POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION (PSSI)

PSSI-Générale

Université de Reims Champagne-Ardenne

Référence : PSSI-G URCA V1

Responsable du projet :

RSSI EMAIL : rssi@univ-reims.fr

Version :

Date : 22/11/2023	1.0	Création du document

SOMMAIRE

1. PREAMBULE

1.1. OBJECTIF DU DOCUMENT

Ce document constitue la Politique de Sécurité des Systèmes d'Information Générale (PSSI-G) de l'Université de Reims Champagne-Ardenne (URCA). 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 de l'URCA.

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-G fait partie intégrante du référentiel cybersécurité de l'URCA.

1.2. PERIMETRE D'APPLICATION

La PSSI-G s'applique de façon transverse à toutes les directions et tous les systèmes d'information de l'URCA.

1.3. ÉVOLUTION

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

- Des évolutions de la réglementation et des engagements contractuels avec les partenaires ;
- Des évolutions des exigences issues de l'autorité de tutelle (le ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation) ;
- 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-G est réalisée, au minimum une fois tous les 3 ans, par le RSSI puis proposée à la Direction Générale de l'établissement pour validation.

1.4. DIFFUSION

La politique de Sécurité Générale est un document interne de l'URCA. 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, laboratoires, écoles ou universités partenaires, auditeurs externes, prestataires, etc.).

1.5. ENTREE EN VIGUEUR

La politique de sécurité est validée par la direction générale. Elle entre en vigueur dès diffusion à l'ensemble des agents publics.

Toutes les directions de l'URCA 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'URCA.

2. ENJEUX ET OBJECTIFS DE LA SECURITE DE L'URCA

2.1. LES ENJEUX EN MATIERE DE SECURITE

2.1.1. Sécuriser les SI : une nécessité

L'évolution sans cesse croissante des technologies et des systèmes de traitement de l'information et celle, concomitante, des menaces informatiques et des cyberattaques, justifie l'attention que l'URCA 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'URCA 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 l'URCA et pour ses partenaires (industriels, ministères, écoles, laboratoires de recherche, etc.) :

- Perte du patrimoine informationnel, par la destruction massive de données de recherche, de formation, de scolarité, 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 la création des dossiers de scolarisation des étudiants voire l'indisponibilité complète des processus de formation et de scolarité (plus de diplomation possible) ;
- Divulgation de données sensibles valorisables (propriété industrielle, innovation scientifique : fuite du secret industriel des partenaires (informations sensibles reçues dans le cadre de partenariat de recherche), fuite de données de santé traitées par la recherche, fuite des données personnelles des étudiants ou des agents publics ;
- Attaque d'un partenaire au travers de l'établissement, de ses SI ou de son personnel ;
- Atteinte à l'intégrité sur les résultats de scolarité pour un ou plusieurs étudiants ;
- Atteinte à l'image en qu'université formant aux Réseaux et Télécommunications, avec une composante cybersécurité ;

- 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 l'URCA, et ce à la hauteur des enjeux qu'ils représentent et en cohérence avec les risques et les menaces qui pèsent sur eux.

2.1.2. Sécuriser les SI : une obligation

Sécuriser les systèmes d'information de l'URCA est également une obligation pour s'aligner avec les évolutions du cadre légal, réglementaire et contractuel (hors droit européen et français).

Le RSSI peut, lorsqu'il le juge nécessaire, s'appuyer sur la Direction des Affaires Juridiques pour accomplir sa mission.

2.1.3. Sécuriser les SI : une opportunité

La sécurité des systèmes d'information est également appréhendée par l'URCA comme une opportunité lui permettant, d'une part, d'adopter sereinement les avancées technologiques, et d'autre part de renforcer la relation de confiance avec ses partenaires (industriels, universitaires, laboratoires, etc.) et le ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation.

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 RSSI de l'URCA veille à la prise en compte de la présente PSSI-G 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.

2.2. LES OBJECTIFS STRATEGIQUES EN MATIERE DE SECURITE

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

- Permettre aux différentes directions 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 de l'URCA ou de nuire à son image ;
- Respecter les exigences réglementaires et législatives auxquelles sont assujetties les différentes directions de l'URCA ;
- Ne pas compromettre les données des partenaires, les données de santé fournies ou l'écosystème qui gravite autour de l'URCA ;
- Protéger son personnel, ses actifs, ses partenaires et ses étudiants contre toute forme de menace, accidentelle ou intentionnelle ;

- Contribuer à la performance globale de l'URCA et préserver sa réputation et son image en tant qu'université formant notamment à la cybersécurité ;
- 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 des directions, du ministère et des partenaires.

Afin de satisfaire ses objectifs stratégiques, l'URCA 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 de l'URCA.

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 l'URCA, en lien direct ou indirect avec les systèmes d'information.

3. LE REFERENTIEL CYBERSECURITE DE L'URCA

Le référentiel cybersécurité de l'URCA est composé de trois niveaux :

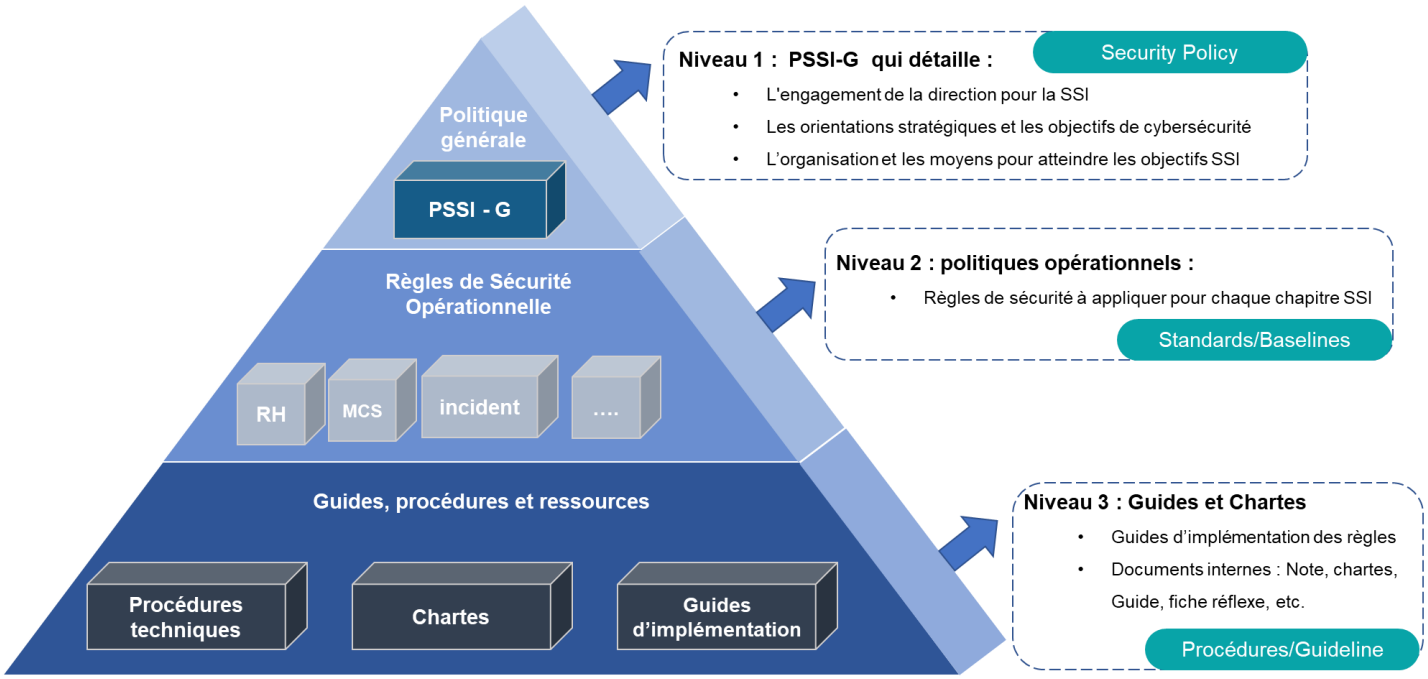

Figure 1 : Eléments constitutifs du référentiel cybersécurité

- **Niveau 1** : Définit la Politique de Sécurité des Systèmes d'information Générale applicable de façon transverse à l'ensemble des systèmes d'information de l'URCA (le présent document) ;
- **Niveau 2** : Définit les déclinaisons opérationnelles des objectifs stratégiques de l'URCA. Cette politique opérationnelle (PSSI-Opérationnelle) formalise les règles de sécurité applicables pour l'ensemble des systèmes d'information de l'URCA afin d'atteindre les objectifs stratégiques ;
- **Niveau 3** : Définit les guides et les méthodes proposées pour un déploiement correct et cohérent des règles de sécurité.

Ces politiques et procédures de sécurité sont issues d'une analyse des risques cybersécurité réalisée et régulièrement mise à jour par le Responsable de Sécurité des Systèmes d'Information.

Elles constituent le cadre de référence conçu pour atteindre les objectifs en matière de sécurité des SI. Elles traduisent la feuille de route que l'URCA entend suivre et faire prendre en compte par toutes les parties prenantes afin d'atteindre la cible définie en matière de sécurité.

4. ORGANISATION ET MANAGEMENT DE LA SECURITE DES SI

4.1. ROLES EN MATIERE DE SECURITE

4.1.1. 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'URCA. Il porte ainsi la responsabilité de la gestion des risques cybersécurité et des travaux de mise en conformité réglementaire.

Cette responsabilité lui incombe 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 l'URCA. À ce titre, le Président réalise, sur la base des travaux effectués par le RSSI, un arbitrage sur l'acceptation des risques et sur la conformité réglementaire et contractuelle, et décide les budgets et les moyens mis à disposition pour le programme sécurité.

La direction générale exprime son leadership et son engagement en faveur du programme sécurité de l'URCA en :

- S'assurant que la politique et les objectifs sécurité sont établies et qu'ils sont compatibles avec l'orientation stratégique de l'URCA ;
- 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 que la politique de sécurité atteint les résultats et objectifs escomptés ;
- Orientant et soutenant les membres de l'URCA pour qu'elles contribuent à l'efficacité du plan d'action et qu'elles respectent les règles de la politique de sécurité ;
- Promouvant l'amélioration continue ;
- Aidant les autres directeurs et responsables concernés à démontrer leur leadership et leur engagement dès lors que cela s'applique à leurs domaines de responsabilité.

4.1.2. Responsable de la Sécurité des Systèmes d'Information

Le RSSI a la responsabilité, au sein de la Direction du Numérique (DN), de conseiller et d'accompagner la Direction Générale dans la définition d'un programme sécurité, conformément aux risques identifiés, aux obligations légales et contractuelles et aux objectifs stratégiques, d'en contrôler le respect et d'exercer un reporting pour assurer le suivi au plus haut niveau du programme.

Cette responsabilité se décline en mission d'expertise, de pilotage et de support :

- Concevoir la gouvernance et le cadre de référence de la sécurité (Politiques et Procédures de sécurité) et veiller à son déploiement ainsi qu'à sa bonne application au sein de toutes les directions de l'URCA ;
- Identifier et fournir la visibilité sur les risques / impacts majeurs ainsi que sur l'efficacité des capacités mises en œuvre pour les traiter ;
- Constituer un pôle d'expertise à même d'assister et de conseiller les directions sur les nouveaux usages et risques sécurité sur leur périmètre d'activité et projet, pour leur permettre de répondre aux enjeux métiers en réalisant des analyses de risques, en proposant des mesures de sécurité pour traiter les risques identifiés et en contrôlant la bonne application des mesures de sécurité ;
- S'assurer de la correcte mise en œuvre des règles de la politique de sécurité, et de la prise en compte des aspects sécurité dans les actions et les projets menés au sein de chaque direction de l'URCA ;
- Contribuer au suivi et à la gestion des incidents de sécurité de l'URCA ;

- Gérer les évolutions des Politiques de Sécurité des Systèmes d'Information et de l'analyse des risques ;
- Participer à la sensibilisation et la formation des agents publics de l'URCA à la sécurité des SI ;
- Assurer le reporting vis-à-vis de la direction générale.

4.1.1. Délégué à la protection des données (DPO)

La DPO a 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 a 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 DN 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.

4.1.2. Responsables

Chaque directeur de recherche, directeur d'unité et chaque responsable des services, d'UFR, instituts et écoles a la responsabilité, au sein de son équipe, de sensibiliser les agents publics sur la nécessité de respecter les règles de la politique de sécurité des systèmes d'information.

Cette responsabilité se décline en mission d'appui et de support du RSSI :

- Reconnaître et soutenir le RSSI : intervenir pour légitimer le rôle du RSSI vis-à-vis de la direction ou du service ;
- Sensibiliser les agents publics pour l'application du référentiel de sécurité (PSSI, procédure, charte, etc.) ;
- Adopter un comportement ayant valeur d'exemple en respectant les mesures de sécurité de la PSSI ;
- Exercer une surveillance permanente et informe le RSSI de toute situation anormale ou présomption d'incident ou de comportement à risque ;
- Participer aux arbitrages réalisés par le RSSI en cas de contrainte organisationnelle ou technique au sein d'une équipe.

Les directeurs sont également responsables des risques au niveau de leur périmètre. Ils valident le niveau de risques SI acceptable de chaque activité dont ils ont la charge, valident la mise en œuvre et font appliquer les mesures de sécurité des SI adéquates, en allouant les ressources en cohérence avec les objectifs et la PSSI.

Pour cela, les directeurs s'appuient sur les travaux réalisés par le RSSI et le Délégué à la protection des données (DPO) pour obtenir les informations nécessaires afin de décider du caractère acceptable ou non des risques.

4.1.3. Utilisateurs internes

Chaque utilisateur interne du système (collaborateurs, chercheurs, enseignants, étudiants, stagiaires, prestataires, vacataires, 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 tout incident ou anomalie constatée.

4.1.4. Direction du Numérique (DN)

Les équipes de la DN 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 les directions et les départements métiers.

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 DN respectent les procédures internes, communes à toute la DN, afin de garantir :

- Une cohérence des activités au sein de la DN ;
- Un niveau de sécurité homogène entre les différents composants du SI, quel que soit l'équipe en charge de la mise en place et de l'exploitation en sein de la DN ;
- Le respect des mesures de sécurité de la PSSI.

Par défaut, la DN est le garant de l'application des mesures de sécurité pour tous les composants du système d'information de l'URCA inscrit dans son périmètre de contrôle. Lorsqu'un périmètre est géré par une autre direction pour des raisons organisationnelles ou techniques, un correspondant sécurité est nommé formellement pour appliquer les mesures de sécurité. Ce transfert se fait sous forme d'une attestation signée par les acteurs concernés.

Cette attestation précise :

- Le périmètre concerné : Description détaillée des composants du système concerné ;
- Les raisons justifiant le transfert de responsabilité ;
- Le responsable qui sera en charge du respect des règles de la PSSI : Le correspondant sécurité ;
- Les modalités de contrôle par le RSSI ;
- Les signatures et leurs rôles/responsabilités : au minimum, le RSSI/DN, le responsable de la direction concernée, et le correspondant sécurité désigné.

4.1.5. Correspondant sécurité des SI de recherche

Pour les besoins de la recherche, les équipes de l'URCA sont souvent amenées à déployer des systèmes dédiés à la recherche et qui ne sont pas contrôlés par les processus et procédures internes de la DN.

Pour assurer la sécurité des SI de recherche, conformément aux objectifs stratégiques de l'URCA, les composants du système d'information dédié à la recherche, qui ne sont pas dans le périmètre de la DN, sont mis sous la responsabilité d'un correspondant sécurité nommé pour chaque périmètre.

Au moment de la mise en place d'un système dédié à la recherche, une décision est prise par le RSSI, pour nommer un correspondant sécurité du système créé. Cette décision est prise conjointement avec :

- Le responsable du département concerné ;
- L'équipe de recherche concernée et son représentant ;
- L'équipe DN concernée.

Chaque composant non pris en charge par la DN dispose ainsi d'un correspondant sécurité qui prend en charge la responsabilité de sécuriser le composant conformément aux objectifs stratégiques de l'URCA. Cette information est documentée par le RSSI et maintenue à jour.

Les responsabilités du correspondant sécurité sont les suivantes :

- Décliner les règles de la politique de sécurité de l'URCA au niveau du composant recherche en prenant en compte les spécificités des procédés de recherches et les contraintes techniques et opérationnelles ;
- Coordonner le déploiement des mesures de sécurité au niveau du composant du SI de recherche ;
- Prendre en charge les mesures de sécurité opérationnelles (Durcissement, Mise à jour de sécurité, analyser des alertes, gérer les incidents, contrôler les droits d'accès, etc.)
- Assurer le relais avec la fonction centrale de cybersécurité portée par le RSSI (Reporting, capitaliser sur les solutions éprouvées, partager les retours d'expérience, etc.)

4.2. LE PILOTAGE DE LA SECURITE

4.2.1. Comité stratégique de la sécurité des SI

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

- Le suivi et l'amélioration continue de la sécurité au niveau de l'URCA ;
- Le suivi des règles de la politique de sécurité ;
- Le suivi des travaux de mise en conformité réglementaire et contractuelle ;
- De maintenir à jour la Direction Générale du niveau de risque cyber qui pèse sur l'URCA ;

- La mise à disposition les 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.).

4.2.2. Comité de Pilotage de la sécurité des SI

Le comité de pilotage de la sécurité des systèmes d'information se réunit au minimum tous les deux mois. Ce comité réunit le RSSI, le DN et les éventuels acteurs de l'URCA concernés par les thématiques abordées. Les sessions de ce comité de pilotage sont l'occasion de :

- Suivre l'avancement et l'exécution des plans d'action de la sécurité des systèmes d'information ;
- Valider les mesures de sécurité proposées pour la gestion des risques ;
- Obtenir les arbitrages et orientations dans les choix concernant la sécurité des systèmes de l'URCA ;
- Assurer le suivi des indicateurs sécurité ;
- Discuter des contrôles et audits relatifs à la sécurité des systèmes d'information.

4.2.3. 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 sont présentés au comité stratégique 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.

4.3. RELATIONS AVEC LES AUTORITES

Des relations appropriées avec les autorités compétentes sont entretenues par le RSSI et le DPO. La procédure de gestion d'incident définit :

- Quand et comment contacter les autorités compétentes
- Comment signaler dans les meilleurs délais les incidents liés à la sécurité de l'information (tels que par exemple une tentative d'intrusion ou une fuite des données à caractère personnel)

Les utilisateurs ne sont pas autorisés à contacter par eux-mêmes les autorités, sauf à y être autorisé du fait de leur fonction, à condition d'informer immédiatement leur responsable qui feront remonter l'information aux RSSI et DPO.

5. PRINCIPES & PROCESSUS DE SECURITE

L'URCA 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.

5.1. GESTION DES RISQUES ET CONFORMITE

L'URCA 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'URCA, 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 de l'URCA. Elle sert à mettre à jour tous les 3 ans la PSSI opérationnelle ;
- **Risques propres à un système :** Si nécessaire, chaque sous-système d'information de l'URCA peut fait 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.

L'URCA élabore et maintient à jour une étude de conformité avec les lois, réglementations et engagements contractuels. Les non-conformités sont identifiées, partagées avec la Direction Générale et associées à des plans d'action SSI.

Pour le cas particulier du Règlement Général sur la Protection des Données (**RGPD**), le RSSI maintient à jour l'étude de conformité conjointement avec la Déléguée à la Protection des Données (DPO) de l'URCA.

5.2. SELECTION ET APPLICATION DES MESURES DE SECURITE

Les mécanismes de sécurité mis en place au sein de l'URCA sont issus :

- Du processus de gestion des risques ;
- Du processus de conformité avec les lois, réglementations et engagement contractuel ;
- Des politiques de sécurité internes.

Ils sont sélectionnés par le RSSI conformément aux objectifs de sécurité fixés, en prenant en compte le contexte de l'URCA.

Les mécanismes de sécurité retenus, qu'ils soient de nature technique ou organisationnelle, sont alors applicables par toutes les parties prenantes des systèmes d'information de l'URCA.

La mise en place des mesures de sécurité techniques et organisationnelles est suivie par le RSSI au moyen de plan d'action SSI, régulièrement présentées à la Direction Générale.

5.3. GESTION DES INCIDENTS DE SECURITE

Les incidents de sécurité sont identifiés, détectés, traités, évalués et leurs causes recherchées. Cette gestion est indispensable à l'amélioration continue de la sécurité ; elle est assurée par le RSSI, avec le concours des acteurs de la DN et des parties prenantes des directions concernées.

5.4. AUDIT ET AMELIORATION CONTINUE

L'activité d'audit est primordiale pour vérifier la bonne mise en œuvre des démarches et mesures de sécurité décrites dans les différentes politiques de sécurité des systèmes d'information de l'URCA.

Des audits de sécurité sont réalisés annuellement, particulièrement sur les activités essentielles de l'URCA.

Les audits de sécurité sont préparés, pilotés et analysés par le RSSI, en concertation avec les acteurs du système d'information concerné par le périmètre de chaque audit.

Les plans d'action d'audit sont proposés par l'auditeur en concertation avec le RSSI et validés par la Direction Générale. Le RSSI assure le suivi de la mise en place des plans d'action issus de chaque audit.

5.5. 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.

L'URCA mène donc des actions de sensibilisation et de formation sous l'égide du RSSI.

5.6. ACCES PAR DES TIERS ET SOUS-TRAITANCE

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

Les accès sont formellement approuvés par le collaborateur de l'URCA auquel ils sont rattachés et le RSSI, et fait l'objet d'un encadrement contractuel via la signature du contrat, où doit être systématiquement annexé les clauses liées à la sécurité des systèmes d'informations.

Les intervenants externes travaillent sous la responsabilité d'un collaborateur de l'URCA.

Les tiers et sous-traitants doivent en conséquence respecter ces clauses sous peine d'une pénalité ou d'une rupture de prestation, selon les conditions énoncées par l'URCA dans le contrat en question.