ULB UNIVERSITÉ LIBRE DE BRUXELLES

Politique de Sécurité des Systèmes d'Information de l'ULB

(approuvée par le Conseil d'administration du 20 avril 2020)

Table des matières

1. Introduction

1.1. Enjeu et besoins

A l'ère de la révolution numérique, l'information constitue une véritable richesse qui attise la convoitise des cybercriminels. Elle peut également être exposée à des menaces involontaires, qu'elles soient humaines, matérielles (panne…) ou naturelles (inondations…). La protection de l'information est par conséquent devenue un enjeu majeur pour les organisations, que vient renforcer l'entrée en vigueur en mai 2018 du Règlement général sur la protection des données personnelles.

1.1.1. Protection des données et des outils de travail

La sécurité de l'information répond à quatre besoins principaux :

- **la confidentialité**, ou la garantie que seules les personnes autorisées ont accès aux éléments considérés (applications, fichiers,…) ;
- **l'intégrité**, ou la garantie que les éléments considérés (données, messages,…) sont exacts et complets et qu'il n'ont pas été modifiés ou perdus ;
- **la disponibilité**, ou la garantie que les éléments considérés (fichiers, messages, applications, services) sont accessibles au moment voulu par les personnes autorisées ;
- **la traçabilité**, ou la garantie que les accès et tentatives d'accès aux informations sont tracés et que les traces sont conservées et exploitables en temps voulu.

La définition précise des besoins de protection au sein de l'institution doit être assurée par les responsables des données. Cette définition est le résultat d'une analyse des risques basée sur des échelles institutionnelles.

1.1.2. Protection de la réputation

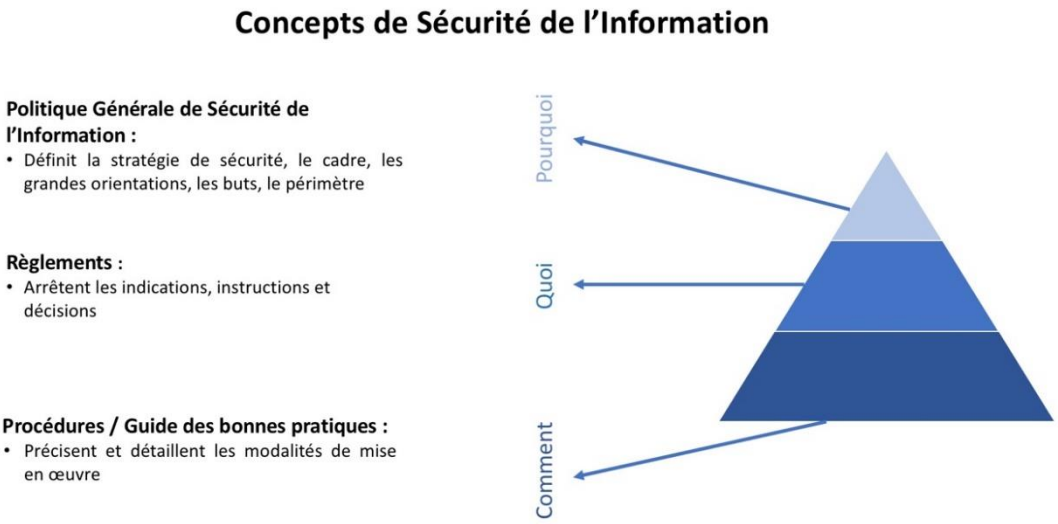
L'estime et la confiance accordées à l'Université par ses différents publics se basent sur la réputation de celle-ci. Une atteinte à cette réputation pourrait impacter négativement :

- le nombre d'inscriptions ;
- la capacité de l'institution à recruter du personnel de qualité ;
- les opportunités de contrats dans le cadre de la recherche ;
- les projets de collaborations interinstitutionnelles, y compris internationales (ex : co-diplomation…) ;
- …

Une prévention contrôlée des risques et une gestion cadrée des incidents de sécurité de l'information permettent de protéger l'image de l'Université, tant en interne qu'à l'extérieur.

1.2. Objectifs

La Politique de Sécurité des Systèmes d'Information définit la vision stratégique de l'Université en termes de sécurité des données. Elle fixe les objectifs et standards de sécurité, le périmètre d'application et traduit l'engagement de l'ULB à mettre en œuvre les mesures de protection adaptées à son contexte ainsi qu'au cadre juridique en vigueur.



Au-delà d'une mise en conformité de l'institution à la législation nationale et supranationale, il s'agit pour l'ULB de se rapprocher des standards internationaux et :

- de réduire les incidents ainsi que leurs impacts sur le fonctionnement de l'Université ;
- de réduire les risques et leurs conséquences potentielles (ex : amendes sévères en cas d'infraction au RGPD, impact sur la réputation) ;
- de prioriser efficacement les actions à entreprendre;
- de rationaliser les coûts et ressources à engager dans le cadre de la mise en œuvre des objectifs et mesures de sécurité;
- de s'inscrire dans un processus d'amélioration continue de la sécurité, qui tienne compte de l'évolution des activités de l'institution (nouveaux risques) et du contexte numérique ;
- d'apporter la garantie d'un traitement sécurisé des données et dès lors d'améliorer la confiance dans le cadre de partenariats (contrats de recherche, conventions inter-institutionnelles…);
- …

La Politique de Sécurité des Systèmes d'Information s'accompagne de :

- règlements, qui arrêtent les instructions et décisions ;
- procédures et bonnes pratiques, qui précisent et détaillent les modalités de mise en œuvre.

La PSSI s'applique à l'ensemble des utilisateurs des systèmes d'information de l'ULB. Elle est sujette à des mises à jour périodiques et approuvée par les autorités.

2. Cadre législatif et normatif

La mise en œuvre de systèmes d'information est soumise à des obligations relevant de dispositions législatives et réglementaires qui confèrent un enjeu juridique important à cette activité. L'institution doit s'assurer de la conformité permanente de la PSSI à celles-ci.

2.1. Règlement Général sur la Protection des données (RGPD)

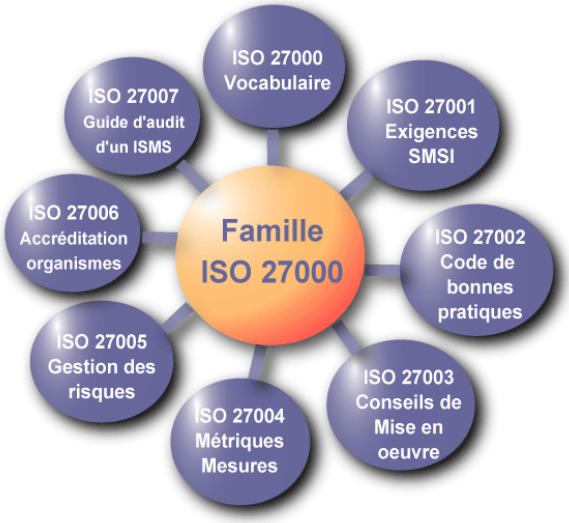
La PSSI incorpore les éléments RGPD qui concernent les données à caractère personnel sous format électronique uniquement[1].

2.2. Protection de la propriété intellectuelle (PI)

La PSSI, bien qu'elle n'en couvre pas tous les aspects, favorise la protection de la propriété intellectuelle.

2.3. Normes ISO 27000

Les normes internationales de sécurité de la série ISO 27000 sont destinées à protéger l'information. Elles découlent d'une recherche de consensus dans le domaine et servent de base à la PSSI de l'ULB.



2.3.1. Exigences pour un Système de Management de la Sécurité de l'Information - ISO 27001[2]

La norme ISO/CEI 27001 s'adresse à tous les types d'organismes (entreprises commerciales, ONG, administrations…) et définit les exigences pour la mise en place d'un système de management de la sécurité de l'information (SMSI).

Le SMSI recense les mesures de sécurité, dans un périmètre défini, afin de garantir la protection des actifs de l'organisme. L'objectif est de protéger les informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion et sinistre informatique.

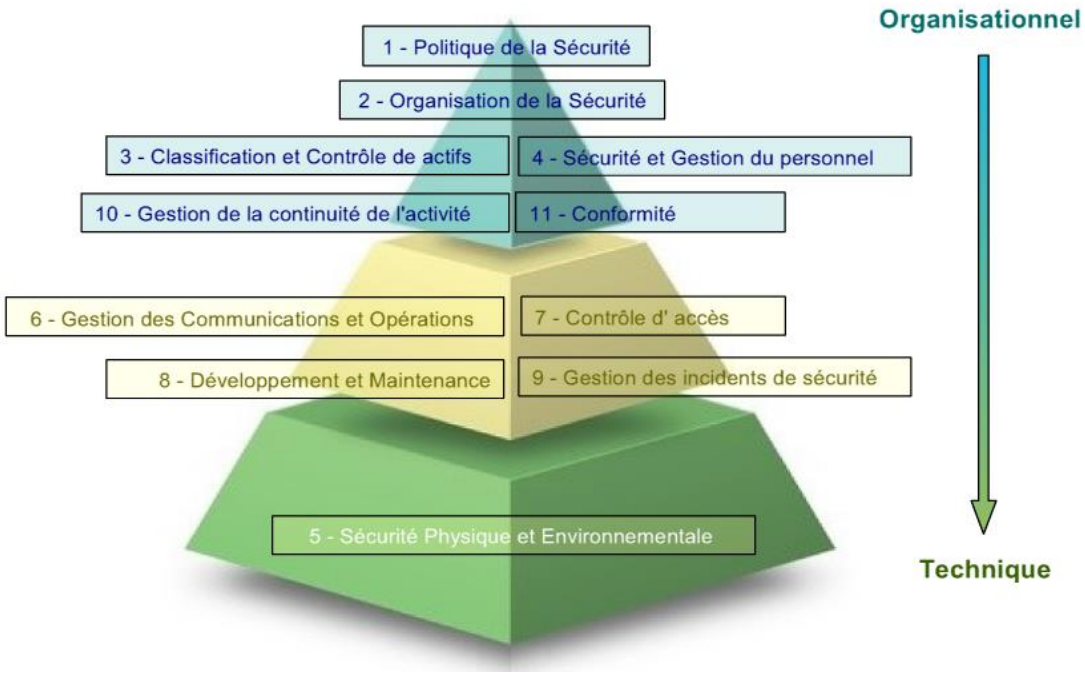
La norme précise que les exigences en matière de mesures de sécurité doivent être adéquates et proportionnées aux risques encourus et donc ne pas être ni trop laxistes, ni trop sévères.

Elle énumère un ensemble de points de contrôle à respecter pour s'assurer de la pertinence du SMSI, permettre de l'exploiter et de le faire évoluer.

[1] https://portail.ulb.be/fr/documents-officiels/protection-des-donnees-a-caractere-personnel
[2] Source : https://www.iso.org/fr/isoiec-27001-information-security.html

2.3.2. Code de bonnes pratiques pour le management de la sécurité de l'information - ISO 27002

La norme ISO/IEC 27002 :2013 constitue un volet concret pour la mise en œuvre du SMSI. Elle est composée de 114 mesures de sécurité réparties en 14 chapitres couvrant les domaines organisationnels et techniques.



2.3.3. Gestion des risques liés à la sécurité de l'information - ISO 27005

La norme ISO 27005[3] propose des lignes directrices traitant spécifiquement de la gestion des risques dans le contexte de la Sécurité des systèmes d'information.

3. Structure organisationnelle

La mise en œuvre de la PSSI s'appuie sur une structure fonctionnelle interne spécialisée en sécurité des systèmes d'information.

3.1. RSSI

Le Responsable de la Sécurité des Systèmes d'Information (RSSI, ou CISO[4] en anglais) coordonne la mise en œuvre de la PSSI. Il :

- veille à la diffusion de l'information ainsi qu'à la formation/sensibilisation des membres de la communauté universitaire ;
- assure un rôle de conseil et d'assistance à la bonne mise en œuvre de la sécurité de l'information ;

[3] https://www.iso.org/fr/standard/56742.html
[4] Chief Information Security Officer

- est l'interface entre les intervenants internes et externes pour les problématiques de sécurité ;
- réalise des contrôles internes réguliers, détermine la périodicité des audits externes et les supervise ;
- effectue un travail de veille technologique.

3.2. DPD

Le Délégué à la Protection des données (DPD, ou DPO[5] en anglais) a pour mission le contrôle des traitements de données à caractère personnel au sein de l'Université. Il :

- collecte des informations pour identifier les activités de traitement ;
- analyse et vérifie la conformité des activités de traitement au RGPD ;
- informe, conseille ou adresse des recommandations au responsable du traitement ou au sous-traitant.

3.3. SIRT

La Security Incident Response Team (SIRT) a pour mission le traitement des incidents présentant un niveau de risque élevé, conformément au processus de gestion adopté par l'institution[6].

Elle collabore étroitement avec le RSSI qui est systématiquement consulté.

La SIRT a autorité pour prendre les décisions qu'elle estime nécessaire afin de réduire les conséquences d'un incident. Les mesures et actions prises par la SIRT doivent être proportionnées, et la responsabilité des conséquences liées à celles-ci est assumée par l'institution.

Il appartient à la SIRT :

- d'établir un plan de réponse;
- lorsque l'incident implique des données à caractère personnel, de se coordonner avec la CPDD -dont le DPO fait partie- conformément au processus institutionnel de gestion des incidents de sécurité ;
- d'avertir les autorités fédérales (FCCU ou Federal Computer Crime Unit) si elle l'estime nécessaire ou si la loi l'y contraint ;
- d'établir des liens et communiquer avec le CERT (Cyber Emergency Response Team) ;
- de consigner chaque incident dans le registre des incidents et proposer des améliorations pour les systèmes, les infrastructures ou les procédures.

En cas de nécessité, elle participe à la gestion de la communication interne et/ou externe sur les incidents.

3.4. COSI

Le Comité de l'Organisation de la Sécurité Informatique (COSI) définit, améliore et encourage de façon continue les politique et stratégie de sécurité, qu'il porte devant le Conseil d'Administration

[5] Data Protection Officer
[6] En annexe

le cas échéant. Il fixe en outre les standards de contrôle et de sécurité de l'information, basés sur les recommandations du RSSI.

Le COSI regroupe les fonctions suivantes :

- Directeur Général
- Directeur du Département informatique
- DPO
- Adjoint du Président aux matières informatiques et numériques
- Conseiller à la sécurité de l'information
- Responsable communication DI

Sa composition transversale permet de fluidifier la transmission de l'information vers les parties concernées, particulièrement dans les situations de crise.

L'impartialité des analyses et des recommandations du RSSI est garantie par son indépendance. Il est néanmoins étroitement associé aux activités du COSI.

3.5. Référents sécurité

Au sein de chaque entité informatique[7], y compris hors administration générale, un Référent sécurité est désigné, qui assure le rôle d'interface entre celle-ci et le RSSI. Celui-ci :

- assume la responsabilité de la sécurité de l'information dans son périmètre technique ;
- veille à l'application des procédures et standards de sécurité pour la partie technique de l'exploitation de systèmes, réseaux, postes de travail et applicatifs ;
- assure une veille (faille de sécurité, vulnérabilité, exploitations des vulnérabilités, etc.…) dans son périmètre d'intervention afin de garantir le maintien du niveau de sécurité (postes de travail, systèmes, réseaux, etc…) ;
- s'assure de la sécurité des locaux techniques et des environnements de travail et signale toute anomalie à l'Administration générale conformément au processus de gestion des incidents.

Les Référents sécurité sont désignés par les organisations locales des entités. Leur identité est déclarée auprès de l'Administration générale et des autorités académiques et de recherche.

3.6. Administrateurs systèmes

Les administrateurs systèmes sont autorisés à agir rapidement pour protéger la sécurité de leurs systèmes. Les actions de protection qu'ils entreprennent, en particulier celles ayant un impact direct sur leurs utilisateurs, doivent être proportionnées.

Les administrateurs système doivent immédiatement signaler tout incident de sécurité à haut niveau de risque à la SIRT, conformément au processus de gestion des incidents de sécurité[8].

[7] « Entité » désigne ici tant les services IT des administrations générale et facultaires que les structures organisationnelles dynamiques telles que des unités de recherche, équipes projet…
[8] Voir annexes

4. Système de gestion de la sécurité de l'information (SMSI)

La mise en œuvre du SMSI de l'ULB applique la méthode PDCA -ou Roue de Deming- proposée par la norme ISO 27001.

- **Phase d'établissement (PLAN) :**
  - définir la politique de sécurité et le périmètre du SMSI ;
  - identifier et évaluer les risques liés à la sécurité et élaborer la politique de sécurité ;
  - traiter le risque par un plan de gestion et identifier le risque résiduel;
  - choisir les mesures de sécurité à mettre en place (voir ISO 27002) ;

- **Phase d'implémentation (DO) :**
  - établir un plan de traitement des risques ;
  - déployer les mesures de sécurité ;
  - générer des indicateurs :
    - de performance pour savoir si les mesures de sécurité sont efficaces ;
    - de conformité qui mesurent l'adéquation des mesures aux normes ;
  - former et sensibiliser les membres de la communauté universitaire ;

- **Phase de maintien (CHECK) :**
  Cette phase consiste à gérer le SMSI au quotidien et à détecter les incidents en permanence pour y réagir rapidement. Trois outils pour détecter ces incidents :
  - le contrôle interne, qui consiste à s'assurer en permanence que les processus fonctionnent normalement ;
  - les audits, internes ou externes, qui vérifient la conformité et l'efficacité du système de management. Ces audits sont ponctuels et planifiés ;
  - les revues (ou réexamens) qui garantissent périodiquement l'adéquation du SMSI avec son environnement ;

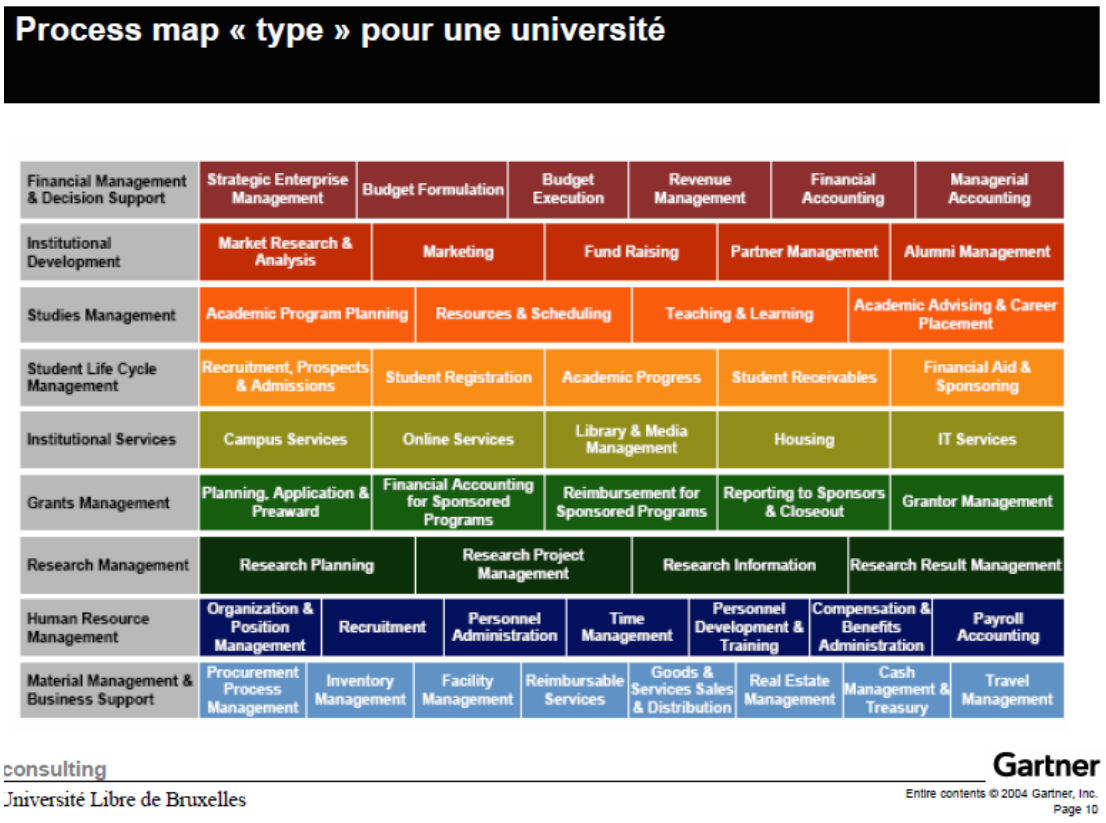
- **Phase d'amélioration (ACT) :**
  Il s'agit à cette étape de mettre en place des actions correctives, préventives ou d'amélioration pour les incidents et écarts constatés lors de la phase de maintien (Check) :
  - actions correctives : agir sur les effets pour corriger les écarts ;
  - actions préventives : agir sur les causes avant que l'incident ne se produise ;
  - actions d'amélioration : améliorer la performance d'un processus du SMSI.

Cette démarche adopte une spirale évolutive continue : la fin d'un cycle entraîne le début d'un nouveau.

4.1. Phase d'établissement (PLAN)

4.1.1. Périmètre

La PSSI de l'ULB s'applique à l'ensemble des processus qui touchent aux missions fondamentales de l'Université, traitent de données à caractère personnel ou précieuses pour l'institution ou mettent en œuvre des technologies TIC sujettes à la cybercriminalité.



Ce périmètre est à considérer comme point de départ, à élargir à terme aux processus annexes.

4.1.2. Registre institutionnel des actifs

Le registre institutionnel des actifs constitue un outil de contrôle central qui permet de rationaliser les ressources et d'en optimiser la maintenance (ex : mises à jour des systèmes d'exploitation).

Chaque actif, ainsi que ses propriétés, doit y être consigné :

- propriétaire
- finalité
- localisation
- niveau de classification
- utilisations appropriées
- …

L'inscription d'un actif au registre institutionnel doit être effectué par son responsable, métier ou technique.

Pour les actifs de type applicatif, il convient d'enregistrer également la catégorie de données selon la classification adoptée par l'institution[9] . Celle-ci permet de s'assurer que l'information reçoive un niveau de protection adapté à son importance. En cas de doute, la classification attribuée doit être la plus restrictive.

[9] Voir annexes

4.1.3. Analyse de vulnérabilité

Tous les systèmes doivent être soumis à des analyses de vulnérabilité régulières. Ces analyses peuvent être effectuées par du personnel qualifié de l'Université ou par des évaluateurs externes agréés. Les systèmes critiques de l'entreprise et les autres systèmes utilisés pour traiter ou stocker des données classées comme critiques doivent être soumis à des tests d'intrusion réguliers réalisés par un évaluateur agréé.

4.1.4. Analyse de risques

L'ensemble du périmètre du système d'information de l'Université doit faire l'objet d'analyses de risques périodiques, basées sur les échelles institutionnelles[10]. Ces analyses relèvent de la responsabilité :

- du service de gestion du réseau , pour les ressources transversales systèmes et réseaux LAN, WAN et Internet mises à disposition des membres de la communauté universitaire, des tiers et des contractants ;
- des services informatiques centraux ou décentralisés, pour :
  - les équipements et ressources informatiques mis à disposition des membres de la communauté universitaire ou de tiers dans le cadre de prestations contractuelles ;
  - les locaux techniques (salles informatiques, …) ;
- des propriétaires de données, pour les applicatifs métiers mis à disposition des membres de la communauté universitaire ;
- des Responsables hiérarchiques, pour le personnel IT ;
- du Service Delivery Manager, pour les utilisateurs finaux du système d'information

4.1.5. Plan de gestion : choix du mode de traitement du risque et identification du risque résiduel

Le plan de gestion ULB applique le modèle du « 4 T's process » . Selon les cas, le RSSI recommande :

- de transférer le risque, lorsque l'institution ne peut pas faire y face par ses propres moyens (ex : souscription d'une assurance ou contrat de sous-traitances) → « **Transfer** » ;
- d'accepter le risque, si la survenance de celui-ci entraîne des répercussions acceptables pour l'institution → « **Tolerate** » ;
- de réduire le risque, de façon à le rendre acceptable → « **Treat** » ;
- d'éviter le risque, lorsque les conséquences d'une attaque sont jugées trop périlleuses pour l'institution → « **Terminate** ».

Les risques résiduels -c'est-à-dire ceux qui persistent après la mise en place des mesures de sécurité- doivent eux aussi être pris en compte. Des mesures complémentaires de protection doivent être appliquées pour les rendre acceptables.

[10] Voir annexes

4.1.6. Sélection des mesures de sécurité

Il convient à cette étape :

- d'identifier les mesures de sécurité -nécessaires, suffisantes et proportionnées- à mettre en place ;
- de réunir les intervenants internes et/ou externes ;
- d'identifier, d'analyser et de sélectionner les solutions ;
- de consigner les points susmentionnés dans un rapport.

4.2. Phase d'implémentation (DO)

4.2.1. Plan d'actions : traitement du risque

Le plan d'actions consiste à détailler l'organisation à mettre en place en vue du déploiement des solutions sélectionnées à l'étape précédente. Il définit les actions à entreprendre ainsi que les responsabilités.

4.2.2. Déploiement des mesures de sécurité

Le déploiement des mesures de sécurité met en œuvre:

- des moyens techniques, tels que :
  - le contrôle des accès au système d'information ;
  - la surveillance du réseau : système de détection d'intrusion… ;
  - la sécurité applicative : séparation des privilèges, audit de code, rétro-ingénierie, mises à jours conformément aux exigences ou recommandations des fournisseurs de logiciels ;
  - l'emploi de technologies ad hoc : pare-feu, UTM, anti-logiciels malveillants (antivirus, anti-spam, anti-logiciel espion) ;
  - la cryptographie : authentification forte, infrastructure à clés publiques, chiffrement ;
  - le plan de continuité d'activité : sauvegarde et restauration de données, plan de reprise d'activité ;
  - …
- des moyens humains, dont principalement la sensibilisation/formation du public concerné.

L'équipe en charge de l'implémentation peut bénéficier sur demande de l'assistance et du conseil du RSSI.

4.2.3. Vérification de la sécurité

Le RSSI a pour charge la vérification régulière de la sécurité du système d'information. A cette fin, il fait usage d'indicateurs de performance mesurant l'efficacité des solutions implémentées.

Le RSSI vérifie également la conformité aux normes des mesures de sécurité.

4.2.4. Gestion des incidents de sécurité avérés

La gestion des incidents de sécurité s'effectue conformément au processus de gestion des incidents de sécurité adopté par l'institution[11].

4.2.4.1. Détection et signalement

La sécurité de l'information est l'affaire de tous. Chaque membre de la communauté universitaire a le devoir de rapporter dans les meilleurs délais tout incident de sécurité dont il est témoin, au choix :

- via le formulaire en ligne disponible sur la plateforme Support ULB ;
- par email à l'adresse support.SSI@ulb.be ;
- par email à l'adresse RGPD@ulb.be, pour les incidents impliquant des données à caractère personnel ;
- par téléphone en formant le 37 37 ;
- en contactant un responsable informatique ULB.

4.2.4.2. Enregistrement

S'il ne l'a pas été automatiquement, l'incident de sécurité doit être enregistré dans le système de gestion du support institutionnel par l'un des acteurs suivants :

- membre de l'équipe Support ULB ;
- agent IT ;
- membre de la Cellule de Protection Des Données (CPDD).

4.2.4.3. Evaluation

Le niveau de risque doit être évalué selon la grille d'évaluation officielle , par un agent IT et/ou un membre de la CPDD.

Le ticket est transféré à la SIRT et/ou au DPD en cas de risque potentiellement élevé.

4.2.4.4. Analyse

L'analyse de l'incident doit permettre :

- d'identifier le fait générateur ;
- de définir le périmètre concerné ;
- d'analyser l'impact.

Le RSSI est associé à l'analyse des incidents à haut niveau de risque.

4.2.4.5. Traitement

Des mesures de réponse immédiates, visant à éviter l'aggravation des conséquences, peuvent être prises dès l'évaluation du niveau de risque. Le cas échéant, un plan de continuité de l'activité (PCA, en anglais DRP[12]) sera activé.

[11] Voir annexes
[12] Disaster Recovery Plan

La résolution de l'incident s'effectue selon le modèle du « 4 T's process » .

Les mesures appliquées doivent être documentées.

4.2.4.6. Communication

L'analyse de risque sert d'appui à la définition d'un plan de communication. Selon la situation, la communication peut poursuivre divers objectifs :

- gestion de l'incident : communication avec d'autres équipes en interne ou avec des équipes externes ;
- conformité : communication de l'incident aux clients concernés et/ou communication à destination des autorités concernées (APD[13], FCCU, CERT…) ;
- réduction de l'atteinte à la réputation : communication vers les membres de la communauté, les partenaires, les médias…

4.2.4.7. Vérification

Le RSSI et la SIRT s'assurent de la bonne résolution des incidents de sécurité à haut niveau de risque.

4.3. Phase de vérification (CHECK)

La cohérence et l'efficacité du SMSI doivent faire l'objet d'une vérification régulière, par le biais :

- de contrôles internes, permettant de vérifier la bonne application des procédures au quotidien ;
- d'audits internes ou externes ;
- de revues de direction, dont l'objectif est de réexaminer avec recul l'adéquation du SMSI à son environnement.

4.4. Phase d'amélioration (ACT)

Cette phase inscrit l'institution dans une logique d'amélioration continue par la mise en place d'actions :

- correctives, visant à corriger les dysfonctionnements et en supprimer les effets ;
- préventives, visant à empêcher les incidents
- d'amélioration des performances des processus.

Toutes les modifications apportées aux systèmes informatiques sont soumises aux processus et procédures de gestion des modifications des services informatiques.

Un logiciel de surveillance de l'intégrité des fichiers doit être utilisé pour détecter les modifications non autorisées du système d'information.

[13] Autorité de Protection des Données (https://www.autoriteprotectiondonnees.be/)

5. Standards de sécurité

La CSSI, sous la houlette du RSSI, définit les standards de sécurité ULB. Ceux-ci évoluent au rythme des avancées technologiques ainsi que du cadre normatif.

5.1. Gestion des identités et des accès

5.1.1. Gestion des identités et authentification

L'identité et les accès de chaque membre de la communauté universitaire ainsi que ceux des tiers devant accéder à des ressources ULB doivent être enregistrés dans le système central de gestion des identités et des accès (IAM[14]).

A chaque identité enregistrée correspond un numéro d'identification unique (UID), à usage des systèmes.

A chaque IUD sont associés un ou plusieurs identifiants, destinés à l'authentification de l'utilisateur dans les systèmes de l'Université. Ce ou ces identifiants sont à usage personnel. Ils ne peuvent en aucun cas être utilisés par un autre utilisateur que celui auquel ils ont été attribués.

Chaque utilisateur se choisit un mot de passe associé à son compte ULB, selon les critères établis. Ce mot de passe est secret. Il ne doit en aucun cas être divulgué -même au personnel IT- ni ne peut être utilisé comme mot de passe au sein de systèmes tiers. Les utilisateurs sont supposés se souvenir de leur mot de passe. En cas d'oubli, ils doivent suivre la procédure de récupération de mot de passe. Enfin, les utilisateurs sont supposés changer ce dernier s'ils soupçonnent celui-ci d'avoir été compromis.

Chaque membre de l'institution se voit également attribuer une adresse électronique unique pour son usage personnel et certains membres peuvent également être autorisés à utiliser une ou plusieurs adresses électroniques génériques (basées sur les rôles). Ces adresses électroniques ne peuvent être utilisées par une autre personne sans la permission explicite de l'utilisateur auquel elles ont été attribuées. Les adresses électroniques sont des ressources appartenant à l'Université et toute utilisation de celles-ci est soumise aux politiques de l'Université.

5.1.2. Contrôle des accès

A l'exception de celui en lecture seule aux informations publiques, l'accès à tous les systèmes d'information de l'ULB doit s'effectuer via le processus d'authentification défini par l'institution. Sauf impossibilité technique, les comptes gérés localement doivent être évités.

L'accès à des ressources ULB -et a fortiori à des données à caractère personnel- est soumis à plusieurs conditions :

- l'utilisateur doit être identifié personnellement (pas d'accès attribué sur base de compte générique) ;

[14] Identity & Access Management

- ces ressources ou données doivent être reconnues par le responsable hiérarchique comme indispensables à l'utilisateur pour l'exercice de son activité professionnelle ;
- l'utilisateur accepte *de facto* les règles de confidentialité du système auquel il accède.

Le principe du « moindre privilège » doit être appliqué.

L'accès aux comptes d'administrateur de réseaux non fiables, de même que l'accès aux comptes administrateurs via l'utilisation d'appareils personnels doit autant que possible être protégé par une authentification multi-facteurs (MFA[15]).

5.1.3. Surveillance et journalisation

Toute utilisation, ou tentative d'utilisation, des systèmes doit être consignée. Les données consignées (« log files ») doivent être suffisantes pour prendre en charge les exigences du système en matière de sécurité, de conformité et de planification de la capacité, sans pour autant être inutilement intrusives. Les utilisateurs de systèmes doivent recevoir des informations claires sur les informations enregistrées, leurs objectifs et le calendrier de conservation des données collectées. Ces informations doivent être mises à la disposition des utilisateurs sous la forme d'une politique de confidentialité spécifique au système.

Il est recommandé que les « log files » soient enregistrés sur un système différent du système surveillé.

Les logs d'audit doivent être configurés pour enregistrer toutes les actions entreprises à l'aide de privilèges d'administrateur. Les journaux d'audit doivent être sécurisés pour prévenir les modifications non autorisées.

5.2. Utilisation des installations à des fins privées

Les installations d'information et de communication de l'Université, y compris les adresses électroniques et les ordinateurs, sont fournies à des fins d'administration, d'enseignement et de recherche et de service à la communauté. Une utilisation à des fins privées très occasionnelle (cfr Convention collective de travail no 81).est autorisée dans la mesure où elle :

- n'entrave pas la réalisation des tâches professionnelles des intéressés et ne perturbe pas le bon fonctionnement des installations ;
- se fasse dans le respect de la loi et ne contrevienne pas aux bonnes mœurs ;
- ne contrevient à aucune politique de l'Université ;
- est ponctuelle et se produit uniquement pendant les temps de pause ;
- n'est pas excessive dans l'utilisation des ressources.

Les membres de la communauté universitaire ne sont pas autorisés à utiliser un compte de messagerie personnel (non fourni par l'Université) pour mener à bien leurs activités à l'Université, et doivent conserver un compte de messagerie personnel et séparé pour leur correspondance privée.

[15] Multi-Factor Authentification

5.3. Utilisation de matériel personnel

L'utilisation de matériel personnel (BYOD[16]) est autorisée sous réserve de respecter les normes minimales de sécurité. Les utilisateurs doivent à tout moment tenir compte des risques liés à l'utilisation d'appareils personnels pour accéder aux informations de l'Université et, en particulier, aux informations classifiées comme confidentielles ou critiques.

5.4. Gestion et utilisation du réseau

5.4.1. Gestion du réseau

Les réseaux de communication de l'Université sont gérés par un personnel spécialement qualifié pour superviser leur fonctionnement quotidien et assurer leur sécurité permanente (confidentialité, intégrité et disponibilité).

Les membres du personnel du Service réseau sont autorisés à agir promptement pour protéger la sécurité du réseau, mais doivent être proportionnés dans les actions qu'ils entreprennent, en particulier lorsque celles-ci ont un impact sur les utilisateurs.

Les membres du personnel du Service réseau doit immédiatement signaler tout incident de sécurité à haut niveau de risque à la SIRT qui, le cas échéant, avertira le DPO conformément au processus de gestion des incidents de sécurité[17].

5.4.2. Conception et configuration du réseau

Le réseau doit être conçu et configuré pour fournir des niveaux élevés de performance, de disponibilité et de fiabilité, adaptés aux besoins de l'Université, tout en offrant un degré élevé de contrôle de l'accès.

Le réseau doit être séparé en domaines logiques distincts avec des contrôles de routage et d'accès mis en place entre les domaines afin d'empêcher tout accès non autorisé aux ressources du réseau, et afin d'éviter tout flux de trafic inutile entre les domaines.

5.4.3. Sécurité physique et intégrité

Les installations de mise en réseau et de communication, y compris les armoires de câblage, les centres de données et les salles informatiques, doivent être correctement protégées contre les dommages accidentels (par exemple, incendie ou inondation), contre le vol ou tout autre acte malveillant.

Le réseau doit, le cas échéant, et dans la mesure du possible, être résilient afin d'atténuer les effets de la défaillance de ses composants.

5.4.4. Gestion du changement

Toutes les modifications apportées aux composants réseau (routeurs, pare-feu, etc.) sont soumises aux processus et procédures de gestion des modifications du service informatique.

[16] Bring Your Own Device
[17] Voir annexes

5.4.5. Connexion de périphériques au réseau

Toute connexion de périphérique au réseau de l'Université doit se s'effectuer exclusivement au moyen de matériel fourni par l'équipe réseau.

Il est permis de connecter du matériel appartenant aux particuliers aux réseaux sans fil de l'université.

Tous les appareils connectés au réseau, quel que soit leur propriétaire, sont soumis à des tests de surveillance et de sécurité, conformément aux pratiques opérationnelles normales.

5.4.6. Gestion des adresses réseau

L'attribution d'adresses utilisées sur les réseaux de l'Université doit être gérée par l'équipe réseau, qui peut déléguer la gestion de sous-ensembles de ces espaces d'adresses à d'autres équipes au sein des services informatiques.

Les adresses réseau attribuées aux systèmes des utilisateurs finaux doivent, dans la mesure du possible, être attribuées de manière dynamique[18].

5.4.7. Contrôles des accès au réseau

L'accès aux ressources du réseau doit être strictement contrôlé pour empêcher tout accès non autorisé. Les procédures de contrôle d'accès doivent fournir des garanties adéquates grâce à des techniques d'identification et d'authentification robustes.

Le service réseau est responsable de la gestion des passerelles reliant le réseau de l'Université à Internet. Des contrôles seront appliqués à ces passerelles pour limiter l'exposition des systèmes universitaires à Internet et ainsi réduire les risques de piratage, d'attaque par déni de service, d'infection par un programme malveillant ou encore d'accès non autorisé à l'information. Les contrôles seront appliqués au trafic entrant et sortant.

5.4.8. Règles de sécurité en matière d'utilisation du réseau

Cette politique définit les responsabilités et le comportement requis des utilisateurs du réseau de l'Université. Tout utilisateur du réseau de l'Université est soumis à cette politique, quel que soit son statut ou son affiliation à l'Université :

- les utilisateurs ne doivent pas exploiter de services qui redistribuent les services du réseau ULB à d'autres personnes, de même que les utilisateurs ne doivent pas donner accès à des services à ceux qui n'y sont pas autorisés ;
- aucun périphérique connecté au réseau de l'ULB ne peut être configuré avec une adresse (IP ou MAC) autre que celle qui lui a été attribuée par les administrateurs du service réseau ;
- les ordinateurs ne doivent pas fonctionner en tant que serveurs à moins d'être enregistrés et autorisés. Les serveurs autorisés doivent répondre aux standards de sécurité définis par le service informatique ;

[18] Protocole DHCP

- le réseau est une ressource partagée et doit être utilisé de manière responsable. Tout utilisateur qui persiste à générer un trafic excessif, après avoir été invité à ne pas le faire par le support réseau, enfreindra cette politique ;
- toute utilisation du réseau ULB doit être en totale conformité avec la loi ;
- les utilisateurs sont responsables de la sécurité de leurs ordinateurs, et doivent s'assurer que ceux-ci ne peuvent pas être utilisés de manière abusive ;
- les utilisateurs doivent suivre les instructions du service informatique pour installer, reconfigurer ou mettre à niveau les logiciels nécessaires afin de garantir la sécurité de leurs ordinateurs.

5.5. Stockage distant des données

Les données classées « internes », « confidentielles » ou « critiques » doivent être stockées dans un système de cloud répondant aux normes d'exigence européenne.

5.6. Autres standards de sécurité

Tout utilisateur s'engage à faire usage du système d'information de l'ULB en bon père de famille et à respecter les standards de sécurité définis dans la PSSI, les règlements, procédures et guides de bonnes pratique de l'ULB.

6. Sous-traitance et conformité des tiers

Avant d'externaliser ou de permettre à un tiers d'accéder aux informations ou systèmes non publiques de l'Université, le personnel possédant l'expérience appropriée doit prendre une décision indiquant que les risques encourus sont clairement identifiés et acceptables pour l'Université. Le niveau d'expérience du personnel dépendra de la nature et de l'ampleur de la sous-traitance.

Lorsqu'un service est officiellement externalisé par l'Université, les normes et les attentes en matière de sécurité de l'information doivent faire partie intégrante du cahier des charges et du contrat mis en place.

6.1. Vérifications

Le processus de sélection d'un fournisseur de services doit inclure une vérification préalable du tiers en question, une évaluation des risques et un examen des conditions générales ; ceci afin de garantir que l'Université ne soit pas exposée à des risques sous-jacents. Ce processus peut impliquer les conseils de membres de l'Université experts en droit des contrats, en informatique, en sécurité de l'information, en protection des données à caractère personnel, en protection des données de recherche et de la propriété intellectuelle, et en ressources humaines. Ce processus doit également inclure la prise en compte de toute politique de sécurité des informations ou d'informations similaires disponibles auprès de la tierce partie.

6.2. Formalisation contractuelle

Tout sous-traitant ayant accès aux informations ou aux systèmes d'informations non publiques de l'Université doit accepter de respecter les règles de sécurité de l'information propres à l'Université. Les clauses de confidentialité doivent être utilisées lors de tout accord contractuel quand une tierce partie a accès aux informations non publiques de l'Université.

Les contrats doivent également contenir des accords de support avec les parties tierces, notamment en cas d'atteinte à la sécurité. Celles-ci comprendront des heures d'assistance, des contacts d'urgence et des procédures d'escalade.

Par ailleurs, tous les contrats de sous-traitance à l'Université doivent faire l'objet de contrôles afin de garantir qu'ils respectent les exigences requises en matière de sécurité de l'information. Ceux-ci doivent effectivement inclure des dispositions appropriées pour assurer la sécurité permanente des informations et des systèmes en cas de résiliation du contrat ou de transfert de ce dernier à un autre sous-traitant.

6.3. Règlement général sur la protection des données

Une évaluation des facteurs relatifs à la vie privée et à la protection des données à caractère personnel doit être réalisée au début de tout projet qui implique potentiellement l'accès à des données à caractère personnel par un tiers. Toute externalisation d'activité impliquant le transfert de données à caractère personnel à une tierce partie doit inclure l'acceptation des conditions standard de traitement des données à caractère personnel de l'Université.

Si la sous-traitance implique le transfert de données à caractère personnel en dehors de l'Espace économique européen (EEE) et des pays ayant fait l'objet d'une décision d'adéquation de la Commission européenne, le contrat doit inclure les clauses contractuelles types émises par la Commission européenne à moins que des règles d'entreprise contraignantes conformes à l'article 47 du RGPD n'aient été approuvées et couvrent ledit transfert.

6.4. Externalisation informelle

6.4.1. Externalisation informelle de données à caractère personnel

L'externalisation informelle de données à caractère personnel n'est pas autorisée.

Afin de minimiser les risques, les services informatiques mis à disposition par l'université doivent être préférés aux solutions extérieures.

Dans le cas où un besoin informatique ne peut être satisfait par les outils de l'Université, il convient de privilégier une solution approuvée par l'institution.

Toute nouvelle solution informatique impliquant des données à caractère personnel doit obtenir une validation de l'institution préalablement à son implémentation/utilisation.

Le personnel de l'Université n'est pas autorisé à configurer sa messagerie ULB de manière à transférer automatiquement le courrier entrant vers des services tiers avec lesquels l'Université n'a pas d'accord formel (ex : messagerie privée).

6.4.2. Externalisation informelle des données relevant de la propriété intellectuelle, littéraire ou artistique ou protégées par le secret professionnel

Il est formellement interdit de télécharger, diffuser, reproduire ou modifier des données dont les droits de propriété intellectuelle, littéraire ou artistique n'ont pas été respectés sans avoir préalablement obtenu l'autorisation des titulaires de ces droits.

Il est également formellement interdit de télécharger, diffuser, reproduire ou modifier des données protégées par le secret professionnel.

6.5. Accès physique par des tiers

Une évaluation des risques doit être effectuée avant de permettre à un service tiers l'accès à des zones sécurisées de l'Université, où des informations non publiques et des actifs peuvent être stockés ou traités. Cette évaluation doit prendre en considération :

- le matériel informatique auquel le tiers pourrait avoir accès ;
- les informations auxquelles il pourrait potentiellement accéder ;
- l'identité du tiers ;
- la nécessité ou non de superviser l'accès du tiers aux zones sécurisées ;
- les éventuelles mesures complémentaires visant à éviter des risques potentiels.

7. Responsabilités

La sécurité de l'information est l'affaire de tous. Experts en sécurité, membres du personnel IT, responsables hiérarchiques, responsables métiers, administrateurs systèmes, utilisateurs finaux… en partagent -à différents degrés- la responsabilité.

7.1. Respect des standards de sécurité

Chaque membre de la communauté universitaire a le devoir de respecter les standards de sécurité définit dans la PSSI et les règlements de l'ULB.

7.2. Mesures en cas de non-respect de la politique de sécurité

Les infractions mineures de la PSSI seront traitées par le COSI. Les supérieurs hiérarchiques peuvent en être informés, en fonction de l'impact sur les activités de leurs équipe ou selon le besoin de mesures disciplinaires de leur ressort.

Les infractions graves (ou les infractions mineures répétées) sont traitées conformément aux procédures disciplinaires de l'Université.

En cas de suspicion d'une activité suspecte qui pourrait nécessiter une ingérence dans la vie privée du travailleur (ex : vérifier le contenu des fichiers, ou les sites web visités par ce travailleur), la Commission de la protection de la vie privée à l'ULB doit être saisie.

Le cas échéant, les infractions pénales seront signalées à la police. Si l'infraction a eu lieu dans un pays autre que la Belgique, l'infraction peut être signalée aux autorités compétentes de ce pays.

8. Glossaire

Actifs

Le NIST (« National Institute of Standards and Technology »), qui est une des références en matière de sécurité des systèmes d'information, définit les actifs comme étant :

Tout élément de valeur pour la réalisation de la mission de l'organisation / des objectifs de l'entreprise. Les actifs ont des caractéristiques interdépendantes qui incluent la valeur, la criticité et la mesure dans laquelle ils sont utilisés pour atteindre la mission / les objectifs de l'entreprise. À partir de ces caractéristiques, des protections appropriées doivent être intégrées aux solutions utilisées par l'organisation. Un actif peut être tangible (élément physique, tel que matériel, logiciel, micrologiciel, plate-forme informatique, périphérique réseau ou autre composant technologique) ou immatériel (informations, données, marque, droit d'auteur, brevet, propriété intellectuelle, image ou réputation).

Anonymisation

L'anonymisation consiste à modifier les données de manière à rendre impossible la « ré-identification » des personnes concernées. Contrairement à la pseudonymisation (voir définition ci-dessous), l'anonymisation est, par définition, un processus irréversible.

Le recours aux techniques d'anonymisation et de pseudonymisation des données est à envisager dans le cadre de traitement de données à caractère personnel -à fortiori lorsqu'il s'agit de données sensibles- ne justifiant pas une identification formelle des personnes (ex : statistiques).

Chiffrement

Le chiffrement est un procédé qui consiste à modifier les données de manière à rendre leur compréhension impossible à toute personne n'ayant pas en sa possession la « clé » permettant le déchiffrement.

Il existe de nombreuses normes de chiffrement disponibles. Seules celles qui ont fait l'objet d'un examen public approfondi et qui se sont révélées efficaces peuvent être utilisées. Le service informatique peut, à la demande, fournir des conseils adaptés aux situations spécifiques.

Dans la plupart des cas, les clés de chiffrement se présentent sous la forme d'un mot de passe ou d'une phrase secrète. Perdre ou oublier la clé de chiffrement rendra les informations chiffrées inutilisables. Il est donc essentiel que les clés de chiffrement soient gérées efficacement. Lorsque les périphériques sont chiffrés par les services informatiques, ceux-ci sont responsables de la gestion sécurisée des clés. Dans tous les autres cas, il appartiendra à chaque utilisateur de gérer les clés. Il est conseillé d'effectuer des sauvegardes sécurisées de celles-ci et d'en stocker des copies chez des tiers de confiance.

Donnée

« Représentation d'une information sous une forme conventionnelle convenant au traitement par des moyens humains ou automatiques.

Note: le traitement inclut la communication et l'interprétation. »[19]

[19] Source: ISO/IEC 2382-16:1996, 16.01.03

Donnée à caractère personnel

Le RGPD définit les données à caractère personnel comme toute information se rapportant à une personne physique identifiée ou identifiable, c'est-à-dire qui peut être identifiée, directement ou indirectement.

Soulignons ici l'importance de l'identification indirecte : s'il est clair que des informations telles que le nom, l'adresse, la date de naissance, etc. sont des données à caractère personnel, il en va de même pour un numéro de plaque d'immatriculation, un numéro de lecteur ou de tout autre identifiant permettant d'identifier une personne physique de manière univoque.

Donnée sensible

Le RGPD définit des catégories particulières de données à caractère personnel, à savoir les données dites « sensibles » :

- les origines raciales ou ethniques ;
- les opinions politiques, les convictions philosophiques ou religieuses ;
- l'appartenance syndicale;
- les données relatives à la santé;
- les données relatives à la vie sexuelle ou à l'orientation sexuelle;
- les données relatives aux condamnations pénales et aux infractions;
- les données biométriques aux fins d'identifier une personne physique de manière unique ;
- les données génétiques.

Les données sensibles font l'objet d'un encadrement renforcé, aussi bien lors de leur collecte que dans leur traitement.

Information

« Connaissance concernant un objet tel qu'un fait, un événement, une chose, un processus ou une idée (y compris un concept), et qui, dans un contexte déterminé, a une signification particulière.

En théorie de l'information : connaissance qui réduit ou supprime l'incertitude concernant la réalisation d'un événement particulier appartenant à un ensemble déterminé d'événements possibles.

Note: en théorie de l'information, le mot "événement" a le sens qu'il prend dans le calcul des probabilités. Un événement peut être, par exemple:

- la présence d'un élément donné d'un ensemble;
- l'existence d'un caractère particulier, ou d'un mot particulier, dans un message déterminé ou dans une position déterminée d'un message;
- n'importe lequel des résultats possibles d'une expérience. »[20]

« Internet Of Things » (IOT)

L'« internet des objets » (plus souvent désigné par son acronyme anglais « IOT » pour « Internet Of Things ») désigne, selon la définition de Wikipédia, l'interconnexion entre Internet et des objets, des lieux et des environnements physiques. L'appellation désigne un nombre croissant d'objets connectés

[20] Source: ISO/IEC 2382-16:1996, 16.01.03

à Internet permettant ainsi une communication entre nos biens dits physiques et leurs existences numériques. Ces formes de connexions permettent de rassembler de nouvelles masses de données sur le réseau et donc, de nouvelles connaissances et formes de savoirs.

Dans la famille des IOT, on retrouve des objets du type : caméras de surveillance connectés, thermostats connectés, toutes sortes de capteurs connectés, etc.

Les objets de type IOT sont devenus des éléments primordiaux dans le domaine de la sécurité. En effet, très fréquemment, ces objets présentent de nombreuses failles de sécurité et il est relativement aisé pour un hacker d'en prendre le contrôle.

Un type d'attaque fréquent consiste à submerger un serveur de demandes de connections de telle sorte qu'il devienne pratiquement inaccessible au public légitime. Ce type d'attaque, appelé habituellement DDos (pour « Distributed Denial of Service attack ») fait en général usage d'un parc important d'objets de type IOT dont l'attaquant a pris le contrôle.

Pseudonymisation

Le RGPD définit la pseudonymisation comme le « traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ».

Le recours aux techniques d'anonymisation et de pseudonymisation des données est à envisager dans le cadre de traitement de données à caractère personnel -à fortiori lorsqu'il s'agit de données sensibles- ne justifiant pas une identification formelle des personnes (ex : statistiques).

Règlement Général sur la Protection des Données (RGPD)

Le Règlement Général sur la Protection des Données (RGPD) est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il est d'application depuis le 25 mai 2018.

Sécurité de l'information

La sécurité de l'information désigne « l'ensemble des moyens organisationnels, juridiques et humains mis en œuvre pour conserver ou rétablir la disponibilité, la confidentialité et l'intégrité de l'information et des systèmes informatiques sur lesquels pèsent différents types de menaces, résultant d'un acte de malveillance ou de circonstances accidentelles ».

9. Références

Les références utilisées dans la rédaction de ce document sont les suivantes :

Les Normes ISO – « famille » ISO 27 000 (https://www.iso.org/)

NIST – National Institute for Standards and Technology (https://www.nist.gov/)

SANS Institute (https://www.sans.org/)

Le standard de sécurité des systèmes d'information de l'Université de Stanford (https://uit.stanford.edu/security)

Le standard de sécurité des systèmes d'information de l'Université de Boston (https://www.bu.edu/tech/services/security/)

Un rapport préliminaire rédigé par Ataya & Partners

Un document rédigé par Alex Genatzy (CISO ULB)

SPF Économie (https://economie.fgov.be/fr/themes/line/securite-de-linformation

10. Auteurs

Genatzy, Alex – Responsable Sécurité des Systèmes d'information de l'ULB

Louies, Stéphane – Expert en Sécurité des Systèmes d'information, Département informatique

Rommelaere, Florence – Analyste, Département informatique

Révision

Doguet, Karin – Directrice, Département informatique

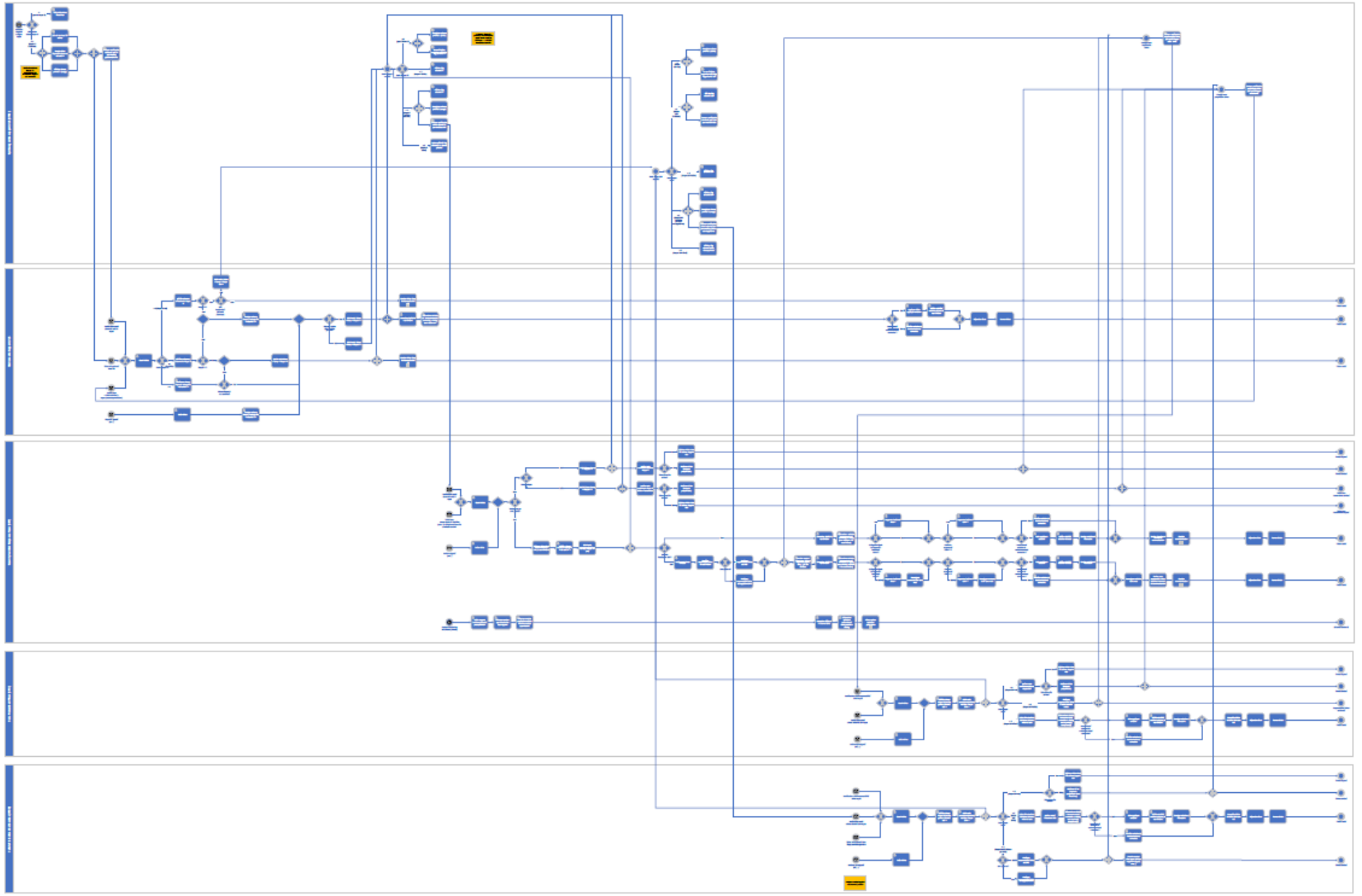
Grégoire, Virginie – Déléguée à la Protection des données de l'ULB

Markowitch, Olivier – Conseiller en Sécurité de l'ULB

Petropoulos, Petroula – Chargée de communication, Département informatique

11. Annexes

Processus de gestion des incidents de sécurité



Analyse de risques

Risque	Niveau du risque	Impact	Exemple
Perte de confidentialité	Niveau 0 > sans conséquence	Pas de gêne notable dans le fonctionnement ou les capacités de l'institution	Données publiques, visibles par tous
	Niveau 1 > gênes de fonctionnement	Diminution potentielle des capacités de l'institution	Données internes, dans un contexte de groupe de confiance, dont toutes les traces écrites sont protégées
	Niveau 2 > conséquences dommageables	Diminution potentielle des capacités de l'institution, avec des conséquences telles que des pertes financières, sanctions administratives ou réorganisation	Données confidentielles
	Niveau 3 > conséquences graves	Susceptible de provoquer une modification importante dans les structures et la capacité de l'institution comme la révocation de dirigeants, sa restructuration, des pertes financières	Données critiques/secrètes
Perte d'intégrité	Niveau 0 > sans conséquence	Pas de gêne notable dans le fonctionnement ou les capacités de l'institution	Aucune vérification de l'intégrité des données
	Niveau 1 > gênes de fonctionnement	Diminution potentielle des capacités de l'institution	Vérification des données, sans validation (des fautes d'orthographe sur une page web nuisent à l'image de marque de l'institution)
	Niveau 2 > conséquences dommageables	Diminution potentielle des capacités de l'institution, avec des conséquences telles que des pertes financières, sanctions administratives ou réorganisation	Données validées et contrôlées par des moyens techniques ou humains
	Niveau 3 > conséquences graves	Susceptible de provoquer une modification importante dans les structures et la capacité de l'institution comme la révocation de dirigeants, sa restructuration, des pertes financières	Données avec au moins deux niveaux de validation et de contrôle différents (techniques ou humains)
Indisponibilité	> 1 semaine	Services apportant un confort supplémentaire mais non indispensables	Imprimantes
	> 8h et ≤ 1 semaine	Ressources pour lesquelles il existe une alternative	Ressource documentaire
	> 2h et ≤ 8h	Sans conséquence vitale	Arrêt du réseau, de la messagerie…
	≤ 2h	Ressources mettant en péril la vie	Expériences biologiques ou physiques pilotées automatiquement, système de sécurité

Classification des données

	Description	Exemples
Données publiques	Données dont la divulgation, l'altération ou la destruction non autorisée entraine peu ou pas de risque pour l'institution ou les partenaires éventuels.	Éphémérides, catalogue des programmes, plans des campus, …
Données internes	Données dont la divulgation, l'altération ou la destruction non autorisée peut entrainer un risque modéré pour l'institution, les partenaires éventuels.	Procès-verbaux non confidentiels, communication générale, …
Données confidentielles	Données personnelles dont la divulgation, l'altération ou la destruction non autorisée peut entrainer un risque élevé pour l'institution ou les partenaires éventuels.	Documents soumis à la législation de la protection des données, notes confidentielles, procès-verbaux, informations confidentielles liées à la recherche ou à un financement, données financières (numéro de compte bancaire)…
Données critiques	Données personnelles sensibles. Données et informations institutionnelles confidentielles. L'utilisation de telles données peut entrainer des actions juridiques, pertes financières et des graves atteintes à la réputation de l'ULB ou d'un de ses collaborateurs.	Information relative à la santé mentale et physique d'un individu, données sous réserve d'une clause de confidentialité, identification biométrique, données relatives à l'appartenance syndicale…