Politique de sécurité des systèmes d'information (PSSI)

Sud Roussillon
COMMUNAUTÉ DE COMMUNES

Référence : PSSI-SR V2

Responsable du projet :
ROUMEGOUS Nicolas, DSI/RSSI informatique@sudroussillon.fr

Versions :

Date : 07/2018	1.0	Création du document
Date : 11/2024	2.0	Modification du document

SOMMAIRE

1. Préambule

1.1. Objectif du document

Ce document constitue la Politique de Sécurité des Systèmes d'Information Générale (PSSI-SR) de la communauté de communes Sud Roussillon.
Il fixe les objectifs, l'organisation en matière de sécurité et les principes de sécurité applicables de façon transverse à tous les systèmes d'information.
Cette politique générale est rédigée et maintenue à jour par le Responsable de la Sécurité des Systèmes d'Information (RSSI). Elle s'appuie sur les orientations stratégiques de la direction générale ainsi que sur des normes et réglementations nationales et internationales sur la sécurisation des Systèmes d'Information.
La PSSI-SR fait partie intégrante du plan d'action cybersécurité de Sud Roussillon comportant :

- PSSI
- Schéma directeur 2025-2030
- Fiches reflexes
- Plan de continuité d'activité

1.2. Évolutions

La présente PSSI-SR évolue pour tenir compte des changements qui peuvent affecter les systèmes d'information et l'environnement, notamment en termes d'enjeux et de menaces. Elle est en conséquence mise à jour en fonction :

- ❖ Des évolutions de la réglementation et des engagements contractuels avec les partenaires ;
- ❖ Des évolutions des exigences issues de l'agence nationales de la sécurité des systèmes d'information (ANSSI) ;
- ❖ Des nouvelles menaces et risques liés à l'évolution des technologies des systèmes d'information et à leur complexification ;
- ❖ Des évolutions des systèmes d'information ;
- ❖ Des résultats des audits concernant sa mise en application ;
- ❖ Des conclusions tirées des rapports de traitement des incidents.

La révision de la PSSI-SR est réalisée lors de modifications majeures, par le RSSI puis proposée à la Direction Générale de l'établissement pour validation.

1.3. Diffusion

La politique de Sécurité Générale est un document interne de la communauté de communes. Il est communiqué aux agents publics, à l'autorité de tutelle et aux partenaires, lorsque c'est nécessaire et dès lors qu'ils sont acteurs des systèmes d'information. Elle peut également être communiquée par le RSSI au cas par cas et sur demande écrite et justifiée à d'autres tiers extérieurs (exemple : organisations officielles, auditeurs externes, prestataires, etc.).

1.4. Entrée en vigueur

La politique de sécurité est validée par la direction générale. Elle entre en vigueur dès diffusion à l'ensemble des agents publics.
Tous les pôles de Sud Roussillon doivent respecter les principes fondamentaux édictés dans cette politique générale ainsi que dans les différentes politiques de sécurité opérationnelles associées.
Elles doivent également être contractuellement imposées aux partenaires et prestataires de l'EPCI.

2. Contexte et objectifs

2.1. Contexte

La Communauté de Communes Sud Roussillon regroupe 6 communes Alenya, Corneilla-del-Vercol, Latour-Bas-Elne, Montescot, Saint-Cyprien et Théza pour une population proche de 24 000 habitants. Cette EPCI a de multiples compétences déclinées en plusieurs services opérateurs. Cette spécificité entraîne l'interconnexion entre plusieurs lieux distants.

- Centre José Arrieta
- Espace Aquasud
- Déchetterie Intercommunale

Situés sur la commune de Saint-Cyprien, ces différents sites peuvent être interconnectés, par différentes technologies. Ils disposent chacun d'un raccordement au réseau national de télécommunication.

2.2. Périmètre de la SSI

La Sécurité des Systèmes d'Information (SSI) couvre l'ensemble des systèmes d'information de l'établissement avec toute la diversité que cela implique dans les usages, les lieux d'utilisation, les méthodes d'accès, les personnes concernées…

- Le système informatique de gestion ;
- Les applications institutionnelles (messagerie, applications et publications Internet, stockage, sauvegarde…) et celles propres aux composantes (applications métiers, traitement des données, bureautique…) ;
- Les systèmes hors du champ informatique s'appuyant néanmoins sur ses ressources (ToIP/VoIP, vidéosurveillance, …) ;
- Les interconnexions entre les différents pôles (Voirie, Service Déchets, etc.…).

2.3. Sécuriser les SI : une nécessité

L'évolution des technologies et des systèmes de traitement de l'information et celle, concomitante, des menaces informatiques et des cyberattaques, justifient l'attention que la communauté de communes Sud Roussillon porte à la sécurité de ses systèmes d'information. Cette attention porte sur la protection des systèmes d'information critiques, mais aussi plus largement sur la protection du patrimoine informatique de l'EPCI qui constitue un actif clé.
De manière accidentelle ou délibérée, provenant de l'interne ou de l'externe, dans un cadre ciblé ou opportuniste, un incident de sécurité pourrait entraîner des conséquences sérieuses pour la collectivité et pour ses partenaires :

- Perte du patrimoine informationnel, par la destruction massive de données se traduisant par une perte de valeurs et/ou désorganisant durablement l'établissement
- Arrêt ou dysfonctionnement de certains processus de l'établissement à des périodes critique, empêchant le fonctionnement normal de celui-ci.

- Divulgation de données sensibles valorisables, fuite de données de santé traitées par les ressources humaines, fuite des données personnelles des agents publics ;
- Attaque d'un partenaire au travers de l'établissement, de ses SI ou de son personnel ;
- Risque juridique, par exemple amende infligée par la CNIL en raison d'une négligence ayant mené à l'exfiltration de données personnelles protégées par la loi, ou liées à une violation de propriété intellectuelle.

Il est donc nécessaire de protéger et de sécuriser les systèmes d'information de Sud Roussillon, et ce à la hauteur des enjeux qu'ils représentent et en cohérence avec les risques et les menaces qui pèsent sur eux.

2.4. Sécuriser les SI : une opportunité

La sécurité des systèmes d'information est également appréhendée comme une opportunité lui permettant, d'une part, d'intégrer sereinement les avancées technologiques, et d'autre part de renforcer la relation de confiance avec ses partenaires privés et publics.
Lorsque la sécurité est traitée en amont des projets, précisément gérée par des acteurs identifiés et avec l'engagement de la Direction, son coût peut être rationalisé et son retour sur investissement, certes indirect, peut être maximisé.
Le DSI veille à la prise en compte de la présente PSSI-SR dans les projets de systèmes d'information, en faisant mener les analyses de risques nécessaires, en décidant des mesures de sécurité techniques ou organisationnelles à mettre en place et en contrôlant leur application.

2.5. Les objectifs stratégiques en matière de sécurité

Afin de répondre aux enjeux de sécurité précédents, Sud Roussillon a défini des objectifs stratégiques qui constituent la cible à atteindre en matière de sécurité des systèmes d'information :

- Permettre à la collectivité d'assurer, même de façon dégradée, les activités métiers ;
- Être en mesure d'anticiper et de contribuer à la gestion coordonnée des situations de crise relatives aux systèmes d'information et celles susceptibles d'interrompre les activités ou de nuire à son image ;
- Respecter les exigences réglementaires et législatives
- Ne pas compromettre les données des partenaires, les données de santé fournies ou l'écosystème qui gravite autour de Sud Roussillon ;
- Protéger son personnel, ses actifs et ses partenaires contre toute forme de menace, accidentelle ou intentionnelle ;
- Contribuer à la performance globale de la communauté de communes et préserver sa réputation ;
- Faire de la sécurité un facteur d'opportunité et de croissance dans la création de nouveaux systèmes, notamment en anticipant les évolutions (nouvelles menaces, nouvelles technologies ...) et en répondant aux attentes de la direction, des élus et des partenaires.

Afin de satisfaire ses objectifs stratégiques, la CC Sud Roussillon définit un ensemble de

politiques de sécurité opérationnelle qui propose des règles et des mesures techniques. Ces politiques opérationnelles visent à garantir une protection efficace, rationalisée, proportionnée aux enjeux et améliorée dans le temps des activités et des processus.
Les politiques de sécurité opérationnelle sont élaborées sur la base des fonctions de sécurité ci-dessous :

- **L'Anticipation** : Anticiper l'occurrence de menaces et de toute non-conformité réglementaire (Gestion des risques, Gestion de la conformité réglementaire, Gestion de la conformité avec les exigences contractuelles des partenaires, etc.) ;

- **La Protection** : Mettre en place des mécanismes de protection adaptés (Protection des actifs, Protection des biens supports, Protection des informations reçues de la part des partenaires, etc.) ;

- **La Détection** : Détecter les événements de sécurité pour se donner la capacité de réagir (Journalisation, Corrélation, Détection, etc.) ;

- **La Réaction** : Réagir face à des incidents de sécurité et reconstruire les actifs pour assurer une reprise d'activité dans les plus brefs délais (Gestion des incidents, Reprise d'activité, Retour à la normale, etc.) ;

- **L'Amélioration** : S'inscrire dans une logique d'adaptation dynamique des postures de sécurité et d'amélioration continue.

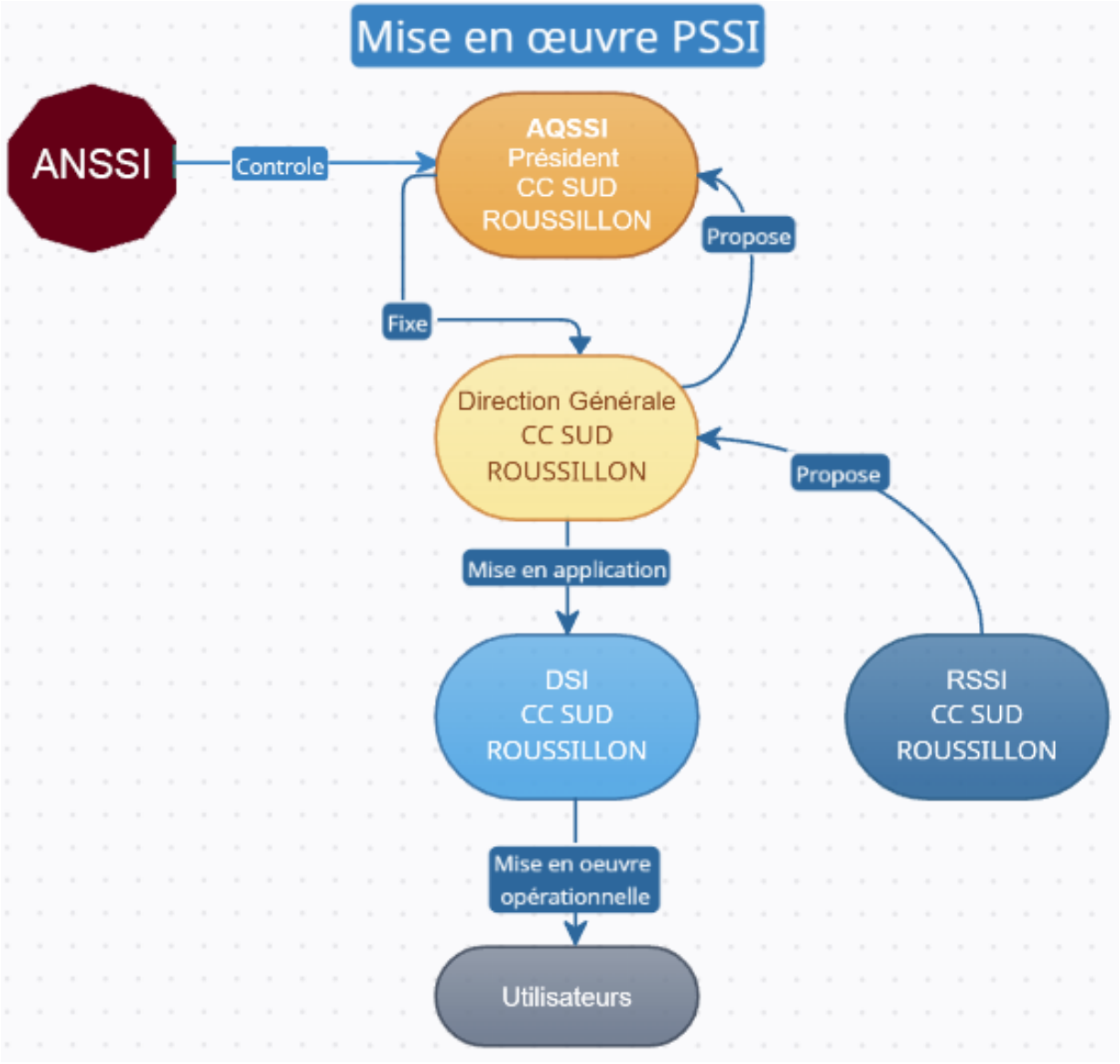
Le respect des politiques de sécurité opérationnelle est une obligation de tous les acteurs - interne et externe de Sud Roussillon, en lien direct ou indirect avec les systèmes d'information.

2.6. Pilotage

Au sein de la Communauté de Communes, la responsabilité générale de la Sécurité des Systèmes d'Information relève du Président en tant qu'Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI). Il est assisté dans cette fonction par le responsable de la sécurité des Systèmes d'Information (RSSI).
Le pilotage courant est de la responsabilité du RSSI/DSI. La mise en œuvre opérationnelle est assurée par le service informatique pour le contrôle des données entrantes et sortantes ainsi que le service commun informatique.
Pour assurer cette fonction, les agents sont des relais essentiels tant pour appliquer et faire respecter la PSSI de l'établissement que pour faire remonter les éventuels incidents.

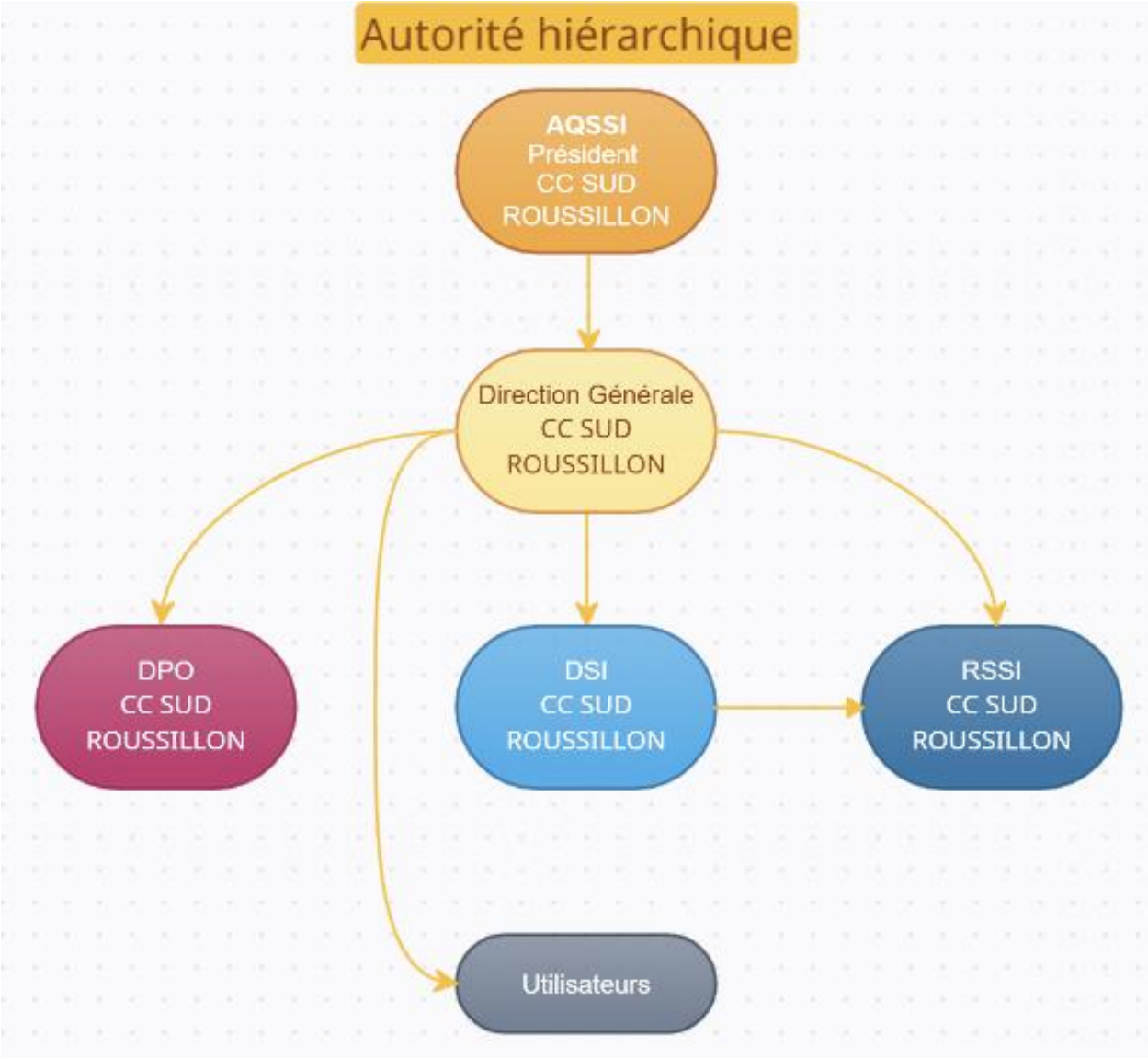
3. Mise en œuvre de la PSSI

La PSSI de la Communauté de Communes Sud Roussillon affiche un ensemble de principes d'ordre organisationnel et technique à caractère prioritaire. Ces principes sont explicités, dans le cadre d'instructions ou dispositions techniques dont la responsabilité d'élaboration, de diffusion et d'information relève de la chaine fonctionnelle SSI.



3.1. Responsabilités des différents acteurs

Les acteurs intervenant en matière de Sécurité des Systèmes d'Information doivent être informés de leurs responsabilités en matière de SSI. Dans l'exercice de leur activité, ils sont liés à leur devoir de réserve en tant qu'agent public, et plus largement à des obligations de secret professionnel.



3.1.1. Président (Autorité Qualifié SSI)

La maîtrise et la gestion de la sécurité globale relèvent de la responsabilité première du Président (en sa qualité d'AQSSI) de l'EPCI. Il porte ainsi la responsabilité de la gestion des risques cybersécurité et des travaux de mise en conformité réglementaire. Cette responsabilité lui enjoint de se doter des moyens et de l'organisation les plus adaptés pour gérer les risques et la conformité réglementaire relatifs aux systèmes d'information de Sud Roussillon. À ce titre, le Président réalise, sur la base des travaux effectués par la chaine SSI des contraintes réglementaires, un arbitrage sur la gestion des risques, et décide des budgets et moyens débloqués pour le programme sécurité.

La direction générale exprime son leadership et son engagement en faveur du programme sécurité en :

- S'assurant que la politique et les objectifs sécurité sont établis et qu'ils sont compatibles avec l'orientation stratégique de la CC Sud Roussillon ;
- S'assurant que les ressources nécessaires pour la mise en place du plan d'action sont disponibles ;
- Communicant sur l'importance d'une continuité d'activité efficace et de se conformer aux exigences de la politique de sécurité ;
- S'assurant via le reporting que la politique de sécurité atteint les résultats et objectifs escomptés ;
- Orientant et soutenant les agents pour qu'ils contribuent à l'efficacité du plan d'action et qu'ils respectent les règles de la politique de sécurité ;
- Promouvant l'amélioration continue ;

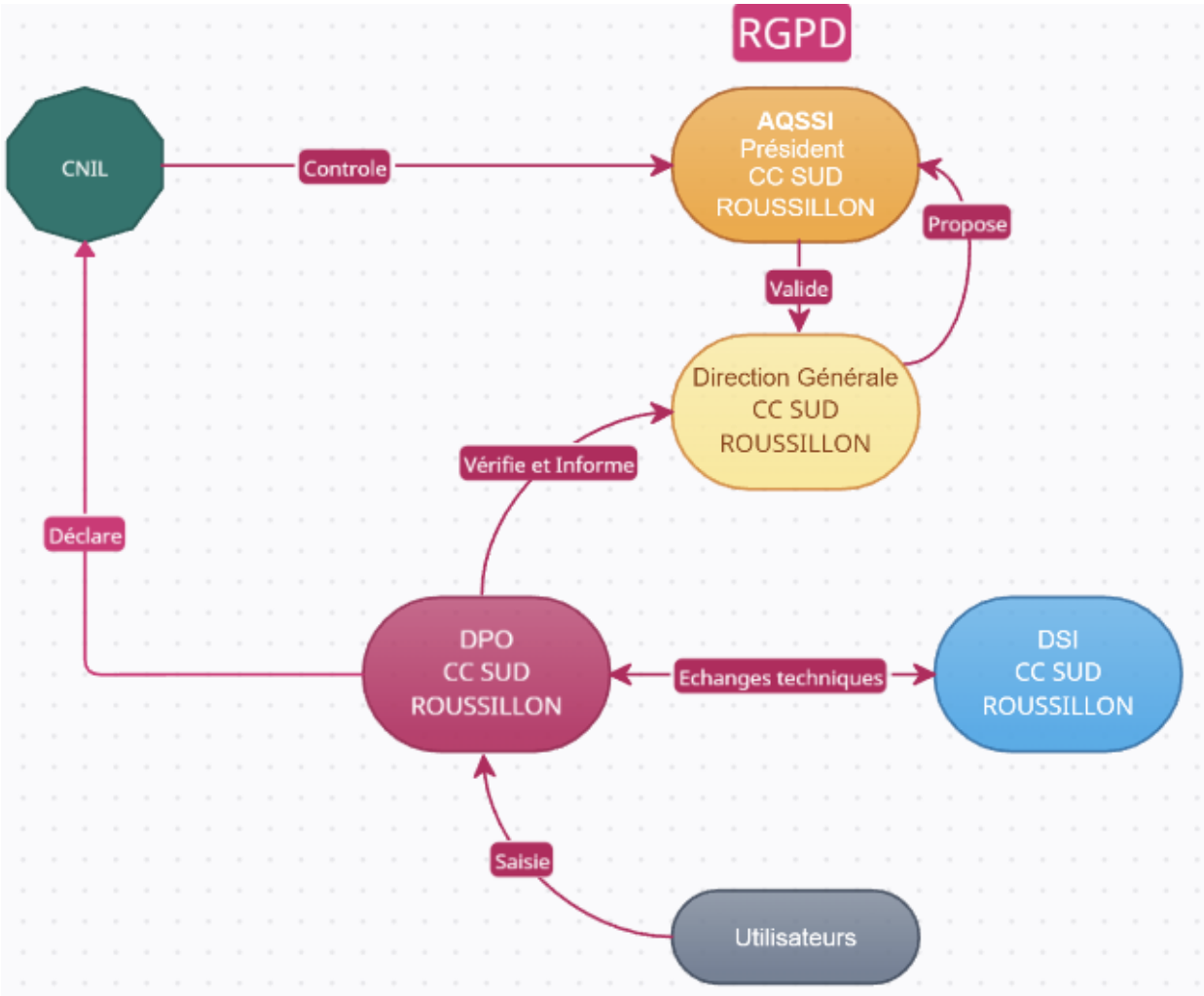
3.1.2. Responsable de la Sécurité des Systèmes d'Information

Le Responsable de la Sécurité des Systèmes d'Information (RSSI) exerce sous l'autorité du Directeur Général des Services, les activités suivantes :

- Contribuer activement à l'élaboration d'une politique de sécurité cohérente admise par tous et la mettre en œuvre.
- Viser tous les projets de l'établissement afin de veiller à la mise en œuvre au sein de ces derniers des éléments technologiques nécessaires à l'application de la PSSI.
- Exploiter et relayer les informations relatives à la sécurité en provenance du CERT-FR et de l'ANSSI…
- Faire connaître et respecter la charte d'utilisation des moyens informatiques et réseau de l'établissement.
- Proposer et mettre en œuvre des actions de sensibilisation et d'information de tous les utilisateurs aux aspects sécurité des systèmes d'information.
- Être l'intermédiaire direct en cas de problème entre la Communauté de Communes et les autorités compétentes.

3.1.3. Délégué à la protection des données (DPO)

Le DPO à la responsabilité de conseiller et d'accompagner la Direction Générale dans la définition d'un programme de mise en conformité avec les exigences juridiques, techniques et sécurité du RGPD.
Le DPO à la responsabilité de contrôler le respect du programme de mise en conformité et d'exercer un reporting pour assurer le suivi au plus haut niveau du programme.
En particulier, le DPO a la responsabilité de traiter, avec l'appui de la DSI et du RSSI, d'identifier les incidents RGPD se produisant sur le SI, et de contrôler l'application du plan de traitement des risques identifiés.



3.1.4. Utilisateurs internes

Chaque utilisateur interne du système (agents, stagiaires, prestataires, etc..) respecte les règles de sécurité édictées par la PSSI et par la charte informatique, respecte les dispositifs et les mesures de sécurité, informe le RSSI de tous incidents ou anomalies constatées.

3.1.5. Direction des systèmes d'information (DSI)

Les équipes de la DSI assurent le développement et le fonctionnement des ressources informatiques et de télécommunication. Ils mettent en œuvre les services de sécurité des SI et de contrôle, en conformité avec la PSSI et pour répondre aux exigences formulées par la direction.
Ils définissent et mettent en application les plans d'action techniques pour :

- L'intégration des règles et mesures de sécurité des SI dans leurs activités ;
- L'intégration des mesures de sécurité en phase de conception de chaque projet (Security By Design) ;
- La détection et la réaction en cas d'incident informatique.

Les équipes de la DSI respectent les procédures internes, afin de garantir :

- Un niveau de sécurité homogène entre les différents composants du SI ;
- Le respect des mesures de sécurité de la PSSI.

Par défaut, la DSI est le garant de l'application des mesures de sécurité pour tous les composants du système d'information inscrit dans son périmètre de contrôle.

3.2. Organisation

3.2.1. Accès des utilisateurs aux ressources informatiques

La mise à disposition de moyens informatiques doit être formalisée à l'arrivée, au changement de fonction et au départ de chaque utilisateur. L'accès aux ressources doit être contrôlé (identification, authentification) et adapté au droit de chacun (droits et privilèges, profil utilisateur).

3.2.2. Charte informatique

Préalablement à son accès aux outils informatiques, l'utilisateur doit prendre connaissance des droits et devoirs que lui confère la mise à disposition de ces outils par la collectivité. Cette information se fait au travers de la « charte du bon usage des moyens informatiques » intégrée dans le règlement intérieur de la Communauté de Communes Sud Roussillon.

3.2.3. Cyber Surveillance

La Sécurité des Systèmes d'Information exige de pouvoir surveiller le trafic sur le réseau et tracer les actions effectuées. Les dispositifs mis en œuvre doivent être conformes à la réglementation en vigueur et respecter les principes de proportionnalité (adaptation du niveau des moyens à l'enjeu effectif de la sécurité) et de transparence (information des partenaires sociaux et utilisateurs).

4. Le pilotage de la sécurité

4.1. Comité stratégique de la sécurité des SI

Un comité stratégique de la sécurité des systèmes d'information réunit le Directeur Général ou tout autre membre de la direction et le RSSI. Il permet d'assurer :

- Le suivi et l'amélioration continue de la sécurité au niveau de Sud Roussillon ;
- Le suivi des règles de la politique de sécurité ;
- Le suivi des travaux de mise en conformité réglementaire et contractuelle ;
- L'information de la Direction Générale quant au niveau de risque cyber qui pèse sur l'EPCI
- La mise à disposition des ressources nécessaires pour assurer la conformité aux règles de la Politique de Sécurité des Systèmes d'Information ;
- Le suivi et la revue des processus de sécurité (Gestion des risques, Gestion d'incident, Gestion de la continuité d'activité, etc.).

4.2. Tableaux de bord de suivi

Le pilotage de la sécurité implique la mise en place d'une structure de suivi et induit la mise en place de tableaux de bord. Ces tableaux de bord sont réalisés par le RSSI et doivent intégrer des indicateurs relatifs :

- Aux risques de sécurité ;
- Au taux d'application de la politique de sécurité ;
- Aux nombres d'incidents de sécurité rencontrés.

5. Protection des données

5.1. Disponibilité, confidentialité et intégrité des données

Le traitement et le stockage des données numériques, l'accès aux applications et services et les échanges de données entre systèmes d'information doivent être réalisés selon des méthodes visant à prévenir la perte, la modification et la mauvaise utilisation des données ou la divulgation des données ayant un caractère sensible.
Une sauvegarde régulière des données avec des processus de restauration régulièrement validés est mise en place. On distinguera les sauvegardes de production (par exemple, restauration d'une donnée) des sauvegardes de recours (par exemple, reprise des services sur des moyens externes suite à incident majeur). Une étude fine des données (criticité, volatilité, fluctuation…) permettra de définir la périodicité et le type de sauvegarde ainsi que la durée de rétention dans le respect des législations en vigueur.

5.2. Protection des données sensibles

Les données présentant un caractère sensible doivent être identifiées. Elles devront faire l'objet d'une protection au niveau du contrôle d'accès (authentification et contrôle d'autorisation), du traitement, du stockage ou de l'échange (chiffrement) pour en assurer la confidentialité.
Avant toute cession ou mise au rebut d'un matériel ayant contenu des données sensibles, il est nécessaire de s'assurer que toutes les données ont bien été effacées par un procédé efficace et selon les recommandations techniques nationales. Si cela s'avère impossible les supports concernés devront être détruits.

5.3. Données à caractère personnel

Les traitements de données susceptibles de contenir des informations à caractère personnel (au sens de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés) doivent faire l'objet des formalités requises par le Règlement Général sur la Protection des Données (RGPD).

Les données à caractère personnel constituent des données sensibles et comme telles doivent faire l'objet de protection.

5.4. Chiffrement

Le chiffrement, en tant que moyen de protection, est obligatoire pour le stockage et l'échange de données sensibles. Les produits matériels et logiciels utilisés doivent faire l'objet d'un agrément par la CDC Sud Roussillon. Une copie des clés permettant de restituer les données en clair doit être fourni au service informatique et stockée dans un lieu sécurisé.

6. Principes et processus de sécurité

La communauté de communes Sud Roussillon appuie la sécurité de ses systèmes d'information sur des processus permettant leur amélioration continue et leur ajustement à l'évolution des missions, du cadre réglementaire et des menaces pesant sur ses environnements numériques. Les principaux processus sont décrits ci-dessous.

Les processus de la présente politique, fixant un cadre général, se valent indépendants des technologies et des mécanismes de sécurité. Elles sont donc complétées par des instructions et mesures de sécurité, sous forme de politiques opérationnelles, qui déclinent au niveau opérationnel les principes fondamentaux.

6.1. Gestion des risques et conformité

Sud Roussillon prend en compte les risques pouvant affecter ses systèmes d'information à différents niveaux :

- **Risques stratégiques :** Une analyse des risques globale, qui couvre tous les périmètres de l'EPCI, est élaborée et maintenue à jour. Elle propose une vision macro des risques qui pèsent sur les systèmes d'information et permet de formaliser les règles de la politique de sécurité. Elle sert à mettre à jour tous les 5 ans la PSSI opérationnelle ;

- **Risques propres à un système :** Si nécessaire, chaque sous-système d'information peut faire l'objet d'une analyse des risques spécifiques en prenant en compte le contexte et l'écosystème du périmètre étudié ;

- **Risques projets informations « Security By Design » :** Chaque projet doit faire l'objet d'une appréciation des risques SSI afin d'élaborer les objectifs sécurité du projet. Ces objectifs sont traduits en exigences sécurités, intégrées dans le cahier des charges et dont le bon respect est contrôlé par le RSSI.

Pour le cas particulier du Règlement Général sur la Protection des Données (**RGPD**), le RSSI se tient à la disposition du Délégué à la Protection des Données (DPO) de l'établissement.

6.2. Sélection et application des mesures de sécurité

Les mécanismes de sécurité mis en place au sein de Sud Roussillon sont sélectionnés par le RSSI conformément aux objectifs de sécurité fixés, en prenant en compte le contexte de la collectivité.

7. Sécurisation du système d'information

7.1. Administration des serveurs

L'administration des serveurs de l'établissement est placée sous la responsabilité de l'administrateur systèmes et réseaux du service informatique.

7.2. Administration des postes de travail

L'administration des postes de travail individuels est placée sous la responsabilité de l'administrateur systèmes et réseaux. L'administration des postes par les utilisateurs eux-mêmes doit demeurer l'exception et être justifiée en termes de besoins et de compétences. L'administrateur systèmes et réseaux peut intervenir à distance pour des opérations de maintenance sur le poste de travail d'un utilisateur après l'en avoir averti et en respectant les principes de la loi Informatique et Libertés.

7.3. Sécurisation des postes de travail et des moyens nomades

La sécurisation des postes de travail et des moyens nomades est placée sous la responsabilité de l'administrateur systèmes et réseaux. L'accès aux postes de travail et moyens nomades doit être protégé par mots de passe suffisamment robustes ; chaque mot de passe est personnel et confidentiel et, à ce titre, il ne doit pas être divulgué à un tiers, quel qu'il soit, ni laissé sans protection.
Les utilisateurs veillent au bon déroulement des applicatifs de sécurisation installés sur les moyens informatiques mis à leur disposition : mises à jour effectives de l'anti-virus, du système d'exploitation et des applications présentes, remontée des dysfonctionnements et incidents auprès de l'administrateur systèmes et réseaux. En particulier, les utilisateurs prendront des mesures spécifiques adaptées en cas d'utilisation des moyens nomades en dehors de leur zone de sécurité (protection contre le vol, chiffrement...).
Les utilisateurs nomades prendront garde à ne pas se reconnecter sur le réseau de Sud Roussillon des lors qu'ils auront une suspicion sur leur poste de travail tant qu'ils n'auront pas eu l'accord de la DSI.

7.4. Contrôle d'accès

Tout accès au système d'information est soumis à l'identification/authentification du demandeur et au contrôle de ses autorisations/habilitations. L'authentification doit se faire, dans la mesure du possible, au travers de l'annuaire LDAP de la Communauté de Communes. Il importe de bien définir les autorisations et de n'attribuer que les privilèges nécessaires. Les accès doivent être journalisés. L'utilisation de comptes partagés ou anonymes doit demeurer l'exception et être justifiée en termes de besoins.
L'attribution et la modification des accès et privilèges d'un service doivent être validées par le chef de service et le DSI.

7.5. Accès par des tiers et sous-traitance

L'infogérance correspond au fait que des sociétés extérieures, chargées de gérer une partie de l'informatique, ont accès au système d'information depuis l'extérieur ou l'intérieur. Un contrat entre Sud Roussillon et chaque société doit clairement préciser les droits d'accès, les engagements de responsabilités et l'imputabilité en cas d'incident. Des mécanismes permettant de s'assurer du respect des limites d'intervention doivent être mis en œuvre dans la mesure du possible.

Tout accès, qu'il soit physique ou logique, local ou à distance, aux ressources et informations de Sud Roussillon par des tiers est accordé dans un cadre strict en fonction des besoins de la mission.

Les accès sont formellement approuvés par l'agent auquel ils sont rattachés et le RSSI.
L'externalisation de la gestion d'exploitation d'un composant critique pour le système d'information est à proscrire, sauf dispositions de garantie spécifiques et validée au niveau du RSSI.

7.6. Réseaux internes

L'administration des réseaux est placée exclusivement sous la responsabilité du DSI.
Les systèmes d'information doivent être protégés vis-à-vis de l'extérieur à l'aide de filtres d'accès appliqués sur les équipements en tête de son réseau. Ces filtres s'appliquent tant sur les flux réseau entrants que sur les flux sortants.
L'accès extérieur aux postes de travail doit demeurer l'exception et être justifié en termes de besoins et de compétences. La politique de définition des filtres d'accès décrivant les flux réseau entrants est systématiquement du type « tout ce qui n'est pas explicitement autorisé est interdit ».
Les serveurs doivent être protégés spécifiquement vis-à-vis des postes de travail et des autres serveurs. On distinguera les serveurs accessibles uniquement à partir du réseau de la Communauté de Communes et ceux accessibles aussi de l'extérieur. Pour chaque réseau de serveurs, les filtres d'accès, tant sur les flux réseau entrants que sur les flux sortants, sont systématiquement du type « tout ce qui n'est pas explicitement autorisé est interdit ». Les serveurs potentiellement accessibles de l'extérieur feront l'objet d'une surveillance accrue (outils d'analyse des traces…). L'accès externe aux serveurs par les moyens nomades s'effectue au travers de connexions dédiées et chiffrées (VPN SSL).

7.7. Réseaux sans fils

L'administration des réseaux sans fil est placée exclusivement sous la responsabilité du DSI.
L'utilisation des réseaux sans fil doit l'être exclusivement dans le cas prévu à cet effet.
Seul le réseau sans fil « externe » peut être mis à disposition d'un utilisateur externe après exclusivement accord explicite du RSSI.

7.8. Maintien du niveau de sécurité

Le maintien du niveau de sécurité doit faire l'objet de dispositions techniques sous la responsabilité du RSSI. Ces dispositions doivent intégrer le maintien au cours du temps de l'état de sécurité des différents matériels : application des correctifs, mises à jour des anti-virus, pare-feu… Elles doivent préciser les conditions de surveillance du fonctionnement du système d'information de manière à s'assurer de son état de sécurité : analyse des journaux, vérification des vulnérabilités, suivi des avis de sécurité…

8. Mesure du niveau effectif de sécurité

8.1. Audits

Le niveau de sécurité des systèmes d'information et la conformité de mise en œuvre des recommandations sur le terrain peuvent donner lieu à des audits internes sous la responsabilité du RSSI ou des audits externes sous la supervision du RSSI.

8.2. Journalisation, tableaux de bord

Le système d'information doit comprendre des dispositifs de journalisation centralisée et protégée de l'utilisation des services.

L'objectif est de permettre de détecter des intrusions ou des utilisations frauduleuses, de tenter d'identifier les causes et les origines, d'éviter des contaminations d'autres sites par rebond et de remettre en place le système. Conformément à la législation française, ces informations peuvent faire l'objet d'une transmission aux autorités compétentes après avis du Président la Communauté de Communes (en tant qu'AQSSI).
La durée de conservation des fichiers de traces à des fins de preuve doit être conforme aux lois et règlements en vigueur. Il importe de définir, et de faire connaître aux utilisateurs, les règles d'exploitation des fichiers de traces (contenu, durée de conservation, utilisation) dans le respect du « principe de proportionnalité » et des contraintes législatives et réglementaires concernant notamment le traitement des informations à caractère personnel.

8.3. Les fichiers de traces

Les fichiers de traces seront systématiquement analysés afin de repérer d'éventuels problèmes et de produire des statistiques et tableaux de bord.

8.4. Mises en garde

L'utilisation de certains matériels ou logiciels peut s'avérer préjudiciable à la sécurité des systèmes d'information. Ces produits font l'objet de « mises en garde » de la part de la chaîne fonctionnelle SSI, visant soit des recommandations d'utilisation, soit une interdiction pure et simple.

8.5. SENSIBILISATION ET FORMATION

Dans la sécurité, les comportements et la vigilance des personnes sont toujours un facteur majeur du succès ou d'échec. C'est un élément majeur de prévention de la survenue d'incidents et de limitation de ses impacts en cas de survenance.

La Communauté de communes Sud Roussillon mène donc des actions de sensibilisation et de formation sous l'égide du RSSI.

8.6. Gestion d'incidents

Chaque acteur du système d'information, utilisateur ou administrateur, doit être sensibilisé à l'importance de signaler tout incident réel ou suspecté ; ceci inclus le vol de moyens informatiques ou de supports de données. Le signalement des incidents au RSSI et aux autorités hiérarchiques est systématique.
Lorsque l'incident peut mettre en cause la Communauté de Communes Sud Roussillon dans son fonctionnement, le RSSI doit être informé directement, voire parallèlement, le Directeur Général des Services selon la gravité de l'incident (données sensibles…). Lorsque l'incident peut mettre en péril la Communauté de Communes, le RSSI, après avis du Président (en tant qu'AQSSI), en informe les autorités compétentes (services de l'ANSSI).
Toute infraction susceptible d'implications juridiques fera l'objet d'un dépôt de plainte par la collectivité auprès des autorités compétentes et après avis du Président de la Communauté de Communes.
Les données relatives à la gestion des incidents sont intégrées dans un tableau de bord de la SSI.

8.7. Gestion de crise

Le Directeur du Système d'Information (DSI) prévoit le dispositif organisationnel propre aux crises de nature informatique, il intègre les risques liés à l'informatique ainsi que les risques ayant une incidence sur la Sécurité des Systèmes d'Information. Le RSSI doit être informé dès le déclenchement de toute crise ayant une incidence sur la Sécurité des Systèmes d'Information

8.8. Plan de continuité

Ce plan doit permettre, si la restauration complète en production est impossible, de maintenir en mode dégradé les activités critiques, puis de récupérer et de restaurer toutes les fonctionnalités du système d'information.

GLOSSAIRE

A

AGILE : méthode de gestion de projet qui prône une démarche collaborative, itérative et incrémentale. Elle est dite « agile », car elle permet de prendre en compte à la fois les besoins initiaux et ceux générés par les changements futurs
AMOA ou AMO : assistance à maîtrise d'ouvrage
ANSSI : Agence nationale de la sécurité des systèmes d'information
API : solution informatique qui permet à des applications de communiquer entre elles et de s'échanger mutuellement des services ou des données

B

BAN : Base adresse nationale, base de données ayant pour but de référencer l'intégralité des adresses du territoire français
Big Data : ressources d'informations dont les caractéristiques en termes de volume, de vélocité et de variété imposent l'utilisation de technologies et de méthodes analytiques particulières pour générer de la valeur
BIM : processus intelligent basé sur un modèle 3D qui offre aux professionnels de l'architecture, ingénierie et construction les informations et les outils nécessaires pour planifier, concevoir, construire et gérer plus efficacement des bâtiments et des infrastructures
Briques techniques : ensemble d'outils ayant des fonctions très précises (authentification par exemple), communiquant avec les autres afin de créer un ensemble cohérent répondant à une problématique métier, sécurité…
Byod ou Bring your own device : utilisation de matériel informatique personnel à des fins professionnelles moyennant en général l'ajout d'un logiciel de contrôle par l'entreprise

C

Chatbot : outil permettant à un utilisateur de demander des renseignements auprès d'un robot en s'exprimant en langage courant
Cloud : recouvre l'ensemble des solutions de stockage distant. En clair, vos données, au lieu d'être stockées sur vos disques durs ou mémoires, sont disponibles sur des serveurs distants et accessibles par internet
CNFPT ou Centre national de la fonction publique territoriale : établissement public paritaire déconcentré doté de trois missions principales : la formation, l'observation et l'organisation des concours des cadres d'emplois A+
Collaboratif : qui permet de travail ensemble (partage de documents …)
Connecteurs : lien entre différents outils permettant la transmission ou l'enrichissement d'informations
CPOM ou Contrat pluriannuel d'objectifs et de moyens : engagement pluriannuel sur des objectifs d'activité et des moyens d'action
CSIRT ou Computer Security Incident Response Team : centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous.
Cyber'Occ : portail de la cybersécurité en Occitanie, créé par le Conseil régional d'Occitanie et son agence de développement économique Ad'Occ. Il centralise un ensemble d'informations liées à la cybersécurité (métiers, aides, documentation, alertes…).

D

Data : données
Data analyst : il met en œuvre des outils informatiques, techniques et méthodes statistiques pour permettre d'organiser, synthétiser et traduire efficacement des données. Bac + 5 en informatique

Data scientist : il exploite, analyse et évalue la richesse, de données structurées ou non pour établir des scénarios permettant de comprendre et d'anticiper de futurs levier métiers ou opérationnels pour l'entreprise. Bac + 5 École d'ingénieur, commerce, statistiques
Datavisualisation : représentation graphique de données statistiques
Décisionnel : outils dont l'objectif est l'aide à la décision (indicateurs, tableaux de bord…)
Design de service : façon de concevoir un service centré sur l'utilisateur de manière qu'il soit utile et facilement utilisable
DEVOPS : pratique technique visant à l'unification du développement logiciel (dev) et de l'administration des infrastructures informatiques (ops), notamment l'administration système. En général, demande également un rapprochement des équipes opérationnelles et des développeurs pour une plus grande réactivité et une réponse aux besoins plus précise
DPO : Data protector officer, traduit en français par Délégué à la protection des données. Personne chargée, dans le cadre du RGPD, de veiller à la protection des données personnelles au sein des entreprises, collectivités…
DUA ou Durée d'utilité administrative : durée pendant laquelle les documents, données ou informations archivées doivent être conservés et gardés en état d'être consultés et utilisés, soit par ceux qui les ont produits, soit par des services d'archives
DSI : Direction des systèmes d'information
DOCK : dispositif informatique conçu pour accueillir, à la manière d'un socle, un appareil informatique portable en le branchant, lui offrant ainsi du courant électrique. Dans le cas d'un ordinateur portable, elle permet de l'utiliser de façon semblable à un ordinateur de bureau

E

EDR ou Endpoint detection and response :
catégorie d'outils et de solutions qui mettent l'accent sur la détection d'activités suspectes directement sur les hôtes du système d'information (ordinateurs, serveurs…). Combiné avec un moteur basé sur de l'intelligence artificielle, le logiciel EDR est très réactif dans la détection et l'arrêt de menaces
EMM ou Entreprise mobile management :
outil de gestion de flotte de téléphones portables
E-inclusion : concept de donner l'accès et la compréhension du numérique au plus grand nombre
Entrepôt (de données) : zone de stockage d'un maximum d'informations, qui pourront être consultées par différents logiciels afin de les exploiter au mieux
EPCI : Etablissement public de coopération Intercommunale
ETP : équivalent temps plein

F

Firewall : logiciel et/ou matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique

G

GED ou Gestion électronique des documents :
procédé informatisé visant à définir, concevoir, produire, organiser, diffuser et gérer des informations et des documents papier ou des documents électroniques au sein d'une organisation
Géomaticien : à la croisée de la géographie et de l'informatique, le géomaticien exploite les données pour modéliser le territoire. Il intervient dans tous les secteurs qui ont besoin d'analyse spatiale : urbanisme, environnement, transport, énergie, marketing…
GMP : logiciel de suivi des mouvements de personnel
GPEC : Gestion prévisionnelle des emplois et des compétences
Green IT : a pour objectif de réduire l'empreinte carbone générée par les systèmes d'information tout en permettant de réaliser des économies

I

IA : intelligence artificielle
IoT ou Internet of things : Internet des objets. Regroupe les objets et équipements connectés (à Internet) et les technologies qui s'y rapportent
IIoT ou Industrial internet of things : Internet industriel des objets ou IOT dans l'industrie
Interopérable : le fait d'avoir des outils capables de communiquer entre eux (ayant des interfaces par exemple)
Itrust : éditeur de solutions de cybersécurité

L

Label ExpertCyber : label destiné à valoriser les professionnels en sécurité numérique ayant démontré un niveau d'expertise technique et de transparence dans les domaines de l'assistance et de l'accompagnement de leurs clients. Le label ExpertCyber est issu d'une collaboration entre cybermalveillance.gouv.fr, ses membres et AFNOR Certification
Lean : appliqué aux systèmes d'information, le lean est l'élimination du superflu afin de rendre leur gestion plus flexible. Le Lean IT amène notamment l'utilisation d'une démarche structurée dans le recueil des besoins, l'amélioration continue…
LIDAR : méthode de télédétection et de télémétrie semblable au radar, mais qui émet des impulsions de lumière infrarouge au lieu d'ondes radio, puis en mesure le temps de retour après avoir été réfléchies sur des objets à proximité
Logiciel métier : outil dont l'objectif est de répondre aux besoins d'un métier particulier
Loi « numérique » : cf. loi Lemaire ci-dessous
Loi « Lemaire » : la loi pour une République numérique (abr. loi numérique) est une loi française initialement proposée par la secrétaire d'État au numérique Axelle Lemaire et promulguée le 7 octobre 2016. L'objectif est double : « donner une longueur d'avance à la France dans le domaine du numérique en favorisant une politique d'ouverture des données et des connaissances » et « adopter une approche progressiste du numérique, qui s'appuie sur les individus, pour renforcer leur pouvoir d'agir et leurs droits dans le monde numérique ». Pour ce faire, la loi s'organise autour de trois axes : la circulation des données et du savoir, la protection des individus dans la société du numérique et l'accès au numérique pour tous
Loi « NOTRe » : la loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République, fait partie de l'acte III de la décentralisation mis en œuvre sous la présidence de François Hollande et vise notamment à renforcer les compétences des Régions et des Établissements publics de coopération intercommunale

M

Mindmap : carte mentale, représentation graphique d'une arborescence d'idées
Monitoring : suivi et affichage de statistiques en direct (consommation électrique ou volume de données occupé par exemple)

O

Occitanie Data : association de préfiguration d'un pôle d'économie de la donnée (entreprises, institutions publiques, collectivités territoriales, acteurs académiques). Occitanie Data consiste à construire un cadre de confiance, éthique et souverain, destiné à permettre aux acteurs de partager et de croiser leurs données tout en respectant les intérêts des individus et des propriétaires des données
On Premise : installation en interne
Opendata : Ouverture de données, obligation règlementaire de diffuser les données non sensibles des collectivités à des fins de transparence et de possible réutilisation par toute personne morale ou physique

P

PCA ou Plan de continuité d'activité : plan regroupant un ensemble de mesures ayant pour objectif de poursuivre au mieux l'activité en cas de problème majeur. Pour cela, il présente de la sécurisation (redondance par exemple), des moyens de contournements ou une priorisation

PCRS ou Plan de corps de rue simplifié : représentation graphique permettant d'améliorer la précision du repérage des réseaux et fiabiliser l'échange d'informations entre les acteurs concernés (collectivités, exploitants de réseaux, maîtres d'ouvrages et entreprises de travaux)

Phishing ou Hameçonnage : technique frauduleuse utilisée pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité, consistant notamment à envoyer des messages en se faisant notamment passer pour une organisation légitime, mais contenant un lien vers un site malveillant

POC ou Proof of concept : prototype d'expérimentation d'un logiciel sur un périmètre restreint dont l'objectif est de montrer sa bonne adéquation avec les besoins. L'évaluation du POC permet d'éclairer la décision de généraliser ou non la solution

PRA ou Plan de reprise d'activité : ensemble de mesures permettant de reprendre l'activité au plus vite et au mieux suite à un incident majeur ayant occasionné une interruption (ex : mise en place de sauvegardes sécurisées)

Prédictif : outil d'aide à la décision simulant une situation future en fonction de données, tendances ou de paramètres (ex : accroissement de la population sur un territoire ou estimation des recettes en cas de facturation des déchets au poids)

Programme TNT : en 2021, le programme Transformation numérique des territoires a pris le relais du programme de Développement concerté de l'administration numérique territoriale (DCANT 2018-2020). Véritable feuille de route de la transformation numérique des territoires, ce programme a été entièrement co-écrit par les associations d'élus et les représentants des services de l'État autour d'une ambition partagée : construire ensemble des services publics numériques fluides et performants

Q

QQOQCCP : le QQOQCCP (Quoi, Qui, Où, Quand, Comment, Combien, Pourquoi), appelé aussi méthode du questionnement est un outil d'aide à la résolution de problèmes comportant une liste quasi exhaustive d'informations sur la situation

QuickCapture : module du SIG permettant la collecte d'observations sur le terrain

R

Ransomwares : logiciels malveillant ayant pour objectif de demander une rançon à leurs victimes

RGPD ou Règlement général de protection des Données : règlement européen de 2016 (entré en vigueur en 2018), qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne

RGS ou Référentiel général de sécurité :
cadre réglementaire qui contraint les autorités administratives à garantir la sécurité de leurs systèmes d'information en charge de la mise en œuvre de téléservices et des échanges électroniques entre l'administration et les usagers.

RSSI ou Responsable de la sécurité des systèmes d'information : personne qui a la charge de la rédaction de la PSSI, de sa mise en application et de son respect

S

SaaS ou Software as a service : modèle de distribution de logiciel au sein duquel un fournisseur tiers héberge les applications et les rend disponibles pour ses clients par l'intermédiaire d'internet

SI : Système(s) d'information

SIG : Système d'information géographique
Smart-city : « ville intelligente ». Il s'agit d'améliorer la qualité de vie des citadins en rendant la ville plus adaptative et efficace, à l'aide de nouvelles technologies qui s'appuient sur un écosystème d'objets et de services. Le périmètre couvrant ce nouveau mode de gestion des villes inclut notamment : infrastructures publiques (bâtiments, mobiliers urbains, domotique, etc.), réseaux (eau, électricité, gaz, télécoms), transports (transports publics, routes et voitures intelligentes, covoiturage, mobilités dites douces - à vélo, à pied, etc.), les e-services et e-administrations
Smart mobility ou mobilité intelligente : désigne les services de transports qui intègrent les solutions des technologies de l'information et de la communication pour améliorer la qualité du service rendu à l'usager
SO ou Système ouvert : système informatique interopérable entre différents fournisseurs et normes, permettant une modularité entre les matériel et les logiciels
Softphone : logiciel utilisé pour faire de la téléphonie par Internet depuis un ordinateur plutôt qu'un téléphone
Spam : courriel (mail) indésirable (ou pourriel), communication électronique non sollicitée. Il s'agit en général d'envois en grande quantité de courriels effectués à des fins publicitaires
SWOT ou Strengths (forces)**, Weaknesses** (faiblesses)**, Opportunities** (opportunités)**, Threats** (menaces) **:** technique d'analyse visant à préciser les objectifs d'un projet et à identifier les facteurs internes et externes favorables et défavorables à la réalisation de ces objectifs

T

Téléservices : services en ligne permettant à l'utilisateur de réaliser diverses opérations (paiement, inscription à la cantine, etc.)
Ticketing (outil de) : outil de suivi de demandes permettant à un utilisateur d'adresser une demande qui sera dirigée vers les bonnes personnes, de suivre son traitement et d'afficher des statistiques liées
To : téraoctet