7.1.1. Archivage des Traces

Les traces générées par les systèmes du SITIV doivent être archivées de manière sécurisée et structurée pour une durée définie, en fonction de leur importance et de leur réglementation applicable. L'archivage permet de garantir leur disponibilité en cas de besoin, que ce soit pour des audits internes, des enquêtes de sécurité, ou des vérifications légales. Les systèmes doivent être équipés de mécanismes d'archivage automatique, permettant de conserver les logs dans des supports protégés et accessibles uniquement aux personnes autorisées.

3.13.7.1.2. Suppression des Traces Obsolètes

Les traces doivent être supprimées de manière sécurisée lorsque leur conservation n'est plus nécessaire ou qu'elles sont considérées comme obsolètes. Cette suppression doit respecter les délais légaux et les politiques internes du SITIV. Des processus automatisés de gestion du cycle de vie des traces doivent être mis en place pour garantir qu'aucune trace obsolète ne soit conservée au-delà de la période définie, réduisant ainsi le risque d'exposition de données sensibles.

3.13.7.1.3. Filtrage des Traces

Un filtrage des traces doit être réalisé pour exclure les données non pertinentes ou redondantes, et ainsi optimiser la gestion des logs. Ce filtrage vise à réduire le volume des traces à analyser, tout en conservant l'intégrité des informations essentielles à la détection et à l'analyse des incidents. Il est essentiel que le filtrage soit effectué sans altérer la qualité des données permettant une reconstruction complète des événements en cas de besoin.

3.13.7.1.4. Analyse des Traces

L'analyse des traces est une étape fondamentale pour détecter des anomalies, des tentatives d'intrusion ou des comportements malveillants dans le système. Les outils d'analyse doivent être utilisés de manière régulière pour traiter les logs en temps réel ou pour effectuer des audits périodiques. L'analyse permet d'identifier des incidents de sécurité, des vulnérabilités, ou des erreurs dans les configurations système. En fonction des résultats, des actions correctives et préventives doivent être prises pour éviter que de tels incidents ne se reproduisent.

3.13.7.1.5. Protection des Traces

Les traces doivent être protégées contre toute altération ou suppression non autorisée. Des mécanismes de contrôle d'intégrité doivent être appliqués pour garantir que les traces restent fiables et ne puissent être modifiées à des fins malveillantes. Cela inclut l'utilisation de hachage cryptographique et d'autres technologies permettant de vérifier l'intégrité des logs au fil du temps. Une protection renforcée

des supports de stockage des traces (serveurs, bases de données, etc.) est également nécessaire pour prévenir tout accès non autorisé.

3.13.7.1.6. Alerte en Cas d'Altération des Traces

Il est essentiel de mettre en place des alertes automatiques en cas d'altération ou de modification des traces. Ces alertes permettent de détecter toute tentative de manipulation des logs, assurant ainsi une réponse rapide en cas de compromission des données. En cas d'alerte, les équipes de sécurité doivent pouvoir identifier immédiatement l'origine de l'incident et les actions correctives à entreprendre.

3.13.7.1.7. Destruction au-Delà du Délai Légal

Au-delà du délai légal de conservation, les traces doivent être détruites de manière irréversible pour éviter toute réutilisation ou accès non autorisé. La destruction sécurisée des traces garantit que les données sensibles ne sont pas exposées une fois qu'elles ne sont plus nécessaires pour répondre à des obligations légales ou des besoins internes. Les méthodes de destruction doivent être conformes aux standards de sécurité, assurant qu'aucune donnée ne puisse être récupérée après la suppression.

3.13.8. Gestion des équipements

Seules les ressources matérielles clairement identifiées, qu'elles appartiennent au SITIV, à son personnel ou à ses prestataires, et participant directement à la réalisation des activités, à la fourniture des services ou au maintien en condition opérationnelle et de sécurité, sont autorisées à se connecter aux systèmes d'information réglementés. Cette approche vise à restreindre l'accès aux systèmes sensibles et à assurer un contrôle total sur les équipements connectés.

Afin de garantir cette restriction, le SITIV met en place des mesures organisationnelles et techniques robustes pour empêcher toute connexion non autorisée de ressources matérielles non identifiées aux systèmes d'information réglementés. Cette mesure vise à limiter les risques d'intrusion ou de contamination par des équipements non conformes.

En ce qui concerne les supports amovibles réinscriptibles, seuls ceux strictement nécessaires à l'accomplissement des activités et services de l'entité, ou au maintien en condition opérationnelle ou de sécurité, sont autorisés à se connecter aux systèmes d'information réglementés. Par ailleurs, les postes de travail, serveurs et équipements mobiles maîtrisés par l'entité, et amenés à traiter des données provenant de sources externes (telles que les supports amovibles, la messagerie électronique ou la navigation web), sont dotés de mécanismes de protection avancés visant à prévenir l'exécution de codes malveillants.

Pour renforcer la sécurité, l'entité procède à une analyse systématique de toutes les données reçues provenant de sources externes, afin d'identifier et d'éliminer toute trace de code malveillant avant leur traitement dans les systèmes d'information. Cette analyse fait partie d'une démarche proactive pour garantir l'intégrité des systèmes et la sécurité des données.

3.13.9. Segmentation réseau

Le SITIV met en place une segmentation réseau rigoureuse afin de cloisonner physiquement ou logiquement l'ensemble de ses systèmes d'information réglementés des autres systèmes d'information. Cette

segmentation vise à limiter les risques d'accès non autorisé et à garantir que les systèmes critiques et sensibles sont protégés contre toute intrusion venant d'autres parties du réseau.

Seules les interconnexions nécessaires au bon fonctionnement des activités et services de l'entité, ou celles requises pour maintenir les systèmes en condition opérationnelle et assurer leur sécurité, sont autorisées entre les systèmes d'information réglementés et les autres systèmes. Ces interconnexions sont scrupuleusement contrôlées par des règles de filtrage strictes, lesquelles n'autorisent que les communications jugées indispensables. Par défaut, toutes les autres communications sont bloquées afin de réduire les surfaces d'attaque et d'éviter les risques de fuite de données ou d'intrusion.

Au minimum, les communications entre les systèmes d'information réglementés du SITIV et ceux des tiers sont filtrées à l'aide de pares-feux spécifiquement dédiés à cet usage, garantissant ainsi que seules les connexions légitimes soient permises. Le SITIV s'assure également, à travers des audits réguliers, que les règles de filtrage sont toujours efficaces et adaptées aux besoins en matière de sécurité. Chaque année, une revue technique complète des configurations et de l'application de ces règles est réalisée pour s'assurer que les dispositifs de filtrage demeurent conformes aux exigences de sécurité actuelles et aux meilleures pratiques.

Commenté [sH14]: Mettre lien avec le doc de segmentation