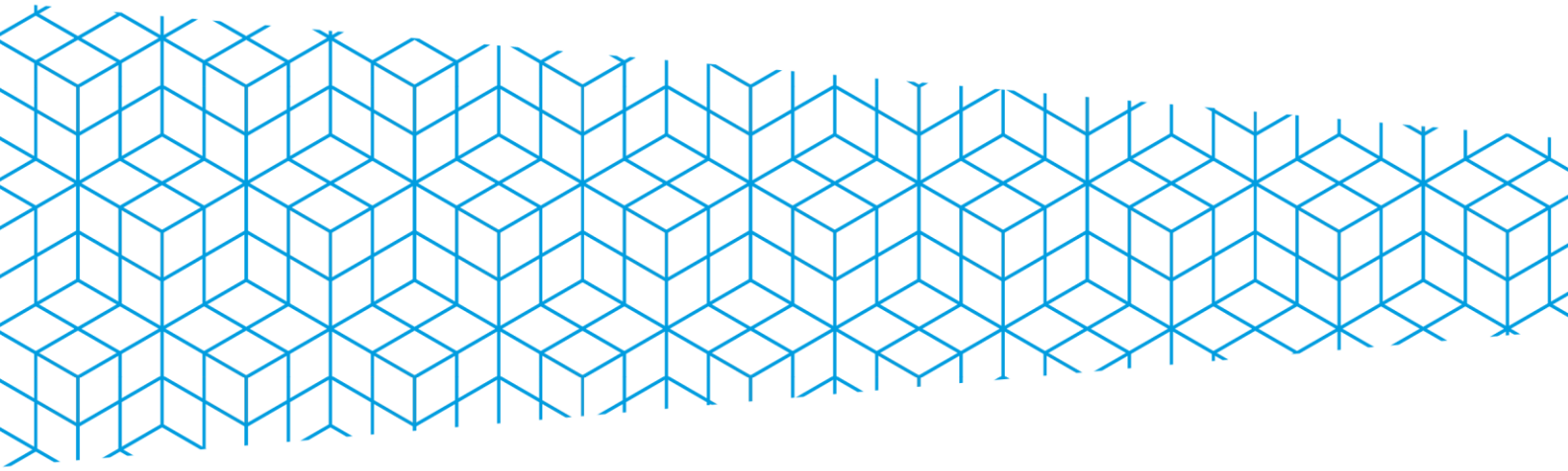
POLITIQUE GENERALE DE SECURITE DES SYSTEMES D'INFORMATION

Version : 1.0
Date de publication : 30/05/2023



université de BORDEAUX

Rédaction
Soben CHHEM (RSSI) Jean-Marc COUVEIGNES (Chargé de mission sécurité) **Principaux contributeurs :** Karim BELEBAS (VP Numérique) Frédéric POMIES (Directeur des Systèmes d'Information)

Table des matières

Lettre d'engagement de la Présidence **3**

I. Définition **5**

II. Introduction **6**

II.1 Objectif 6

II.2 Fondements juridiques 6

II.3 Périmètre d'application 6

II.4 Corpus documentaire SSI 7

III. Organisation et gouvernance de la SSI **8**

III.1 Rôles et responsabilités 8

III.1.1 L'AQSSI 8

III.1.2 Le VP Numérique 9

III.1.3 Le Chargé de mission SSI 9

III.1.4 Le RSSI 9

III.1.5 Le DSI 10

III.1.6 Le Fonctionnaire Sécurité et Défense (FSD) 10

III.1.7 Le correspondant SSI 10

III.2 Instances de gouvernance de la sécurité 11

III.2.1 Le Comité stratégique de la sécurité des SI 11

III.2.2 Le Comité de pilotage de la sécurité des SI 12

III.2.3 Le Comité de suivi de la sécurité des SI 12

IV. Principes de mise en œuvre **13**

IV.1 Garantir la sécurité des SI 13

IV.2 Identifier les risques et définir les mesures prioritaires 13

IV.3 Intégrer la sécurité dans les projets 14

IV.4 Gérer les incidents SSI 15

IV.5 Contrôler et assurer la conformité 15

IV.5.1 Cadre réglementaire et conformité 15

IV.5.2 Audits internes 16

IV.5.3 Réévaluer la PGSSI 17

Lettre d'engagement de la Présidence

Par cette politique générale de sécurité des systèmes d'information (**PGSSI**), la Présidence de l'université de Bordeaux, consciente de l'accroissement et de la diversification des risques, et de l'importance cruciale de la cybersécurité pour la continuité et la qualité de ses activités, souhaite réaffirmer son engagement total en la matière.

L'université de Bordeaux est une grande institution française reconnue en Aquitaine, sur le territoire national et dans le monde, pour l'excellence de ses formations, la qualité de sa recherche, l'intensité et la diversité de son activité d'innovation et de diffusion.

Afin de mieux répondre aux défis scientifiques, aux attentes sociétales et aux urgences environnementales, l'université de Bordeaux s'affirme comme **université étendue**, connectée, ancrée dans ses territoires, ouverte à la société et à la diversité, innovante et intensive en recherche.

Pour réussir cette transformation, l'université de Bordeaux entretient et développe de **nombreux partenariats** scientifiques, institutionnels, territoriaux, culturels.

Vecteur de connaissances, de progrès social et sociétal, d'ouverture, de performance et de rationalisation, la **transition numérique** est au cœur du projet de l'Université. Elle est un instrument majeur de l'innovation pédagogique, de la recherche scientifique, de la qualité de vie sur le campus, de l'efficacité administrative et énergétique, de l'information et de la documentation scientifiques, de la visibilité et de l'attractivité de l'Université.

Le succès de cette transition numérique conditionne donc la réussite du projet de l'Université.

Parce que la **confiance** dans les systèmes d'information est indispensable à la transition numérique, la **cybersécurité** est un **enjeu majeur** de cette transition.

L'Université doit en effet garantir la résilience et l'interopérabilité de ses systèmes d'information. Elle doit protéger son patrimoine informationnel et les utilisateurs de ses systèmes d'information. Elle doit se conformer aux exigences légales et règlementaires et respecter ses engagements contractuels en matière de sécurité.

Pour y parvenir l'Université informe et mobilise **l'ensemble de la communauté académique** (personnels, usagers, partenaires) sur les enjeux, les règles et les bonnes pratiques de la cybersécurité, la prévention et la gestion des risques.

Elle met en place une organisation et une gouvernance de la sécurité des systèmes d'information qui sont décrites dans la politique générale de sécurité des systèmes d'information.

Cette politique générale de sécurité des systèmes d'information de l'université de Bordeaux fournit **un cadre de référence** et de cohérence à la sécurité des systèmes d'information. Elle définit les principes généraux de sécurité à respecter, ainsi que **l'organisation et les responsabilités en matière de sécurité des SI**. Comme l'ensemble des politiques et directives de sécurité, elle s'applique à toutes les structures de l'Université et à tous les utilisateurs de ses systèmes d'information.

Sous la coordination du Responsable de la sécurité des systèmes d'information, plusieurs axes majeurs sont à prendre en compte :

- Renforcer la confiance numérique pour améliorer l'attractivité de l'Université
- Faire évoluer le modèle de gouvernance et de pilotage de la sécurité intégrant les partenaires et les tiers
- Être un acteur de la conformité et assurer la protection de l'information
- Assurer un niveau de résilience élevé pour l'ensemble des activités

L'engagement de l'université de Bordeaux pour la cybersécurité s'inscrit dans une démarche de qualité du service public, d'excellence et de rayonnement scientifique, de progrès sociétal et environnemental, d'efficacité, de conformité règlementaire.

Cet engagement est celui de toute la communauté universitaire.

Le Président
Le 06/01/22

I. Définition

Analyse de risques	Processus visant à identifier les risques, déterminer leurs impacts et leur probabilité d'occurrence et définir les mesures de sécurité nécessaires
Audit	Opération visant à analyser les actions effectuées sur des données ou des biens ou à mesurer l'écart par rapport à un référentiel (par exemple la PSSI-E) ou par rapport à l'état de l'art.
Autorité Qualifiée pour la sécurité des systèmes d'Information (**AQSSI)**	Autorité juridiquement responsable de la sécurité des systèmes d'information de l'université de Bordeaux. Sa responsabilité ne peut être déléguée
Partie prenante	Personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité
Plan d'assurance sécurité (**PAS)**	Ensemble des dispositions que le prestataire prendra pour garantir le respect des exigences de sécurité du bénéficiaire.
Protection du potentiel scientifique et technique de la nation (**PPST)**	Dispositif protection contre l'espionnage technologique visant à protéger, au sein des établissements publics et privés, les savoirs et savoir-faire stratégiques ainsi que les technologies sensibles qu'ils détiennent.
Politique de sécurité du système d'information (**PSSI)**	Ensemble de règles et d'exigences permettant d'assurer un niveau de sécurité conforme aux besoins de l'Université et permettant d'assurer une conformité règlementaire
Sécurité des systèmes d'information (**SSI)**	Ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire à la protection des systèmes d'information contre les accidents (pannes, pertes, événements etc.), les erreurs (d'utilisation, de conception) et les actes malveillants (piratage, vol, captation d'information, ingénierie sociale, etc.).
Système d'information (**SI)**	Ensemble d'applications, services, actifs informationnels ou autres composants permettant de gérer l'information.

II. Introduction

II.1 Objectif

La Politique Générale de Sécurité du Système d'Information (**PGSSI**), a pour objectif de fournir un cadre de référence et de cohérence en matière de sécurité des systèmes d'information de l'université de Bordeaux. C'est un document fondateur qui s'inscrit dans un ensemble plus large de documents décrivant les exigences et règles de sécurité attendues afin d'assurer la protection des SI et la conformité règlementaire sur l'ensemble de ses activités, de ses projets vis-à-vis de ses partenaires, ses campus distants et ses annexes.

Elle définit les principes généraux de sécurité, le périmètre ainsi que l'organisation et les responsabilités en matière de sécurité des SI afin de :

- Renforcer la confiance numérique pour améliorer l'attractivité de l'Université
- Faire évoluer le modèle de gouvernance et de pilotage de la sécurité intégrant les partenaires et les tiers
- Être un acteur de la conformité et assurer la protection de l'information
- Assurer un niveau de résilience élevé pour l'ensemble des activités

II.2 Fondements juridiques

La PGSSI s'appuie sur les règlements et les directives ministérielles suivantes :

- La Politique de Sécurité des Systèmes d'Information de l'État (PSSI-E)
- Le décret n°2022-513 du 8 avril 2022 relatif à la sécurité du système d'information et de communication de l'État et de ses établissements publics
- L'instruction générale interministérielle n°1337/SGDSN/ANSSI
- Le référentiel général de sécurité (RGS)
- Le règlement général sur la protection des données (RGPD)
- La réglementation sur l'hébergement des données de santé (HDS)
- Le code de la défense
- Le code de l'éducation, notamment l'Article L712-2

La PGSSI s'appuie également sur les recommandations de l'agence nationale de la sécurité des systèmes d'information (ANSSI).

II.3 Périmètre d'application

La PGSSI s'applique à toutes les structures de l'université de Bordeaux, à tous les utilisateurs et les constituants de ses systèmes d'information (les données, les processus, les composants techniques matériels et logiciels, les infrastructures, etc)

Par structures de l'Université on entend les composantes de l'Université mentionnées à l'Annexe 3 des statuts de l'Université, notamment les collèges, les composantes de formation,

l'IUT, l'INSPE, l'ISVV, le collège des écoles doctorales, les départements de recherche, les unités et structures de recherche, l'OASU, … ainsi que les pôles, directions et services.

Par utilisateur on entend toute personne accédant aux moyens informatiques de l'Université, notamment et non exclusivement les personnels titulaires ou contractuels de l'Université, les étudiants, les personnels des partenaires, les bénéficiaires ou prestataires de l'Université, les visiteurs, les invités, les intervenants extérieurs, etc.

Les termes université de Bordeaux et Université seront employés indifféremment.

La direction de chacune des structures administratives, composantes de formation, laboratoires de recherche et plateformes scientifiques interagissant avec le SI de l'université de Bordeaux est responsable de l'application de la PGSSI et des politiques de sécurité sur l'ensemble de son périmètre d'activité.

D'autre part, les utilisateurs des systèmes d'information de l'Université doivent respecter la charte informatique.

Il est entendu que l'application de la PGSSI se fait dans le respect du décret n°82-447 du 28 mai 1982 relatif à l'exercice du droit syndical dans la fonction publique et de la charte de l'élu en vigueur au sein de l'établissement et de tout document qui viendrait à s'y substituer.

La PGSSI est diffusable et peut être communiquée à toute entité justifiant le besoin d'en connaître.

II.4 Corpus documentaire SSI

La politique de sécurité du système d'information de l'Université fait partie d'un référentiel documentaire à quatre niveaux :

- Le présent document, la Politique Générale, en constitue le premier niveau. Il décrit le cadre de référence en matière de sécurité du SI et fixe les enjeux et les principes de gouvernance.
- Un standard de sécurité (socle commun d'exigences de sécurité attendues) et des politiques thématiques (un ensemble de documents qui définit plus précisément les processus et règles de sécurité à mettre en œuvre par thème)
    - Politique de gestion des vulnérabilités
    - Politique de gestion des risques
    - Politique d'autorisation des exceptions
    - etc
- Des directives, à savoir les conditions, les lignes de conduite et les règles à adopter pour utiliser et gérer les services et actifs des SI de l'Université
- Des déclinaisons techniques. Il s'agit de guides, des bonnes pratiques, des procédures et des FAQ qui viennent compléter les politiques thématiques, dans des environnements techniques et organisationnels spécifiques.

La politique générale de sécurité et les politiques de sécurité thématiques de l'université de Bordeaux précisent les lignes directrices et les principes de sécurité à mettre en œuvre.

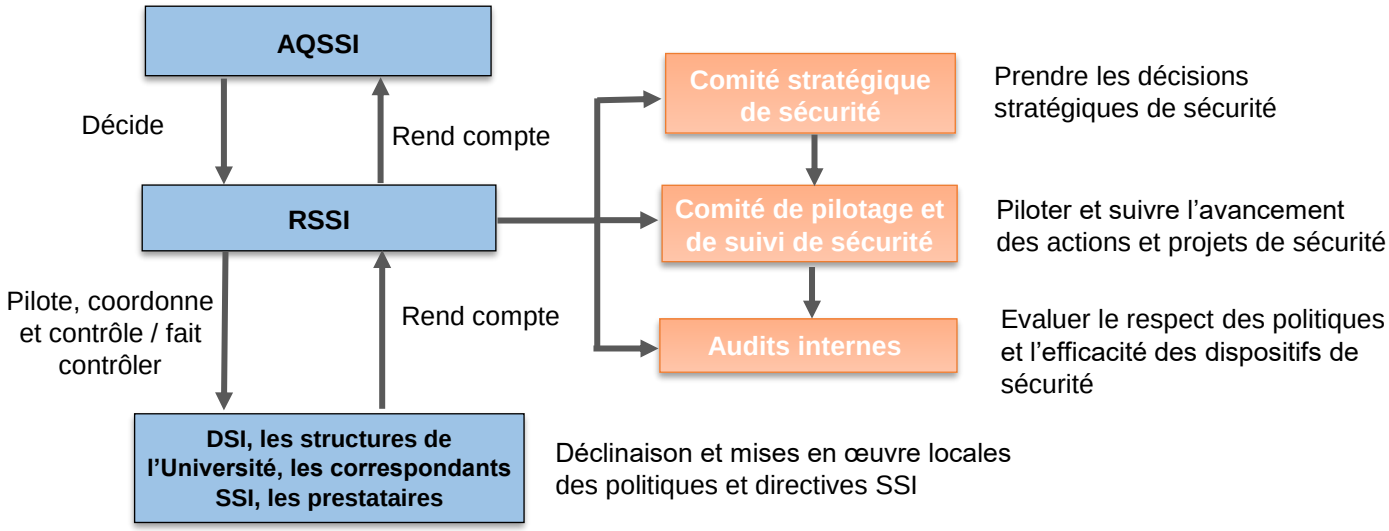
Il revient ensuite à chaque structure de décliner sa propre politique de sécurité, en se basant sur les principes et mesures de sécurité de l'Université, afin de prendre en compte les

spécificités de son environnement (enjeux, menaces, besoins, règlementation sectorielle ou orientations des autres tutelles).

Chaque structure est responsable de la mise en œuvre opérationnelle.

III. Organisation et gouvernance de la SSI

La présidence de l'Université est l'autorité qualifiée en matière de SSI (AQSSI).
A travers un dispositif organisationnel dédié, elle s'appuie sur des rôles et responsabilités distribués à tous les niveaux pour coordonner l'ensemble des actions et mesures de sécurité et faciliter l'application de la PGSSI sur son périmètre.



III.1 Rôles et responsabilités

III.1.1 L'AQSSI

L'autorité qualifiée pour la sécurité du système d'information (AQSSI) est le responsable juridique de la sécurité des SI au sein de son établissement. A ce titre il est le décisionnaire de l'organisation de la SSI et des mesures de sécurité à appliquer. Le président de l'université de Bordeaux en tant que Chef d'établissement porte cette fonction.

Il a pour rôle principal :

- De définir la politique de sécurité des systèmes d'information et de fixer les objectifs en matière de sécurité des SI pour l'établissement et pour toutes les entités rattachées, ou bénéficiaires des moyens informatiques mis à disposition par la DSI de l'université de Bordeaux.
- D'assurer la responsabilité globale du niveau de sécurité nécessaire pour toutes les activités portées au sein de l'établissement
- De veiller au respect du cadre réglementaire et légal
- D'arbitrer le plan de traitement des risques et les ressources et moyens alloués

- De faire mener les contrôles et audits nécessaires au sein même des structures de l'université de Bordeaux, mais aussi chez les partenaires extérieurs et prestataires
- D'intenter des actions en justice si nécessaire

L'AQSSI nomme et mandate le RSSI pour mener toutes les actions utiles au sein de l'université de Bordeaux au regard des exigences réglementaires et de l'état de l'art en matière de SSI.

III.1.2 Le VP Numérique

Le VP numérique, entre autre missions, assure le pilotage politique de la SSI, sa mise en application au sein de l'Université et des composantes qui lui sont rattachées, et la bonne articulation et meilleure cohérence avec la protection du potentiel scientifique et technique (PPST). Il est aussi responsable de la définition et de la mise en œuvre du cadre partenarial de la SSI, notamment en lien avec les organismes nationaux de recherche avec lesquels l'Université partage la tutelle des laboratoires.

III.1.3 Le Chargé de mission SSI

Le chargé de mission SSI assiste le VP Numérique dans le portage politique de la SSI.
Il est l'interlocuteur privilégié des Directeurs des structures, des composantes de formation, des laboratoires de recherche et des plateformes scientifiques dans la déclinaison et la mise en oeuvre des politiques de sécurité.

Il anime le réseau des correspondants SSI et supervise la mise en œuvre des actions de sécurité, les analyses de risques, les plans d'actions préventifs et l'appropriation des enjeux SSI sur l'ensemble du cycle de vie des projets informatiques portés par chaque entité.

En matière de sécurité des SI, il représente l'équipe politique de l'Université auprès des organismes et services de l'Etat ainsi qu'auprès des partenaires de l'Université.

III.1.4 Le RSSI

Le Responsable de la Sécurité des Systèmes d'Information, rattaché hiérarchiquement à l'AQSSI, a pour mission de formaliser les politiques de sécurité des SI, d'organiser et de coordonner la mise en œuvre des politiques de sécurité. Il est force de proposition et de conseil auprès du VP Numérique, du chargé de mission, des directions, des responsables de structures et des responsables de départements.

Il s'appuie sur la DSI et les correspondants SSI de chaque structure pour la mise en œuvre des actions de sécurité, les analyses de risques, les plans d'actions préventifs et l'appropriation des enjeux de la SSI sur l'ensemble du cycle de vie des projets informatiques portés par chaque entité.

Le RSSI est l'interlocuteur opérationnel privilégié pour les organismes et services de l'état (ANSSI, DGSI, COSSIM…), les structures de l'Université, et toute entité collaborant avec l'Université ou en interaction avec elle (partenaires, prestataires, collectivités, associations, etc.).

Le RSSI est associé au pilotage des projets et définit les exigences de sécurité afin d'impulser les actions de sécurisation adaptées aux contextes, à l'état de l'art et dans le respect des exigences règlementaires.

III.1.5 Le DSI

Le Directeur des Systèmes d'Information (DSI), dirige les Systèmes d'Information de l'université de Bordeaux. Il s'appuie sur les accords de coordination établis avec les composantes, laboratoires et plateformes scientifiques pour articuler leurs systèmes d'information propres.

Le DSI, définit la stratégie en matière de mise en oeuvre de la SSI, afin de décliner les politiques et objectifs de sécurité en projets, en mesures et actions de sécurisation.

Dans cet objectif, le DSI coordonne l'action de ses équipes avec le RSSI et le DPO en vue d'intégrer les exigences de sécurité sur l'ensemble des systèmes d'information et des services associés, tout en respectant le besoin de protection des données à caractère personnel, et plus largement le patrimoine informationnel.

III.1.6 Le Fonctionnaire Sécurité et Défense (FSD)

Le Fonctionnaire de sécurité et de défense (FSD) est nommé par le Haut Fonctionnaire de défense et de sécurité (HFDS). En tant que relais fonctionnel du HFDS, le FSD est placé sous l'autorité du président de l'Université qu'il assiste pour l'exercice de ses responsabilités en matière de défense et de sécurité.
A ce titre, le FSD veille à la déclinaison et à la mise en œuvre des dispositions relatives à la protection du potentiel scientifique et technique (PPST) qui s'inscrivent dans le cadre de procédures réglementaires nationales. Son action vise ainsi à protéger les laboratoires contre les atteintes à leurs intérêts économiques et contre les risques de détournement de travaux de recherche à des fins de prolifération ou de terrorisme.

Le FSD, en outre, participe à la protection du patrimoine informationnel de l'université en étroite liaison avec le RSSI. Il est en charge du déploiement des plans nationaux de défense et de protection, en particulier le plan VIGIPIRATE. A cet égard, il identifie et évalue les risques et propose des parades et s'assure de leur mise en œuvre effective.

III.1.7 Le correspondant SSI

Chaque responsable de structure (directeur d'unité, de composante d'enseignement, de laboratoire, de pôle, direction ou service, …) est responsable de la sécurité au sein même de sa structure, et doit par conséquent respecter les exigences SSI de l'université de Bordeaux. À ce titre il doit désigner un correspondant SSI pour sa structure. Ce dernier sera le correspondant direct du RSSI, dans le cadre des actions et projets menés conjointement.

Les activités possibles du correspondant SSI pourront être, selon le contexte :

- Piloter des analyses de risques de son entité
- Mettre en œuvre des mesures de sécurité
- Diffuser en interne des bonnes pratiques
- Participer à la sensibilisation de la SSI auprès des usagers du SI

- Participer aux comités de sécurité organisés par le RSSI
- Participer à la déclinaison des exigences de sécurité sur son entité en coordination avec le RSSI
- Assurer le maintien en conditions de sécurité du SI de son entité : conception, déploiement, supervision, administration et exploitation du SI
- Participer aux traitements des incidents en coordination avec le RSSI et la DSI

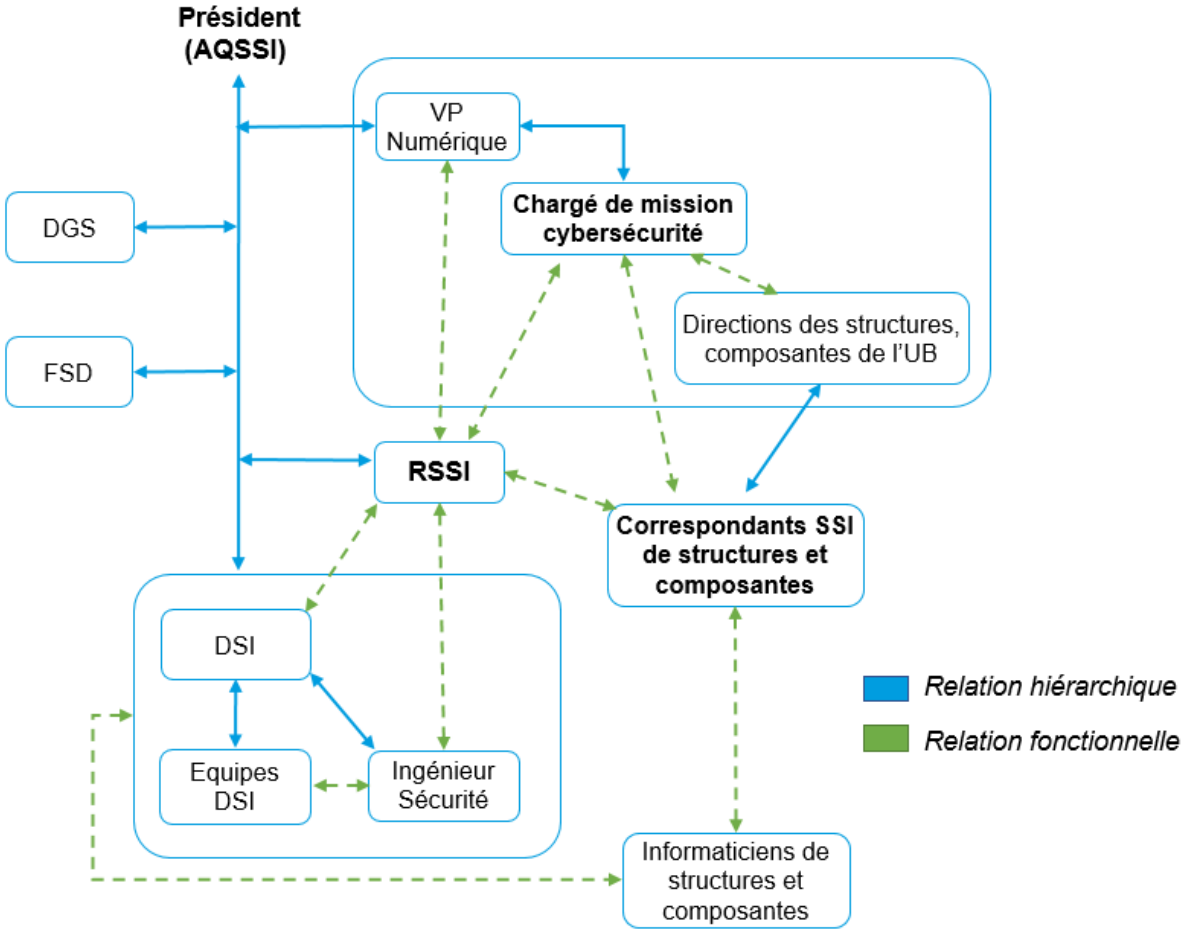


Figure 1 Organisation de la Sécurité des Systèmes d'Information

III.2 Instances de gouvernance de la sécurité

III.2.1 Le Comité stratégique de la sécurité des SI

Le comité stratégique, instance annuelle, composé des membres du Comité de Direction, du VP Numérique, du chargé de mission sécurité, de la DSI, du fonctionnaire de sécurité défense (FSD), du RSSI et du DPO, permet de partager et valider :

- La stratégie de la sécurité des systèmes d'information
- Une vision prospective sur l'évolution des risques cyber
- La feuille de route et les objectifs
- Le plan de traitement des risques

- Les moyens et ressources nécessaires à mettre en œuvre
- Les budgets nécessaires
- Les évolutions de la PGSSI

Ce comité est dirigé par le Président de l'université de Bordeaux, qui s'appuie sur le RSSI pour le pilotage du comité et son animation.

III.2.2 Le Comité de pilotage de la sécurité des SI

Le Comité de pilotage est une instance mensuelle permettant le pilotage et le suivi de la mise en œuvre des actions et des projets de SSI :

- Pilotage de la feuille de route SSI
- Suivi des projets et actions en cours
- Identification des évolutions nécessaires
- Suivi des indicateurs de pilotage

Le comité de pilotage est dirigé par le RSSI en coordination avec les Responsables de Direction en charge de la SSI (FSD, DPO, DSI, Chargé de mission SSI, VP Numérique…).

III.2.3 Le Comité de suivi de la sécurité des SI

Le comité de suivi est une instance bimensuelle sur demande du RSSI, permettant de suivre l'avancement des activités opérationnelles de sécurisation sur l'ensemble du système d'information :

- Suivi des actions de sécurisation
- Analyse des évènements et incidents de sécurité
- Amélioration des processus qualité

Le comité de pilotage est dirigé par le RSSI en coordination avec les correspondants SSI concernés, et les équipes de la DSI.

IV. Principes de mise en œuvre

Les principes de mise en œuvre s'articulent autour d'un pilotage et d'une démarche d'intégration de la sécurité du système d'information à tous les niveaux et d'une chaine de responsabilité. Ils sont basés sur les activités suivantes :

- Engager les responsabilités, au travers de la gouvernance et du pilotage de la sécurité, de chaque structure et tiers utilisateurs du SI
- Identifier les risques et définir les mesures prioritaires
- Implémenter les mesures prioritaires
- Piloter la mise en œuvre et contrôler périodiquement le niveau d'application des mesures
- Identifier et mettre en œuvre des actions en fonction des écarts.

IV.1 Garantir la sécurité des SI

Chaque Responsable de structure (directeur de composante ou de service) et chaque partenaire de l'Université est **responsable de la sécurité de son entité**, et doit pouvoir présenter des garanties en la matière. Il doit assurer un niveau de sécurité et de résilience adapté aux activités qu'il porte, et suffisant pour ne pas compromettre les moyens et services numériques proposés par l'université de Bordeaux. Par conséquent, il est garant de la bonne gestion et maitrise des actifs du SI (PC, équipements industriels, objets connectés, …) auxquels son entité accède. Il répond de la présence légitime ou illégitime d'équipements non référencés et introduits sur le SI dans son périmètre d'activité, par un personnel de son entité ou par un tiers.

À cette fin, au regard des enjeux de SSI, en fonction des missions, des projets et attentes de chaque responsable d'entité, un ensemble d'exigences minimales à respecter, sera défini afin d'établir une zone de confiance favorisant la confidentialité, l'intégrité et la disponibilité de l'information.

Les réseaux de l'Université sont interconnectés avec le réseau national RENATER et au-delà à des réseaux internationaux (exemple le réseau GEANT).

La vigilance de l'université de Bordeaux contribue ainsi à la sécurité de la recherche nationale et internationale. Pour assurer la sécurité des SI, RENATER et l'Université déploient des outils d'analyse et de détection des menaces et attaques.

En cas de besoin, l'Université peut bloquer les communications sur le réseau, généralement en lien avec les administrateurs des équipements concernés. En cas d'urgence cela peut se faire sans délai.

IV.2 Identifier les risques et définir les mesures prioritaires

Les mesures de sécurité, quel qu'en soit le périmètre, doivent être définies au regard des risques spécifiques de SSI en lien avec la démarche globale du management des risques traités au sein même de l'université de Bordeaux.

Les risques majeurs doivent être identifiés et réévalués périodiquement en fonction de l'état du SI, de ses vulnérabilités, de l'évolution générale des menaces, et des impacts que la réalisation de ces menaces pourrait provoquer sur les actifs critiques. Pour ces raisons, les biens critiques doivent être identifiés et classifiés. La classification est appréciée selon les quatre critères de sécurité (disponibilité, intégrité, confidentialité, et traçabilité).

Le RSSI met en place une méthodologie d'évaluation et de traitement des risques, applicable à l'ensemble des systèmes d'information, et en coordination avec la direction pédagogique, les laboratoires, la DSI et la Présidence de l'université de Bordeaux. Cette dernière s'appuiera sur les évaluations et résultats d'analyses pour piloter le management des risques dans sa globalité (indicateurs de pilotage).

Le RSSI coordonne de manière régulière avec les correspondants SSI, les différentes analyses de risques à mener selon le périmètre du SI identifié (plate-forme, portail web, équipements des laboratoires, etc.) et nécessaires au regard de sa sensibilité, de ses évolutions, des nouveaux usages, et des contraintes réglementaires.

A l'issue de chaque évaluation, un plan de traitement est formalisé pour réduire les risques identifiés à un niveau acceptable.

En complément, des tests d'intrusions pourraient-être réalisés périodiquement ou à chaque évolution majeure, afin de vérifier à minima la robustesse des systèmes d'information.
Les résultats des tests alimenteront les tableaux de bords, notamment la cartographie des risques.

IV.3 Intégrer la sécurité dans les projets

La sécurité des SI doit être prise en compte dans toutes les phases des projets informatiques, et sur l'ensemble du cycle de vie de ces derniers (MOA/MOE), dès la phase d'opportunité d'un projet.

Tout projet devra prendre en compte le principe de « security by design » stipulant que la SSI est prise en compte dès la phase de conception, et que cette dernière garantira la robustesse et le bon niveau de protection des composants (matériel, logiciel, données).

Cette exigence devra s'intégrer dans la démarche méthodologique des parties prenantes, afin de garantir le bon niveau de protection, de la phase de conception jusqu'à la mise en production.

La sécurisation sera atteinte par la mise en œuvre de mesures proportionnées et adaptées visant à assurer le niveau de sécurité requis en terme de :

- **Confidentialité** : capacité à protéger les informations de toute diffusion et divulgation à des personnes, des entités ou des processus non autorisés.

- **Intégrité** : capacité à préserver les informations de toute altération, destruction ou modification non autorisée.

- **Disponibilité** : capacité à maintenir l'accessibilité aux informations et aux applications dans des conditions d'horaire et de délai attendues.

- **Traçabilité** : capacité à enregistrer et à conserver des logs systèmes et les traitements des informations selon la règlementation et les politiques de sécurité.

Dans le cadre d'un recours à un fournisseur ou un prestataire, les exigences de sécurité pourront être complétées par un Plan d'Assurance Sécurité (PAS). Ce document indiquera les engagements et les mesures de sécurité du fournisseur en matière de protection et de sécurité du système d'information concerné.

IV.4 Gérer les incidents SSI

L'objectif est de définir une organisation cohérente, coordonnée et efficace de gestion des incidents liés à la sécurité de l'information, incluant :

- La communication des évènements et des failles liées à la sécurité
- Des enregistrements des évènements et traces liés aux incidents
- Une capitalisation par des actions correctives et préventives

En relation directe avec les correspondants SSI de chaque entité, le RSSI avec la DSI, reçoit et analyse les remontées d'alertes, et appuie le cas échéant, les correspondants SSI dans la qualification des incidents. Le traitement des incidents sera porté soit par la DSI et ses équipes soit par les informaticiens des partenaires, en coordination avec le RSSI. Cette centralisation permettra d'améliorer la réactivité nécessaire en cas d'attaque informatique.

En cas **d'incident majeur ou de situation de crise**, impactant fortement les activités de l'université de Bordeaux, **une cellule de crise sera activée**, impliquant l'ensemble des acteurs permettant de remédier à la situation, et de gérer la crise. Cette cellule pourra en coordination avec le RSSI, s'appuyer sur les services de l'État et les partenaires concernés.

IV.5 Contrôler et assurer la conformité

L'université de Bordeaux souhaite s'inscrire dans une démarche de conformité et de respect du cadre réglementaire. A ce titre, et au regard des exigences de conformité, l'université de Bordeaux s'appuie sur la politique de sécurité de l'État, la PSSI-E, et celle de son ministère de tutelle, la PSSI-M.

IV.5.1 Cadre réglementaire et conformité

Le Référentiel Général de Sécurité (RGS v2.0)

En tant qu'Autorité Administrative comme tout établissement public, l'université de Bordeaux est tenue de respecter le Référentiel Général de Sécurité établi par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), officialisé par le décret n° 2010-112 du 2 février 2010.

À ce titre, l'université de Bordeaux doit mener à bien les homologations nécessaires, afin d'attester formellement auprès des utilisateurs de son système d'information que celui-ci est sécurisé conformément aux objectifs de sécurité fixés.

La Loi de Programmation Militaire

Compte-tenu des enjeux en matière de protection de l'information, l'université de Bordeaux est tenue de prendre en compte les exigences et contraintes relatives à la sécurité des systèmes d'information des opérateurs d'importance vitale, ces derniers pouvant être partenaires dans des projets de recherche notamment.
À ce titre, elle doit sécuriser ses Systèmes d'Information, afin d'attester que ceux-ci sont protégés conformément aux objectifs de sécurité fixés entre les parties. Elle doit également désigner un officier de sécurité à qui incombe l'organisation, la gestion et le contrôle interne de la protection des informations et supports classifiés et de l'application de la réglementation.

Protection des données à caractère personnel (RGPD)

Pour l'ensemble de ses activités, l'université de Bordeaux participe à la mise en œuvre de traitements de données à caractère personnel. À ce titre, l'université de Bordeaux doit s'assurer que ces traitements sont réalisés conformément aux exigences de la Loi Informatique et Libertés (loi 78/17), ainsi qu'au règlement EU 2016/679 dont la date d'applicabilité est définie au 25 mai 2018.

Réglementation Hébergement des données de santé (HDS)

L'université de Bordeaux héberge son système d'information et les plates-formes le cas échéant des structures et autres entités. Au regard de la typologie des données, et dans le cadre des activités de recherche, l'obligation d'être certifiés HDS par un organisme accrédité peut s'avérer nécessaire, et l'université de Bordeaux pourra s'inscrire dans cette démarche ou s'appuyer sur un hébergeur certifié.

IV.5.2 Audits internes

Afin de satisfaire au cadre réglementaire, et de vérifier l'application correcte des principes et règles de sécurité émanant de la PGSSI et de tout document relatif à la déclinaison de cette dernière, au travers de directives et actions de sécurité à mener au sein des entités, des contrôles pourront être menés sous la responsabilité du RSSI. Ces contrôles auront pour but notamment d'apporter une meilleure cohérence, et d'évaluer le niveau de maturité sur l'ensemble des entités, afin d'améliorer la résilience de l'université de Bordeaux, de ses partenaires et de tous bénéficiaires du système d'information et services associés.

En complément des contrôles ponctuels évoqués, des audits relatifs au cadre réglementaire, de conformité ou audits internes à l'appréciation du RSSI et en coordination avec l'équipe du contrôle d'audit interne, seront programmés sur l'année, pour analyser et évaluer la pertinence des mesures, l'efficacité des organisations et moyens mis en œuvre. Ces différents audits pourront être aussi menés par des prestataires référents en la matière selon la nécessité, pour appuyer les activités d'audit.

Tout partenaire ou tiers pourra être audité à la demande du RSSI, pour s'assurer du respect des politiques de sécurité des SI et vérifier la bonne application des mesures et les moyens déployés, au regard des enjeux de sécurité, et des niveaux de risques évalués périodiquement.

Concernant la qualification et le référencement des prestataires, fournisseurs, éditeurs et partenaires technologiques externes, ces derniers devront pouvoir apporter des garanties, et démontrer leur capacité à répondre aux exigences de sécurité, exprimées dans l'annexe de sécurité des appels d'offres et marchés de l'Université, précisant notamment, l'acceptation de chacun à pouvoir être audité et contrôlé pendant toute la durée de la relation contractuelle.

Par conséquent, des audits seront réalisés par le RSSI pour vérifier l'application des exigences de sécurité de l'université de Bordeaux, et la pertinence des moyens déployés.

IV.5.3 Réévaluer la PGSSI

La politique devra faire l'objet d'une revue périodique visant à valider son champ d'application ainsi que l'ensemble des principes énoncés et essentiels au regard des enjeux de sécurité des SI. Cette réévaluation devra avoir lieu une fois tous les 2 ans, voire dans un délai plus court si elle est motivée et justifiée par une évolution du contexte et de l'environnement de l'université de Bordeaux. Elle sera portée par le RSSI.

La révision de la PGSSI, imposera de réévaluer les impacts sur le corpus documentaire, et notamment la pertinence des politiques thématiques suivantes :

- Politique de mot de passe
- Politique de chiffrement
- Politique de traitement des vulnérabilités
- Politique de gestion des actifs
- etc

En savoir +

www.u-bordeaux.fr

@ univbordeaux

univbordeaux

universitedebordeaux

universite-de-bordeaux

université de BORDEAUX