CA du 12 DÉCEMBRE 2023
ANNEXE 31

Suivi des versions:

Version	Date de validation	Par	Modifications
v2			ORG-SSI : CIL => DPO, Présidence NOMAD_08 : Télétravail NOMAD_05 : Chiffrement des portables, antivirus de l'établissement
v1	02/06/2015	CA	Version initiale.

1. Politique, organisation, gouvernance

1.1. Objectif 1 : organisation de la SSI

Organisation SSI [ORG-SSI]

Pour conduire la politique de sécurité des systèmes d'information et faciliter sa mise en œuvre, l'Université de Lorraine, sous l'autorité de l'AQSSI (présidence), s'appuie sur une chaîne fonctionnelle interne spécialisée en SSI qui s'inscrit elle-même dans la chaîne fonctionnelle nationale animée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

La chaîne fonctionnelle SSI de l'Université de Lorraine est composée comme suit :

- du Directeur Général des Services, assisté du Fonctionnaire Sécurité Défense (FSD), le VP du Numérique et le Directeur du Numérique. Ils sont chargés de :
  - la préparation des mesures de défense, de vigilance et de prévention de crise ;
  - la gestion des situations d'urgence (plan Vigipirate, pandémies,...) ;
  - la protection du patrimoine scientifique et technique ;
  - l'exécution des plans de défense et de sécurité.
- des responsables de la sécurité des systèmes d'information (RSSI), nommés par l'AQSSI de l'Université de Lorraine. Correspondants auprès des structures nationales de la SSI, ils contribuent activement à l'élaboration d'une politique de sécurité cohérente et à sa mise en œuvre. Ils en assurent au sein de l'établissement le suivi de l'état. Ils ont pour mission :
  - participer au Comité Sécurité du Système d'Information, dans le cadre de l'élaboration de la Politique de SSI de l'Université de Lorraine ;
  - constituer et coordonner un réseau interne de correspondants de sécurité (CSSI)
  - contrôler régulièrement le niveau de sécurité du système d'information par l'évaluation des risques résiduels et en rendre compte au COPIL Sécurité ;
  - informer et sensibiliser les utilisateurs du système d'information aux problématiques de sécurité ;
  - évaluer et ajuster le niveau de sécurité des systèmes d'information, afin de garantir une sécurité adéquate au regard des missions et des enjeux ;
  - effectuer une étude des besoins de sécurité des nouveaux projets, exprimés en termes de disponibilité, de confidentialité et d'intégrité des données ;

- prévoir en liaison avec le DPO de l'établissement, la sensibilisation de tous les utilisateurs aux aspects sécurité des données à caractère personnel ;

- être l'intermédiaire entre les différents intervenants en cas d'incident de sécurité et évaluer la gravité des incidents et la nécessité d'alerter la gouvernance de l'établissement ;

- exploiter et relayer les informations relatives à la sécurité reçues via le CERT RENATER, le CERT-FR et toute structure liée à la sécurité.

- Au sein du comité de sécurité opérationnelle les RSSI participent activement à l'élaboration des référentiels de sécurité, à leur mise en œuvre et leur suivi.

- des correspondants de la sécurité des systèmes d'information (CSSI), leur rôle - en liaison avec les RSSI - est la mise en œuvre de la SSI au niveau de leur périmètre thématique et/ou structurel. En particulier :

- mettre en œuvre la PSSI de l'Université de Lorraine ;

- veiller à la mise en place des mesures de sécurité nécessaires ;

- veiller à l'application des instructions et recommandations SSI transmises par les RSSI ;

- veiller à la bonne exploitation des avis des CERT RENATER et CERT-FR ;

- vérifier l'application des mesures de sécurité (mises à jour des OS, etc.) sur les infrastructures et dans les projets de SI (analyse de risque, etc.) ;

- signaler tout incident de sécurité, gérer les alertes et incidents en lien avec les RSSI ;

- veiller à la prise en compte de la sécurité dans la rédaction des contrats de sous-traitance et les cahiers des charges des applications, et l'installation de tout nouvel équipement ;

- veiller au respect des formalités requises par la loi Informatique et Libertés pour les traitements de données à caractère personnel ;

- sensibiliser les utilisateurs à la SSI.

- du délégué à la protection des données (DPO) désigné par l'AQSSI qui veille à la bonne application de la loi « Informatique et Libertés » dans l'établissement. Il doit établir et maintenir un registre des traitements mis en œuvre.

Identification des acteurs SSI [ORG-ACT-SSI]

L'organisation SSI de l'État s'appuie sur des acteurs SSI clairement identifiés, à tous les niveaux d'organisation de l'État. Les acteurs responsables en matière de SSI pour la protection du secret de la défense désignés dans l'IG11300, et les agents chargés de les assister dans cette mission, sont responsables de la mise en application générale de la politique SSI de l'État Ils sont référencés dans un annuaire interministériel. Cette chaîne fonctionnelle s'appuie, pour chaque ministère, sur le HFDS, assisté par un fonctionnaire de sécurité des systèmes d'information (FSSI).

Formalisation des responsabilités [ORG-RESP]

Une note d'organisation fixe la répartition au sein de chaque entité et au niveau local des responsabilités et rôles en matière de SSI. Cette note sera, le plus souvent, proposée par le RSSI et validée par l'autorité qualifiée.

Définition et pilotage de la PSSI [ORG-PIL-PSSIM]

La Politique de Sécurité des Systèmes d'Information de l'établissement est établie sous la responsabilité de l'AQSSI. Cette politique reprend le socle commun établi par la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE). La Commission du Numérique est chargée de sa mise en place, de son évolution, de son suivi et de son contrôle.

Application de l'instruction dans l'entité [ORG-APP-INSTR]

Les RSSIs planifient les actions de mise en application de la PSSI. Ils rendent compte régulièrement de la mise en application des mesures de sécurité auprès de leur autorité qualifiée et du FSD.

Formalisation de documents d'application [ORG-APP-DOCS]

Le RSSI formalise et tient à jour les documents d'application, approuvés par l'autorité qualifiée, permettant la mise en oeuvre des mesures de la PSSIE sur son périmètre.

2. Ressources humaines

2.1. Objectif 2 : ressources humaines

Responsabilités génériques [PER_01]

Un ensemble de chartes d'usage et de sécurité des systèmes d'information, destinées aux différentes populations utilisatrices du système d'information (personnels administratifs, enseignants, chercheurs, et étudiants de l'Établissement), précise les droits, devoirs et responsabilités qui incombent à tout utilisateur du système d'information en matière de sécurité :

- Règles d'utilisation des outils (poste de travail bureautique ou nomade) et des services génériques (messagerie, Intranet…) mis à la disposition de chacun.
- Règles de protection des biens.
- Responsabilités de l'utilisateur vis-à-vis de la sécurité[1].

Manquement aux exigences [PER_04]

Les chartes utilisateurs définissent les conditions d'usage du système d'information en termes de sécurité. Les chartes informent les utilisateurs des contrôles effectués et mentionne le processus disciplinaire (rappel aux bonnes pratiques, sanction administrative, poursuite pénale…) mis en œuvre en cas de d'infraction aux règles de sécurité[1].

Aspects Sécurité dans les contrats [PER_06]

Pour le personnel de la fonction publique, la soumission au devoir de réserve est rappelée dans le contrat. Les sanctions en cas de manquement à l'obligation de réserve le sont également.

[1]Document : Charte Informatique

[1]Document : Charte Informatique

Information du personnel [PER_07]

Les droits, les devoirs et les responsabilités associées à chaque poste en matière de Sécurité du Système d'Information sont communiqués à toute personne lors de sa prise de fonction ou d'un changement de poste.

Un document (charte ou procédure), fourni à chaque membre du personnel, l'informe des consignes de sécurité à respecter dans le cadre des tâches qu'il exécute au sein de l'établissement.

L'information du personnel concerne à la fois les personnels de l'établissement (personnels administratifs, les enseignants, les chercheurs), mais aussi les étudiants, tiers et contractants.

Sensibilisation des personnels [PER_08]

Il est important que chaque personne impliquée dans le traitement d'informations sensibles de l'établissement soit sensibilisée aux enjeux de « sécurité » et soit formée de manière à pouvoir gérer les mesures de sécurité qui lui incombent.

Des sessions d'information à la sécurité sont assurées périodiquement afin de maintenir la sensibilisation des personnels administratifs, enseignants, chercheurs, et étudiants, sur les bonnes pratiques de sécurité ou sur les règlements en vigueur.

Des formations spécifiques sont réalisées pour les personnels dont les fonctions requièrent une sensibilisation particulière en termes de sécurité (personnels liés à la DSI, chercheurs).

Disponibilité des personnes critiques [PER_09]

Une gestion adaptée des ressources humaines est mise en place de manière à ce qu'il n'y ait pas de vacance sur un poste critique qui puisse impacter la sécurité, ou induire une indisponibilité incompatible avec les objectifs de sécurité retenus. Il convient en particulier que les ressources affectées soient en cohérence avec les objectifs en matière de disponibilité.

3. Gestion des biens

3.1. Objectif 3 : cartographie des SI

Plan de classification [GDB_01]

Un plan de classification est défini au niveau de l'établissement pour hiérarchiser les niveaux de protection et gérer les biens conformément aux besoins de sécurité identifiés.

Ce plan de classification définit les échelles de sensibilité à partir des critères confidentialité, intégrité, et disponibilité.

Identification et inventaire des biens sensibles [GDB_02]

On qualifie de « bien sensible » toute composante qui traite d'information ou de fonction de niveau 2 selon le plan de classification. On appelle « critique » un bien supérieur au niveau 3 selon le plan de classification.

Les biens sensibles participant au fonctionnement du système d'information (informations, biens logiciels, biens physiques, services, etc.) sont inventoriés par domaine. Chaque bien recensé fait

l'objet d'une identification renseignant le niveau de classification (établi sur la base du plan mentionné ci-dessus), son détenteur ou responsable, et les personnes qui y ont accès (pour les données).

Un extrait de l'inventaire est réalisé afin d'identifier les biens « critiques » parmi l'ensemble des biens constituant le système d'information de manière à pouvoir protéger les éléments vitaux de l'organisme identifiés en cas de sinistre majeur.

3.2. Objectif 4 : qualification et protection de l'information

Marquage des biens [GDB_03]

Les biens sensibles sont marqués selon leur sensibilité en confidentialité telle que définie par le plan de classification.

Ce marquage s'applique aux informations, aux fichiers les contenant dans la mesure du possible (entêtes ou pieds de page par exemple), comme aux biens physiques contenant ces informations (supports électroniques, documents imprimés, serveur de données, local informatique, armoires, etc…).

Le marquage peut consister dans certains cas à associer à un local ou à un serveur, un message d'avertissement de restriction d'accès.

Toute information non marquée est considérée comme publique.

Responsabilités dans l'utilisation des biens sensibles [GDB_07]

Chacun (personnel administratif de l'Établissement, enseignant, chercheur, étudiant, tiers,) est responsable de l'utilisation qu'il fait des biens sensibles et veille à respecter les règles d'utilisation propres à chaque niveau et critères de sensibilité. Tout manquement à ces règles d'utilisation fait l'objet de sanctions. Toute irrégularité constatée est signalée.

Utilisation des biens sensibles [GDB_08]

Tout matériel n'appartenant pas à l'établissement et n'étant pas géré par les équipes d'exploitation du SI, est considéré comme un composant externe (PC, clé USB, équipement réseau,…).

Toute connexion de matériels externes au réseau de l'établissement est soumise à un accord préalable de la DN.

Tout matériel appartenant à l'Établissement et géré par les équipes d'exploitation du SI respecte les règles d'exploitation définies. En particulier, les droits d'administration pour les utilisateurs ne sont pas autorisés sauf dérogation justifiée validée par la hiérarchie et acceptée par la DN.

4. Intégration de la SSI dans le cycle de vie des systèmes d'information

4.1. Objectif 5 : risques

La sécurité est prise en compte à toutes les étapes du cycle de vie d'un projet, interne ou externe, lié au système d'information. Les applications informatiques sont sécurisées, en cohérence avec la sensibilité des informations traitées et échangées.

Étude et dossier de sécurité [PDM_01]

Une identification préalable des projets sensibles (manipulant des données sensibles ou des données personnelles, soumis à des contraintes réglementaires, ou présentant de forts besoins de disponibilité) est réalisée pour identifier les enjeux et les risques.

Tout nouveau projet sensible, ou tout projet ayant de fortes interactions avec le système d'information existant, est précédé d'une étude de sécurité permettant de formaliser les exigences de sécurité à mettre en œuvre. Le Comité de Sécurité Opérationnelle valide les résultats de l'étude.

Formalisation et documentation [PDM_02]

L'analyse de sécurité s'appuie sur une méthode et un processus formalisés et documentés. Elle est reprise dans un dossier de sécurité qui accompagne le projet sensible et sera complété au fur et à mesure de l'avancement de celui-ci.

4.2. Objectif 6 : maintien en condition de sécurité

Gestion et contrôle des opérations de maintenance [MAINT_01]

Les opérations de maintenance sont documentées (périmètre, actions…) et planifiées en concertation avec les utilisateurs.

Des mesures sont prises (par exemple des tests de non régression) pour vérifier que l'opération de maintenance réalisée n'a pas altéré le système opérationnel.

Un retour en arrière en cas de dysfonctionnement constaté ou d'altération des données faisant suite à l'opération de maintenance réalisée doit toujours être possible.

Les actions de maintenance sont effectuées de préférence localement.

Une présence constante auprès des mainteneurs est assurée pendant que ceux-ci opèrent localement.

Les opérations effectuées au titre des opérations de maintenance sont tracées et journalisées. Un compte-rendu des opérations est systématiquement rédigé.

Télémaintenance [MAINT_02]

Les services de télémaintenance sont systématiquement encadrés par des accords contractuels qui précisent les conditions dans lesquelles sont effectuées les opérations de télémaintenance.

Les accès de télémaintenance (comptes dédiés, accès réseau) sont fermés en dehors des périodes de télémaintenance. Ils sont ouverts à la demande des télémainteneurs et à l'initiative des exploitants du système télémaintenu et sont fermés à la fin de toute opération de télémaintenance.

Il convient de s'assurer, via les conditions d'emploi, que les télémainteneurs informent systématiquement les exploitants de la fin de chaque opération de maintenance afin de leur permettre de fermer les accès.

Les opérations de télémaintenance sont tracées et journalisées. Elles font l'objet d'un contrôle a posteriori systématique.

Procédure de gestion des changements [GCH_01]

L'établissement dispose d'une procédure formelle et documentée de gestion des évolutions continues du système d'information.

Dans le cadre de cette procédure, toute évolution de l'infrastructure support implique une analyse sur le plan de la sécurité des applications supportées.

Mise en œuvre des évolutions logicielles majeures [GCH_02]

Les évolutions logicielles majeures sont planifiées. Elles sont testées avant leur mise en œuvre effective. Une procédure de repli est systématiquement définie.

4.3. Objectif 7 : produits et services qualifiés ou certifiés

Acquisition de produits et services de confiance [INT-AO-PSL]

Lorsqu'ils sont disponibles, des produits ou des services de sécurité labellisés (certifiés, qualifiés) par l'ANSSI doivent être utilisés.

4.4. Objectif 8 : maîtrise des prestations

Formalisation des services et des échanges applicatifs [EDI_01]

Les services et les échanges applicatifs mis à la disposition de tiers comme l'utilisation de services tiers externes sont définis dans le cadre de projets qui incluent une analyse sécurité permettant :

- D'identifier les connexions et flux de données nécessaires sur un plan fonctionnel ou technique.
- De déterminer leurs besoins de sécurité (confidentialité, intégrité, authenticité, non-répudiation).
- D'évaluer la menace et les risques induits.

- De sélectionner des contre-mesures permettant de ramener ces risques à un niveau acceptable.

Autorisation d'accès [EDI_02]

L'ouverture d'un accès pour un tiers est soumise à autorisation et nécessite la signature d'un accord préalable entre ce tiers et l'Établissement. Il en est de même pour tout accès à un service tiers externe. Ces accords contractuels incluent l'aspect sécurité et définissent les procédures à respecter.

Contrôle des accès et protection des échanges [EDI_03]

Le tiers – système, applicatif ou utilisateur – accédant au système d'information de l'établissement, est identifié et authentifié. L'utilisation d'un protocole sécurisé (SSL, SSH) ou d'une liaison garantissant cette identité (LS, VPN) est recommandée. L'autorisation et les moyens cryptographiques utilisés sont soumis à validation par le Comité de Sécurité Opérationnelle.

Des mesures de sécurité spécifiques sont mises en œuvre en fonction de la sensibilité des informations échangées (chiffrement, scellement, signature…).

Les connexions établies et les échanges réalisés sont tracés, journalisés et régulièrement audités.

Mise au rebut et recyclage en fin de projet [PDM_11]

Une procédure décrit les précautions à prendre lors de la mise au rebut ou du recyclage de tout support d'information.

Des moyens techniques sont mis à disposition des administrateurs pour assurer :

- Une destruction sécurisée des documents relatifs au projet.
- Un effacement sécurisé ou une destruction physique des disques durs et des supports informatiques ayant contenu des données sensibles.

La destruction peut être réalisée par effacement, broyage, ou par enlèvement par une société spécialisée.

Réaffectation des matériels en fin de projet [PDM_12]

Préalablement au recyclage, à l'attribution à un nouveau propriétaire ou à la réaffectation d'un poste de travail ou d'un équipement matériel, les informations sensibles sont effacées de manière à ce qu'il ne soit pas possible de les récupérer ; les logiciels sous licence sont désinstallés.

L'effacement des supports ayant contenu des données est réalisé à l'aide d'une solution agréée par le comité de sécurité opérationnelle, adaptée à la sensibilité de ces données.

Hébergement des données [INT-REX-HB]

L'hébergement des données sensibles de l'administration sur le territoire national est obligatoire, sauf accord du HFDS, et dérogation dûment motivée et précisée dans la décision d'homologation.

5. Sécurité physique

5.1. Objectif 9 : sécurité physique des locaux abritant les SI

Définition des périmètres de sécurité physique [PHY_01]

Afin d'empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux et informations, des périmètres de sécurité sont définis. La définition des zones est adaptée au contexte d'utilisation des locaux de l'Établissement et à leur accès par les différentes catégories de personnes.

- Zone 0 : zone accessible à toute personne
- Zone 1 : zone destinée à l'accueil du public, des étudiants : locaux destinés aux enseignements (salle de cours, de travaux pratiques, bibliothèque,…), et aux fonctions administratives avec le public.
- Zone 2 : zones réservées aux personnels administratifs, personnels enseignants, personnels chercheurs (laboratoires). Zones non accessibles au public.
- Zone 3 : zone sensible donnant accès aux bureaux de personnes à responsabilité ou titulaires de postes de confiance, aux plateformes de développement.
- Zone 4 : zones dédiées aux équipements informatiques (serveurs, calculateurs), réseau et postes sensibles. Il doit s'agir de bâtiments ou de locaux dédiés, protégés par contrôle d'accès spécifique.

Protection physique et environnementale des matériels [PHY_02]

La localisation des équipements dans les zones est adaptée à la sensibilité des informations qu'ils supportent et du besoin de disponibilité du service qu'ils fournissent.

Les matériels sensibles sont situés dans des zones de niveau 3 ou 4.

Travail dans les zones sécurisées [PHY_03]

L'intervention des personnels dans les zones sécurisées (zone 3 et zone 4) est encadrée par des procédures, prenant en compte notamment les points suivants :

- Modalités d'accès des personnes, et en particulier de visiteurs
- Interventions de prestataires et de sociétés externes (maintenance,...)
- Autorisations de travail isolé

5.2. Objectif 10 : sécurité physique des centres informatiques

Mise en œuvre des contrôles d'accès physiques [PHY_04]

Des moyens de protection contre les accès physiques sont définis et mis en œuvre pour chacune des zones :

- Le mode de contrôle d'accès physique est défini : aucun contrôle (zone 0-1), présentation visuelle d'un moyen d'identité (carte étudiant, carte d'identité, port de badge) (zones 2), sas, portes verrouillées, lecteur de badge électronique, digicode, (zones 3 et 4)
- Les horaires autorisés d'accès sont définis : par zone, locaux et par catégorie de personnes
- Les modalités d'enregistrement d'accès aux zones sont définis : aucun, registre papier, fichier informatique, vidéo,…
- Le mode de surveillance et d'alarme est défini : ronde gardien, détection d'ouverture de porte, vidéosurveillance, alarme volumétrique, …

A partir de la zone 3, des moyens de contrôles d'accès permettent de limiter les accès à des groupes de personnes définies, et des contrôles d'accès individuels sont mis en œuvre.

A partir de la zone 4, des contrôles d'accès individuels sont mis en œuvre, avec identification de la personne.

Gestion des autorisations d'accès physique [PHY_05]

Les conditions d'accès aux différentes zones sont définies.

Des autorisations individuelles sont mises en œuvre pour l'accès aux zones sensibles (3 et 4).

Les demandes d'autorisation d'accès en zone 4 sont, de plus, validées par le responsable de la DN (ou le responsable de la zone). Les accès sont accordés sur la base de ces demandes formalisées et motivées en fonction du besoin d'en connaître. Les demandes d'accès sont archivées.

Accueil des visiteurs [PHY_07]

Les zone 0 et 1 sont en circulation libre pour les visiteurs.

Des conditions d'accompagnement des visiteurs en zones 2 sont définies.

Une procédure décrit les modalités permettant d'autoriser l'accès dans les zones sécurisées (zone 3 et zone 4) aux visiteurs présentant un besoin. Cette procédure prend en compte notamment les points suivants :

- Contrôle de l'identité des visiteurs
- Traçabilité des visites (registre)
- Information des visiteurs sur leurs responsabilités et sur les enregistrements (vidéo, registres)
- Accompagnement des visiteurs dans la zone par une personne autorisée

Sortie d'un matériel [PHY_09]

En zone 2 et au-delà, des règles et procédures de sortie de matériel sont formalisées et documentées. Elles prennent en compte la sensibilité des informations contenues dans ce matériel et formalisent les mesures à suivre en dehors des locaux pour assurer la protection des biens de l'entreprise en dehors des locaux.

En zone 2 et au-delà, toute sortie de matériel sensible est enregistrée et préalablement autorisée.

Destruction des biens sensibles [PHY_10]

Les procédures de mise au rebut des biens sensibles sont formalisées et communiquées à l'ensemble du personnel présentant un besoin d'en connaître

La mise au rebut des supports papiers contenant des informations sensibles est réalisée au moyen d'une déchiqueteuse ou d'incinérateurs. La conservation des documents est effectuée en lieu sûr avant leur destruction.

La mise au rebut des supports électroniques est réalisée de manière sécurisée : par effacement sécurisé, par broyage, incinération ou par enlèvement par une société spécialisée. La conservation des matériels est effectuée en lieu sûr avant destruction.

Localisation des matériels [PHY_11]

Les matériels du système d'information, présentant une valeur attractive, fragiles, ou supports d'information sensibles sont disposés dans des emplacements appropriés garantissant leur sécurité (imprimantes, vidéoprojecteurs, ordinateurs libre-service, serveur de données, etc…).

Notamment ces matériels sont entreposés dans des salles ou armoires fermées à clés en absence des personnes responsables, disposent d'équipement anti-vol, de marquage indélébile en empêchant la revente, etc…

Surveillance des locaux informatiques [PHY_14]

Des rondes sont régulièrement effectuées sur les zones de niveau 4.

5.3. Objectif 11 : sécurité du SI de sûreté

Gestion des données de vidéoprotection [PHY_13]

La rétention des données de vidéosurveillance est effectuée sur une fenêtre d'un mois glissant. Les vidéos de surveillance sont conservées sur un système isolé dont la console d'exploitation est restreinte aux seules personnes habilitées.

Adéquation des équipements d'infrastructure [INFRA_01]

Tout site de zone 4 dispose des équipements d'infrastructure nécessaires au fonctionnement des moyens informatiques du site et à leur sécurité : climatisation (climatiseurs, arrivées d'eau…), équipements de protection incendie (sprinklers, extincteurs…), alimentation électrique (onduleurs, groupes électrogènes, arrivées électriques…), moyens de télécommunication (PABX, lignes…).

Le dimensionnement des équipements d'infrastructure mis en œuvre permet d'assurer le bon fonctionnement des moyens informatiques et réseaux du site comme de leur sécurité.

Maintenance des équipements d'infrastructure [INFRA_03]

Les équipements d'infrastructure sont couverts par des contrats de maintenance et si nécessaire par des contrats de services permettant d'assurer la disponibilité du service rendu par ces équipements.

Protection des câbles [INFRA_04]

Les salles informatiques disposent de faux planchers ou de goulottes appropriées permettant un passage sécurisé des différents câblages.

Un plan de câblage est formalisé.

6. Sécurité des réseaux

6.1. Objectif 12 : usage sécurisé des réseaux nationaux

Passerelles Internet et de sécurité [NET_01]

Des équipements d'infrastructure sont mis en place afin de protéger et d'isoler les réseaux internes vis-à-vis de l'extérieur.

Cette utilisation de passerelles a pour but de faciliter la gestion de la sécurité réseau tout en limitant les risques qui proviendraient de la multiplicité et de la variété des moyens d'échange et d'accès.

Plan d'adressage [NET_02]

Le plan d'adressage est classifié comme sensible.

Partitionnement des réseaux [NET_05]

Le LAN interne est partitionné en sous-réseaux afin d'assurer un isolement des « branches sensibles » et de permettre de confiner, si besoin est, une branche réseau en cas d'incident. Les connexions sont filtrées et un contrôle d'accès activé au niveau d'un sous-réseau.

L'accès au LAN serveur Gestion (SIG) est explicitement réservé :

- au LAN interne de Gestion (administration)
- au LAN interne des Services Numérique de Gestion
- au réseaux privés virtuels (VPN) de gestion

Du fait de la règle (NET_04), les accès externes aux réseaux internes de Gestion (administration) sont interdits.

Isolement des réseaux sensibles [NET_06]

Sont considérés comme réseaux sensibles :

- les réseaux hébergeant des serveurs ou applications contenant des informations sensibles ou des processus métier sensibles, tels que les serveurs d'applications en production, les serveurs de sécurité (annuaire, firewall, proxy, serveur d'authentification), les serveurs de sauvegarde, les réseaux de gestion d'infrastructures.
- les réseaux pour lesquels la sécurité n'est pas connue ou maîtrisée par l'établissement (réseaux d'un partenaire, d'un laboratoire, application non maîtrisée). Il convient de cloisonner les réseaux sensibles vis-à-vis du LAN interne par des mesures de sécurité réseau (pare-feu, antivirus, proxy, VLAN, authentification…).

Tout accès depuis un réseau extérieur sur une machine connectée à un réseau de l'Établissement est soumis à autorisation et validé de manière formelle en cohérence avec la politique d'accès de l'Établissement.

Contrôle des accès réseau [NET_22]

Tout flux de communication (flux et protocoles réseau) entrant et par défaut interdit. L'autorisation d'accès est fournie sous la responsabilité des personnes a qui est confié la gestion du LAN.

L'accès à Internet est individualisé et authentifié et donne lieu à journalisation des accès.

Protection des flux réseau [NET_23]

Tout échange entre l'Établissement respecte le principe du moindre privilège.

Les règles relatives aux flux d'informations sont :

- Tout flux d'information établi entre l'Établissement et un réseau dit « non sûr » transite obligatoirement par une plate-forme d'interconnexion approuvée par le RSSI.
- Les flux échangés entre l'Établissement et l'extérieur sont maîtrisés, surveillés et réduit au strict minimum.
- Tout flux d'un niveau de sensibilité donné est protégé (chiffrement, scellement, signature,) lorsqu'il transite via un réseau ayant un niveau de sensibilité inférieur. Par exemple l'accès aux serveurs de gestion depuis un réseau de recherche.

6.2. Objectif 13 : usage sécurisé des réseaux locaux.

Par équipements non maîtrisés par l'établissement, on entend les équipements réseau (modems, routeurs, etc.) voire de sécurité (ces équipements peuvent contenir des fonctions de sécurité) mis en œuvre ou administrés par des tiers (Ces tiers sont généralement des opérateurs de

télécommunication. Ces équipements peuvent être la propriété de l'établissement ou de ces tiers. Leur installation peut être faite sous la responsabilité de l'établissement ou de ces tiers.

Identification des matériels en réseau [CA_07]

Seuls les matériels autorisés peuvent se connecter aux réseaux internes qualifiés de sensibles (réseau de gestion). Le contrôle est réalisé par authentifiant, adresse IP ou adresse Mac dans un réseau d'administration, ou à partir de réseaux virtuels chiffré (VPN).

Cloisonnement des réseaux [NET_04]

Des zones ou périmètres de sécurité sont définies afin de cloisonner le système d'information en périmètres de niveaux de confiance homogènes différents.

Les réseaux de l'établissement sont séparés, en réseaux **Recherche, Gestion, Pédagogie, Services Numériques, Périphériques**.

Ces réseaux peuvent être séparés en LAN interne et LAN serveurs. Les LAN serveurs peuvent être privés (dédiés aux LAN internes) ou accepter des connexions externes (DMZ).

Lorsqu'un LAN serveur existe, les accès externes au LAN interne sont interdits ou nécessitent un accès VPN.

Identification des équipements non maîtrisés [NET_20]

Il convient d'identifier et répertorier les équipements réseau et de sécurité non maîtrisés par l'établissement. Leur utilisation fait l'objet d'une étude de sécurité et d'une autorisation préalable à leur installation.

Protection de sécurité des équipements non maîtrisés [NET_21]

En l'absence d'un contrat spécifique prenant en compte la sécurité, il convient de considérer comme inexistantes les fonctions de sécurité disponibles sur les équipements non maîtrisés par l'établissement.

Les mesures de sécurité ne doivent pas reposer sur celles proposées par les équipements non maîtrisés, tels que fournis par les services des Fournisseurs d'Accès Internet (sauf contractualisation spécifique).

Il convient de doubler tout équipement non maîtrisé par l'établissement pouvant avoir un impact potentiel négatif pour la sécurité, par un équipement réseau ou de sécurité permettant de contrer les risques identifiés.

Autorisation d'accès à Internet [INET_01]

L'accès au réseau Internet (web) est systématiquement autorisé. Il peut être retiré sur demande de la hiérarchie ou de la DN en cas de violation des règles d'usage du service. L'accès alloué est personnel. Il est essentiellement réservé à un usage professionnel. Les utilisations de cet accès sont tracées et journalisées et font l'objet d'un examen périodique.

Diffusion des règles d'accès et d'utilisation [INET_02]

Les règles régissant la navigation sur Internet et l'utilisation des outils de communication sont formalisées dans une charte utilisateur, diffusées à l'ensemble du personnel, connues et acceptées. Elles sont notamment rappelées lors des sessions de sensibilisation à la sécurité[1].

6.3. Objectif 14 : accès spécifiques

Par infrastructure réseau, on entend les équipements matériels et logiciels, le câblage, les prises réseaux.

Sécurisation des équipements d'infrastructure réseau [NET_17]

Les configurations des équipements d'infrastructure réseau bénéficient de mesures de durcissement

Des procédures de durcissement sont définies et appliquées. Elles concernent a minima les aspects :

- Sécurisation de l'accès, contrôle d'accès logique à l'interface d'administration
- Désactivation des ports et services non utilisés (telnet, rlogin, ftp, etc…)
- Sélection des composants logiciels, désactivation des utilitaires et paquetages non utilisés
- Gestion des comptes et privilèges d'administration
- Mises à jour des correctifs de sécurité
- Activation des traces d'audit
- Stratégie de sécurité (mot de passe, verrouillage)

Protection du câblage et des prises réseau [NET_18]

Les prises réseau sont identifiées et localisées, et seules les prises utilisées sont brassées. L'accès aux panneaux de raccordement et aux tableaux de brassage est contrôlé. L'accès aux têtes de ligne est contrôlé et protégé. Les câbles de l'infrastructure réseau sont protégés contre les risques d'interception ou de dommage.

Disponibilité des équipements réseau [NET_19]

Les équipements d'infrastructure critiques (tels que les routeurs, les commutateurs fédérateurs) sont dupliqués ; à défaut, des matériels de remplacement sont disponibles.

[1]Document : Charte Informatique

6.4. Objectif 15 : usage sécurisé des réseaux sans fil

Utilisation du Wifi dans l'établissement [WIFI_01]

L'accès aux points de connexion WiFi est contrôlé, et réservé aux seuls utilisateurs autorisés. Des mesures d'authentification des utilisateurs accédant aux points d'accès Wifi, et des mesures de chiffrement des flux Wifi sont réalisées en fonction du besoin.

Utilisation de réseau wifi non chiffré [WIFI_02]

Lors de l'utilisation de réseau wifi non chiffré : réseau ouvert ou "portail captif" avec authentification dans un navigateur. Il est impératif de transmettre les informations sensibles uniquement avec des protocoles chiffrés et de vérifier la validité des certificats.

6.5. Objectif 16 : sécurité des mécanismes de commutation et de routage

Journaux des opérations d'administration et d'exploitation des réseaux [NET_10]

Les opérations sensibles d'administration sont tracées et journalisées, au moyen de rapports d'intervention pour les opérations physiques, via l'enregistrement des connexions pour les opérations logiques.

Les journaux sont sauvegardés et conservés pendant une période adaptée aux besoins de suivi et contrôle, en respectant les exigences réglementaires.

Dimensionnement des réseaux [NET_11]

Il convient de surveiller les activités réseaux et de s'assurer que l'infrastructure réponde aux besoins de disponibilité, de dimensionnement et de qualité de service de l'Établissement.

Contrôle d'accès logique aux équipements réseau [NET_12]

Un contrôle d'accès logique aux équipements réseaux est mis en œuvre.

Les mots de passe constructeur par défaut sur les équipements sont systématiquement modifiés. Si possible, des comptes d'administration et de supervision nominatifs sont créés. Les mots de passe sont régulièrement modifiés.

Il est régulièrement procédé à un contrôle des accès aux équipements réseau et des droits alloués aux administrateurs et aux exploitants.

Protection de l'administration réseau [NET_13]

L'administration et la supervision des réseaux sont effectuées depuis des réseaux et des équipements dédiés.

L'accès aux ports (physiques et logiques) d'administration et de supervision est contrôlé et limité aux équipements ou réseaux dédiés.

Surveillance continue de l'activité sur les réseaux [NET_14]

La DN assure une surveillance continue des réseaux sous sa responsabilité.

Cette surveillance porte notamment sur :

- Le contrôle du bon fonctionnement des réseaux.
- Le contrôle de la charge des réseaux et de leur disponibilité.
- L'utilisation réalisée au travers des réseaux.

Cette surveillance s'appuie sur des moyens dédiés et protégés, qui sont éventuellement partagés avec ceux utilisés pour l'administration et l'exploitation des systèmes et des réseaux.

Journalisation des événements réseau [NET_15]

Des dispositifs d'audit sont mis en place qui permettent l'enregistrement dans des fichiers de traces (dits journaux d'audit) des principaux événements liés à la sécurité des réseaux.

Cette journalisation porte notamment sur les événements suivants :

- Les anomalies pouvant être révélatrices d'un incident de sécurité.
- Les atteintes à la sécurité : détections de virus, tentatives d'intrusion, erreurs de connexion…
- L'activité des personnes en charge de l'exploitation des réseaux : configuration et paramétrage des équipements de communication, gestion des habilitations et des droits d'accès…
- Les événements liés à : accès réseau, sites consultés, volumétrie des échanges, connexions des nomades…

Les journaux d'audit sont systématiquement revus afin de détecter les problèmes de sécurité. Les événements révélateurs d'un possible problème de sécurité sont analysés quotidiennement. Les autres événements (traces d'activités de gestion ou d'utilisation des SI par exemple) sont revus sur une base hebdomadaire.

Conservation des journaux réseau [NET_16]

Les journaux d'audit sont des biens sensibles, qui sont sauvegardés et protégés. Ils sont conservés pendant une période suffisante pour répondre aux besoins opérationnels tout en satisfaisant les exigences légales, réglementaires ou contractuelles.

Analyse des flux réseau [NET_24]

Tous les flux réseaux sont analysés par un mécanisme de contrôle (tels qu'un antivirus), et, si nécessaire, par d'autres mécanismes tels que proxy, détection d'intrusion, etc.

Les flux jugés dangereux (mails, attaques, etc.) sont détruits.

Traçabilité, surveillance et alerte [NET_25]

Des équipements sont mis en œuvre pour assurer la traçabilité des accès et des flux entrants et sortants avec le réseau Internet, et pour l'accès aux applications métiers sensibles.

Les événements tracés sont enregistrés et les traces protégées en intégrité.

Les équipes réseau effectuent un monitoring des événements critiques (alarmes) remontés par les équipements ainsi qu'une analyse quotidienne des journaux d'événements. Les alarmes et les événements susceptibles de révéler un incident de sécurité sont investigués.

Analyse des fichiers entrants et sortants [INET_03]

Dans la mesure du possible, tout contenu transmis ou récupéré par un utilisateur fait l'objet d'une analyse antivirale, soit par l'antivirus du poste de travail, soit par un antivirus de passerelle, ou encore par une station dédiée. Cela s'applique en particulier outre les fichiers transmis par mail, à tous les fichiers téléchargés.

Contrôle des accès et de l'utilisation [INET_04]

Des mesures de contrôle d'accès et d'utilisation de l'Internet sont mises en œuvre :

- Les accès et flux sont indirects et transitent par un serveur mandataire (proxy).
- L'accès est individualisé et les utilisateurs sont authentifiés au niveau de ce serveur mandataire.
- Les accès utilisateur sont contrôlés en fonction du site (listes noires et/ou listes blanches) et des protocoles utilisés.
- Dans la mesure du possible, les contenus des flux sont analysés à la recherche de virus, codes mobiles ou signatures d'attaque.
- Toutes les connexions sont tracées, journalisées et régulièrement auditées.

6.6. Objectif 17 : cartographie réseau

Identification de l'infrastructure réseau [NET_07]

L'infrastructure réseau est répertoriée et documentée. Il existe une description à jour de cette infrastructure incluant :

- Une cartographie du réseau recensant les principaux éléments de l'infrastructure et présentant l'organisation générale du réseau (Ligne Spécialisée, LAN, accès Internet, autre accès…)
- Un dossier de sécurité réseau, définissant l'infrastructure réseau (interface sur l'extérieur, équipements réseaux,…)
- Un recensement des principaux flux de données internes ou externes,
- Un descriptif détaillé du câblage interne,
- Un inventaire des équipements, leur localisation et leur configuration,

- Une description des moyens de sécurisation utilisés (filtrage, chiffrement, authentification,…) et de leur mise en œuvre opérationnelle au niveau des équipements de sécurité réseau.

La documentation réseau est actualisée lors de toute modification fonctionnelle des flux ou de l'infrastructure technique du réseau. Elle est revue au minimum une fois par an.

Documentation d'administration et d'exploitation des réseaux [NET_08]

Les procédures d'exploitation du réseau sont formalisées et documentées. Parmi ces procédures, une attention toute particulière est apportée à la procédure d'ouverture de règles au niveau des équipements de filtrage réseau.

Les éléments (documents, fichiers) décrivant l'infrastructure réseau et sa configuration sont documentés.

La documentation est tenue à jour. L'accès à cette documentation est limité aux personnes disposant du besoin d'en connaître.

Protection de la documentation et des données réseau [NET_09]

La documentation réseau et les procédures d'administration et d'exploitation des réseaux sont des documents sensibles ; elles sont protégées contre tout accès non autorisé par des personnes ne disposant pas du besoin d'en connaître.

Des mesures mise en œuvre par la DSI garantissent la disponibilité et l'intégrité de ces éléments.

7. Architecture des SI

7.1. Objectif 18 : architecture sécurisée des centres informatiques

Maillage des liaisons [NET_03]

Tout service réseau est analysé d'un point de vue disponibilité afin d'évaluer sa criticité vis-à-vis des besoins de l'établissement et des utilisateurs, et dimensionné en conséquence.

Politique de sauvegarde [SAU_01]

Une politique de sauvegarde est formalisée, qui tient compte d'une part des besoins de sécurité des données, des contraintes techniques et du cadre règlementaire.

Cette politique de sauvegarde est revue au minimum une fois par an et mise à jour lors de toute évolution du système d'information.

Test des sauvegardes [SAU_04]

Le bon déroulement des sauvegardes est validé avant stockage des supports ; cette validation est effectuée soit par les moyens techniques fournis par le système de sauvegarde s'ils le permettent, soit par des vérifications manuelles.

Le volume de données sauvegardé doit être suivi par les équipes d'exploitation, pour anticiper les problèmes liés à la capacité des supports.

Restauration [SAU_05]

Les procédures de restauration sont documentées. Des tests de restauration sont effectués au minimum 2 fois par an et les résultats de ces tests sont conservés.

Il convient que des moyens de restauration soient également disponibles hors du site sauvegardé pour pouvoir restaurer les données en cas d'incident ayant détruit le système d'origine.

Gestion et protection des supports de sauvegarde [SAU_06]

Les supports de sauvegarde sont conservés dans des locaux sécurisés ou des armoires fortes adaptés à leur niveau de sensibilité (équivalent à celui des données sauvegardées). Il convient que ces locaux soient suffisamment éloignés des systèmes sauvegardés pour éviter toute destruction simultanée des données et de leurs sauvegardes. Il convient d'utiliser de préférence des armoires ignifugées.

L'accès à ces locaux ou armoires fortes est limité à un nombre restreint de personnes autorisées.

Externalisation des sauvegardes [SAU_07]

En cas d'externalisation des sauvegardes (prestataire), il convient de s'assurer par contrat que les conditions de stockage fournies par le prestataire sont conformes aux besoins exprimés par l'établissement. La mise en œuvre effective des mesures de sécurité par le prestataire est contrôlée régulièrement.

8. Exploitation des SI

Par systèmes et serveurs, on entend les serveurs bureautiques, les serveurs applicatifs et les serveurs dits d'infrastructure (serveurs hébergeant des services transversaux nécessaires au fonctionnement du SI : serveurs de messagerie, serveurs de domaine Active Directory), ainsi que les systèmes dits de sécurité tels que des pare-feu, serveurs antivirus, proxies,…[1]

8.1. Objectif 19 : protection des informations sensibles

Stockage d'une information sensible sur support amovible ou mobile [GDB_12]

Dès lors qu'elles sont stockées sur un support amovible ou mobile, les informations sensibles font l'objet d'un chiffrement approprié.

[1]Document : Charte Informatique

Publication de données sur Internet [INET_05]

L'authenticité des informations mises en ligne est régulièrement contrôlée par leur propriétaire. Il convient que la mise à disposition d'informations particulières telles que programmes, patches ou fichiers de configuration soit toujours associée à celle d'un motif d'intégrité ou d'un scellement permettant à un tiers d'en contrôler l'intégrité.

Recueil d'informations personnelles auprès de tiers (connus ou inconnus) [INET_06]

Ces informations (demandes, coordonnées…) sont collectées par l'Établissement dans un but précis et peuvent être confidentielles ou à caractère personnel. À ce titre :

- Les informations collectées sont protégées contre tout accès non autorisé.
- La personne doit être explicitement informée de la finalité du recueil ainsi que de son droit de consultation et de rectification ou suppression des données personnelles recueillies.

Contrôle des informations mises à disposition [INET_07]

Les informations reçues et mises à disposition par l'Établissement, sont analysées (recherche de virus et de codes mobiles, détection de signatures d'attaque…) et filtrées afin d'éliminer tout élément malveillant, et d'éviter sa retransmission.

Protection des mécanismes de recueil d'information via le web [INET_08]

Les mécanismes de recueil sont protégés contre les attaques par une rupture des flux entre Internet et le système d'information (utilisation d'un serveur mandataire).

8.2. Objectif 20 : surveillance et configuration des ressources informatiques

Sécurisation des serveurs [EXP_01]

Les systèmes d'exploitation des serveurs bénéficient de mesures de durcissement.

Des procédures de durcissement sont définies et appliquées. Elles concernent a minima les aspects :

- Sécurisation de l'accès au BIOS, contrôle d'accès logique au système
- Désactivation des ports et services non utilisés (telnet, rlogin, ftp, etc…)
- Sélection des composants logiciels, désactivation des utilitaires et paquetages non utilisés
- Gestion des comptes et privilèges d'administration
- Mises à jour des correctifs de sécurité
- Activation des traces d'audit
- Stratégie de sécurité (mot de passe, verrouillage)

Documentation des procédures d'exploitation [EXP_02]

Les procédures d'exploitation des systèmes informatiques sont documentées.

Cette documentation précise les instructions à suivre pour toute tâche qui relève de l'administration, de l'exploitation, de la supervision et de la maintenance des systèmes informatiques. Elle est tenue à jour, actualisée si nécessaire, et revue au minimum une fois par an.

Seules les personnes ayant le besoin d'en connaître accèdent à cette documentation.

Maîtrise des modifications et des configurations [EXP_03]

Les configurations des systèmes informatiques et les modifications de ces systèmes font l'objet d'un contrôle strict. Une procédure précise les conditions de mise en œuvre des modifications.

Les impacts des modifications sont évalués et les changements testés. Les modifications importantes sont planifiées. Il convient de définir une procédure de repli.

Les configurations des SI sont documentées. Tous les changements sont consignés.

Partionnement et cloisonnement des applications [APP_06]

Pour limiter l'impact d'un défaut de sécurité il est nécessaire de partitionner et cloisonner les applications par instance en fonction de la sensibilité des données traitées.

8.3. Objectif 21 : autorisations et contrôles d'accès

Gestion des profils et des droits alloués [HGDA_01]

Un certain nombre de catégories (Business Category - BC) définissent des profils d'utilisateurs : chercheurs, enseignants, étudiants, agents administratifs par métier, retraités ...

Le référentiel des catégories permet de définir des procédures de création, de modification et de suppression des comptes utilisateurs, et donc des droits associés à ses profils.

Les droits alloués à chaque profil sont limités aux seuls droits nécessaires à l'accomplissement des missions qui incombent aux titulaires de ce profil.

La liste des catégories et des droits alloués à chaque profil est tenue à jour. Les profils comme les droits alloués sont périodiquement révisés.[2]

Demandes concernant les habilitations et droits d'accès [HGDA_02]

Un document précise les habilitations et droits d'accès par défaut aux applications et aux serveurs, selon les catégories de profils[4].

Retrait des habilitations et droits d'accès [HGDA_05]

Un processus de retrait des droits d'accès est défini selon les profils (en particulier révisé pour les agents à chaque changement de poste ou de fonction)

[2]Document : Référentiel des BC

[4]Document : Services par BC

Les droits d'accès des étudiants sont systématiquement supprimés en fin de cycle d'enseignement,[2].

Identification et authentification [CA_01]

Les utilisateurs des applications et des serveurs sont identifiés individuellement, de manière unique et normalisée. A chaque identifiant est associé un authentifiant respectant les exigences stipulées en la matière[1].

Gestion des comptes [CA_02]

Un processus formel décrit la manière dont les comptes utilisateurs sont gérés, et en particulier comment ils sont créés, modifiés ou supprimés, selon les applications et les profils. Les règles de diffusion des identifiants et authentifiants aux utilisateurs sont aussi formalisées[2].

Caractéristiques des comptes [CA_03]

Tout compte permet d'identifier son titulaire.

Les identifiants respectent la codification interne de l'établissement.

Caractéristiques des authentifiants [CA_04]

Un document d'application définit les principes de gestions des authentifiants.

Lorsque des mots de passe sont utilisés comme authentifiants, ils respectent les règles de bonnes pratiques spécifiées dans document d'application, par exemple :

- Une taille minimale (8 caractères).
- Un niveau minimal de complexité limitant les risques de découverte (mélange de lettres et chiffres, utilisation prohibée de termes faciles à deviner…).

Des dérogations à ces règles sont limitées aux applications qui ne supportent pas ces contraintes.

Confidentialité des authentifiants [CA_05]

Les authentifiants permettant d'accéder à un compte doivent rester strictement confidentiels. À cet effet, ils doivent être mémorisés ou stockés de façon sécurisée par la mise en œuvre de mécanismes cryptologiques.

La transmission d'authentifiant doit impérativement utiliser un protocole chiffré.

Les authentifiants de l'établissement, en particulier les mots de passe, ne doivent pas être utilisés sur des applications externes à l'établissement.

[2]Document : Référentiel des BC

[1]Document : Charte Informatique

[2]Document : Référentiel des BC

Systèmes de gestion des mots de passe [CA_06]

Les logiciels ou fonctions utilisés pour générer ou contrôler les mots de passe choisis par l'utilisateur répondent aux exigences définies par la règle [CA_04], en refusant les mots de passe qui ne répondent pas aux critères retenus. Les mots de passe sont stockés de façon sécurisée par la mise en œuvre de mécanismes cryptologiques.

Suivi des accès [CA_08]

Tous les accès aux données sensibles et fonctions sensibles sont tracés et sont régulièrement analysés et contrôlés.

Les traces sont sauvegardées et conservées de façon sécurisée pendant une période de temps suffisante pour répondre aux besoins opérationnels et satisfaire les exigences réglementaires.

Gestion des comptes système génériques ou partagés [CPRIV_02]

Rentrent dans cette catégorie les comptes tels que « root » sous Unix ou « Administrateur » sous Windows, les comptes dédiés à l'administration de progiciels… L'utilisation de tels comptes peut s'avérer indispensable pour réaliser certaines opérations d'administration et de supervision.

Chaque compte a un titulaire responsable identifié.

Le titulaire a en charge la gestion du mot de passe du compte.

L'utilisation des comptes privilégiés partagés est limitée au strict nécessaire. L'utilisation de comptes système personnels est privilégiée.

Si un compte système est utilisé par une autre personne que le titulaire ou un utilisateur accrédité, l'utilisation se fait en présence du titulaire du compte ou d'une personne qualifiée pour le représenter. Le mot de passe est changé après toute utilisation par un tiers.

Gestion des comptes système utilisés par les constructeurs [CPRIV_04]

Il s'agit principalement de comptes destinés à l'installation ou à la maintenance des matériels et des logiciels.

Les comptes destinés uniquement à l'installation des produits sont supprimés, ou au minimum désactivés, dès l'installation terminée.

Les comptes destinés uniquement à la maintenance sont désactivés en dehors des opérations de maintenance ou leurs mots de passe changés dès la fin de toute opération de maintenance.

Restriction d'emploi des utilitaires systèmes et de sécurité [CPRIV_07]

L'utilisation des programmes permettant de contourner les mesures de sécurité, notamment en accédant directement à l'information stockée ou transportée, sans passer par la couche applicative, est fortement encadrée et tracée, et réservée aux administrateurs autorisés. Il en va de même pour l'utilisation de tout utilitaire de sécurité, permettant par exemple de connaître ou de manipuler le paramétrage des systèmes, d'accéder aux fichiers de journalisation, ou de réaliser toute autre action dangereuse.

L'installation et l'utilisation de tels outils par des utilisateurs non administrateurs est obligatoirement justifiée et préalablement autorisée par les RSSIs.

Séparation des tâches [HGDA_06]

Afin de limiter les risques d'erreur ou de mauvais usage, il convient d'établir une séparation des tâches et des responsabilités entre :

Au niveau fonctionnel :

- Les administrateurs systèmes et réseaux
- Les administrateurs bases de données

Au niveau système :

- Les personnes chargées de l'exploitation des infrastructures support du SI (i.e. les exploitants, administrateurs de niveau 1).
- Et les personnes chargées d'en contrôler l'utilisation (i.e les administrateurs de niveau 2).

Au niveau des comptes applicatifs :

- Les personnes chargées d'autoriser les droits d'accès applicatifs.
- Les personnes utilisant les comptes applicatifs.
- Et les personnes chargées d'attribuer les droits.

8.4. Objectif 22 : sécurisation de l'exploitation

Journalisation des événements système [SURV_02]

Les principaux événements liés à la sécurité sont enregistrés dans des fichiers de traces.

Cette journalisation porte notamment sur les événements suivants :

- Les anomalies pouvant être révélatrices d'un incident de sécurité.
- Les atteintes à la sécurité : détections de virus, tentatives d'intrusion, erreurs de connexion…
- L'activité des personnes en charge de l'exploitation du SI : configuration et paramétrage des systèmes, gestion des habilitations et des droits d'accès…
- L'activité « système » des utilisateurs : connexions et déconnexions, accès et utilisation des ressources sensibles du système d'information…

Les journaux d'audit sont systématiquement revus afin de détecter les problèmes de sécurité. Les événements révélateurs d'un possible problème de sécurité sont analysés quotidiennement. Les autres événements (traces d'activités de gestion ou d'utilisation des SI par exemple) sont revus sur une base hebdomadaire.

Conformité des dispositifs de surveillance et de journalisation [SURV_03]

Il convient de s'assurer que les dispositifs de surveillance et de journalisation mis en œuvre sont conformes à la législation en vigueur, adaptés et proportionnels à l'enjeu et aux risques encourus : il convient de s'assurer que les informations journalisées respectent les exigences légales et réglementaires en matière de trace ainsi que la vie privée des utilisateurs (données personnelles).

Il convient notamment d'informer les instances représentatives des personnels lors du choix de ces dispositifs et de la définition des modalités d'utilisation, et d'informer les utilisateurs de leur mise en œuvre.

Conservation des journaux systèmes [SURV_04]

Les journaux d'audit sont des biens sensibles, qui doivent être sauvegardés et protégés. Ils sont conservés pendant une période suffisante pour répondre aux besoins opérationnels et satisfaire les exigences légales, réglementaires ou contractuelles.

Dispositif de veille et d'évaluation des vulnérabilités [VULN_01]

Une structure de veille permet d'être informé en temps voulu des vulnérabilités identifiées et des correctifs publiés par les éditeurs ou les sites autorisés (par exemple, les CERT).

La criticité de chaque vulnérabilité (i.e. l'impact qui résulterait de leur exploitation) et de chaque correctif (c'est-à-dire des vulnérabilités corrigées) est évaluée ainsi que les actions à entreprendre. Cette évaluation inclut une détermination du niveau d'urgence de ces actions.

Les corrections de failles de sécurité critiques sur des serveurs sensibles doivent être réalisées au plus tôt.

L'application des autres correctifs de sécurité donne lieu à une analyse évaluant le niveau d'urgence et les impacts des modifications sur la continuité de service.

Gestion des mises à jour et correctifs [VULN_02]

Des mesures permettent de s'assurer de l'authenticité des mises à jour et correctifs reçus ou téléchargés. En particulier, ceux concernant les « produits du commerce » sont uniquement obtenus des sites des éditeurs ou de sites sûrs (CERT). Leur intégrité est systématiquement contrôlée.

Dans le cas des systèmes et applications sensibles, les mises à jour et correctifs sont systématiquement testés et validés préalablement à leur diffusion (i.e. publication sur des serveurs relais internes ou de confiance) ou à leur mise en œuvre dans des environnements de test représentatifs des environnements de production. Ces tests comprennent des tests de compatibilité avec l'existant et des tests de non régression.

Les mises à jour et correctifs sont appliqués dans des délais cohérents avec leur niveau de criticité et leur niveau d'urgence. Un « plan de gestion des mises à jour et correctifs » définit les règles permettant cette mise en œuvre dans les meilleurs délais, notamment pour les serveurs critiques.

La bonne application des correctifs est contrôlée et mesurée, en particulier sur les postes des utilisateurs, et les mesures nécessaires sont définies pour traiter les systèmes en défaut.

Assurer la migration des systèmes obsolètes [EXP-OBSOLET]

L'ensemble des logiciels utilisés sur le système d'information doit être dans une version pour laquelle l'éditeur assure le support, et tenu à jour. En cas de défaillance du support, il convient d'en étudier l'impact et de prendre les mesures adaptées.

Isoler les systèmes obsolètes restants [EXP-ISOL]

Il est nécessaire d'isoler les systèmes obsolètes, gardés volontairement pour assurer un maintien en condition opérationnelle des projets, et pour lesquels une migration n'est pas envisageable. Chaque fois que cela est possible, cette isolation doit être effectuée au niveau du réseau (filtrage strict), des éléments d'authentification (qui ne doivent pas être communs avec le reste du SI) et des applications (pas de ressources partagées avec le reste du SI).

8.5. Objectif 23 : défense des systèmes d'information

Séparation des environnements [HGDA_07]

Les différents environnements et équipements (développement, test, exploitation…) sont séparés.

Les règles de passage d'un environnement à l'autre sont formalisées et documentées.

Les données opérationnelles sont « blanchies » s'il est nécessaire de les utiliser pour des besoins de développement ou de test.

Surveillance continue des systèmes [SURV_01]

La DN assure une surveillance continue des systèmes et serveurs sous sa responsabilité.

Cette surveillance porte notamment sur :

- Le contrôle du bon fonctionnement du système d'information.
- Le contrôle de la charge des systèmes et serveurs et de leur disponibilité.
- L'utilisation des systèmes d'information et des serveurs.

Cette surveillance s'appuie sur des moyens dédiés et protégés, qui sont éventuellement partagés avec ceux utilisés pour l'administration et l'exploitation des systèmes et des réseaux.

Gestion des autorisations d'accès aux applications [APP_01]

Les autorisations d'accès aux applications (attribution d'un droit d'accès, révision, retrait) s'appuient sur des règles et procédures mises en place au titre du processus de gestion des habilitations et des droits d'accès.

Les droits alloués sont régulièrement réévalués.

Contrôle d'accès aux applications [APP_02]

L'accès aux applications est contrôlé. Ce contrôle d'accès s'appuie sur les mécanismes mis en œuvre au titre de l'identification des utilisateurs, de leur authentification et des droits hérités de leur profil et du contexte d'utilisation.

Ces mécanismes conditionnent également l'accès aux différentes fonctions et données au sein des applications.

L'accès alloué à un utilisateur est strictement personnel.

Contrôle et suivi de l'utilisation des applications [APP_03]

Les utilisations des fonctions applicatives sont tracées et journalisées (en fonction de leur sensibilité et des données accédées).

Les journaux applicatifs sont régulièrement analysés afin de détecter les erreurs d'utilisation, les dysfonctionnements et les utilisations illicites.

8.6. Objectif 24 : exploitation sécurisée des centres informatiques

Installation et hébergement [SRV_01]

Les serveurs sont installés en zone de niveau 4, dans des locaux dédiés, sécurisés (contrôle d'accès, protection environnementale, télésurveillance) adaptés à la sensibilité des données qu'ils traitent et des informations qu'ils hébergent.

Systèmes a priori sensibles [SRV_02]

Les systèmes suivants sont automatiquement considérés comme sensibles et sont protégés :

- Contrôleurs de domaine
- Serveurs antivirus
- Serveurs de messagerie
- Serveurs Web, serveurs FTP et autres serveurs d'échanges en DMZ
- Serveurs applicatifs.

Disponibilité des serveurs sensibles [SRV_03]

Les serveurs d'infrastructure sont systématiquement redondés.

Il convient d'estimer la nécessité d'une redondance, de dispositif de secours ou de contrat de maintenance adapté pour les serveurs bureautiques ou applicatifs en fonction des besoins de disponibilité analysés.

Administration et supervision [SRV_04]

L'administration et la supervision des serveurs sont réalisées par des personnels autorisés depuis des environnements protégés (locaux, VLAN, consoles de supervision).

Les flux d'administration et de supervision sont protégés en confidentialité.

Les actions d'administration et de supervision sont tracées et font l'objet de revues périodiques.

Déconnexion automatique des sessions [SRV_05]

Une période d'inactivité des sessions d'administration est définie pour les systèmes sensibles, au delà de laquelle une nouvelle identification et authentification sont rendues obligatoires.

Synchronisation des horloges [SRV_06]

Les ressources informatiques nécessitant de disposer d'un horaire fiable pour leurs traitements ou pour la production de log d'enregistrement, sont synchronisées à un système de référence de temps. Selon le besoin de précision, la mise à l'heure est effectuée de façon manuelle par l'administrateur du système ou réalisée par une synchronisation automatique (NTP).

9. Sécurité du poste de travail

9.1. Objectif 25 : sécurisation des postes de travail

Attribution des postes de travail [PDT_01]

L'attribution d'un poste de travail est soumise à autorisation par le responsable hiérarchique ; les usagers autorisés doivent prendre connaissance de la charte informatique de l'établissement[1].

Identification des postes de travail [PDT_02]

Tout poste est identifié par une étiquette indélébile et inventoriée. Il existe un inventaire de l'ensemble des postes de travail, de leur localisation « principale », de leur spécificité, et de leur utilisateur.

Rappel des règles de protection des postes de travail [PDT_03]

Les principales règles et dispositions relatives à la sécurité des postes de travail et à leur utilisation sont rappelées lors d'opérations périodiques de sensibilisation des utilisateurs. Les utilisateurs sont sensibilisés à l'usage de moyens de protection physique des postes et matériels de travail en dehors de leur présence : fermeture des locaux, rangements dans des armoires fermées à clé, fixation lorsqu'ils sont susceptibles d'être facilement emportés, etc…

Administration des postes de travail [PDT_04]

Une équipe locale chargée de la gestion des postes est responsable de l'administration des postes de travail. En règle générale, l'utilisateur ne dispose pas des droits lui permettant de réaliser des opérations d'administration sur son poste de travail.

L'administration d'un poste de travail bureautique par son utilisateur reste une exception. Elle fait l'objet d'une demande formelle motivée et validée par la hiérarchie de l'utilisateur.

[1]Document : Charte Informatique

Sécurité des postes de travail [PDT_05]

Tous les utilisateurs de poste de travail doivent être identifiés par authentification ou accès physique limité.

À cet effet,

- l'intégrité du poste de travail doit être assuré par l'usage d'anti-virus, les mises à jour du système et des applications, la non utilisation des droits d'administration.
- les utilisateurs doivent s'assurer de limiter l'accès à leur environnement de travail en leur absence : fermeture ou verrouillage de session, de porte.
- les données doivent être sauvegardées. Les données sensibles ne doivent pas être conservés sur les postes de travail.

En particulier, les accès anonymes à Internet sont interdits (cf: NET_22)

Politique de sécurité des nomades [NOMAD_01]

Un document d'application spécifique à la mobilité est défini : il traite a minima les points suivants :

- Ouverture de session protégée par mot de passe
- obligation d'un mode d'accès sécurisé (VPN) pour l'accès au réseau interne
- utilisation de moyens de chiffrement des données sur les postes nomades,
- rappel des risques de connexions sur des moyens non sûr avec ses identifiants universitaires (cybercafé, borne, …)

Dispositifs de sécurité installés sur les nomades [NOMAD_05]

Tout poste nomade doit disposer par défaut d'un verrouillage de session.

Tous les ordinateurs professionnels doivent disposer par défaut de :

- L'antivirus choisi par l'établissement

- Le chiffrement du disque dur

Selon les besoins identifiés et les informations traitées, des configurations durcies peuvent être mises à disposition des usagers : outil de sécurisation de la connexion VPN, outil de chiffrement des dossiers, outil de sauvegarde spécifique, support amovible sécurisé, outil de contrôle de double connexion.

9.2. Télétravail

Télétravail. [NOMAD_08]

Le télétravail comme le traitement ou le stockage de données propriété de l'établissement ne peuvent être réalisés que sur les équipements mis à la disposition des utilisateurs par l'établissement. Ces équipements doivent être intégrés aux systèmes de gestion de l'établissement après accès par VPN dédié. Les disques durs des équipements doivent être chiffrés. L'usage de documents imprimés est à proscrire.

Cette réglementation ne s'applique au télétravail ponctuel que dès lors que des solutions auront été mises en place et travaillées avec les organisations syndicales pour garantir l'égal accès de l'ensemble des agents, qu'ils soient en directions centrales ou dans les composantes de formation ou de recherche, au télétravail ponctuel avec les meilleures garanties de sécurité de l'Établissement.

9.3. Supports informatiques mobiles

Usage des supports d'informations amovibles et mobiles. [PDT_07]

Il est impératif d'utiliser exclusivement des supports informatiques d'origine connue et contrôlée (clés USB, disques durs externes, téléphones mobiles, lecteurs de musique, appareils photos, etc...)

Les utilisateurs sont sensibilisés sur les risques de leur utilisation au sein de l'établissement (introduction de virus, divulgation d'information en cas de perte ou vol), et appliquent les consignes qui leurs ont été communiquées dans la charte informatique[1].

Stockage d'une information sensible sur support amovible ou mobile [PDT_08]

Dès lors qu'elles sont stockées sur un support amovible ou mobile, les informations sensibles font l'objet d'un chiffrement approprié.

Politique du bureau propre [PDT_09]

Les personnels de l'établissement ne laissent pas d'informations sensibles exposées à la vue ou à la convoitise de personnes non autorisées ; en particulier, chaque personne est responsable du rangement de son bureau ou des espaces partagés qu'elle utilise.

Les supports (tableaux, paper-boards, papiers, …) utilisés dans des locaux partagés pour traiter des informations sensibles sont systématiquement effacés ou détruits.

Mise au rebut des supports amovibles [PDT_10]

Les supports de données mobiles ou amovibles (disque dur, DVD, papier, etc…) contenant de l'information sensible sont préalablement effacés avant leur mise au rebut.

[1]Document : Charte Informatique

9.4. Bureautique

Sécurité des documents bureautiques utilisateurs [BUR_01]

Des espaces bureautiques sécurisés et sauvegardés sont mis à la disposition de chaque utilisateur. L'accès à ces espaces utilisateurs sécurisés est limité à l'utilisateur et aux administrateurs autorisés.

Les documents bureautiques confidentiels sont stockés dans ces espaces sécurisés et sauvegardés.

Sécurité des espaces bureautiques partagés (groupware) [BUR_02]

Des espaces bureautiques partagés sécurisés et sauvegardés sont créés à la demande (pour des projets, des applications bureautiques). L'accès à ces espaces partagés est sous le contrôle d'un responsable identifié.

Les documents bureautiques confidentiels partagés sont stockés dans ces espaces partagés sécurisés et sauvegardés.

9.5. Messagerie

Formalisation des règles d'utilisation de la messagerie électronique [MES_01]

Les règles relatives à l'utilisation de la messagerie sont formalisées et mises à la disposition des utilisateurs. Elles sont rappelées dans la charte informatique[1].

Contrôle d'accès à la messagerie électronique [MES_02]

L'accès à la messagerie nécessite une identification et authentification préalable de l'utilisateur.

Analyse des messages [MES_03]

Les messages électroniques sont systématiquement analysés en DMZ ou sur le serveur de messagerie par un antivirus d'une technologie différente de celle employée sur les postes de travail.

Chiffrement des messages et pièces jointes [MES_04]

Les utilisateurs ayant besoin d'échanger des informations sensibles disposent sur leur poste de travail d'un logiciel de chiffrement de fichier validé par le Comité de Sécurité Opérationnelle.

Les utilisateurs privilégient l'échange d'informations sensibles au travers de pièces jointes chiffrées plutôt que dans le corps du message. Si le corps du message est également sensible, il fera également l'objet d'un chiffrement au niveau de la messagerie.

[1]Document : Charte Informatique

9.6. Objectif 26 : sécurisation des copieurs multifonctions

Durcissement des imprimantes et copieurs multifonctions [IMP_01]

Les imprimantes et copieurs multifonctions hébergés localement dans une entité doivent faire l'objet d'un durcissement en termes de sécurité : changement des mots de passe initialement fixés par le « constructeur », désactivation des interfaces réseau inutiles, suppression des services inutiles, chiffrement des données sur le disque dur lorsque cette fonctionnalité est disponible, configuration réseau statique. Les imprimantes et copieurs multifonctions sont des ressources informatiques à part entière qui doivent être gérées en tant que telles. Elles ne doivent pas pouvoir communiquer avec l'extérieur.

Configuration des imprimantes [IMP_02]

Les données mémorisées sur les imprimantes mutualisées sont régulièrement effacées par les administrateurs.

Les imprimantes mutualisées sont configurées afin de ne pas permettre de transmettre de documents scannés par mail à l'extérieur de l'établissement.

Protection des impressions [IMP_03]

Des mesures organisationnelles permettent de limiter le temps de présence des impressions sensibles sur les imprimantes.

Les impressions sensibles sont réalisées sur des imprimantes contrôlées (localisation physique protégée, imprimantes sur un réseau contrôlé), et configurées pour permettre au seul propriétaire de pouvoir récupérer les impressions.

9.7. Objectif 27 : sécurisation de la téléphonie

9.8. Objectif 28 : contrôles de la conformité des postes de travail

Disponibilité et utilisation quotidienne des antivirus [VIR_02]

L'équipe locale chargée des SI s'assure que tout équipement concerné dispose d'un antivirus actif et à jour et qu'un scan a lieu quotidiennement. Cela peut être réalisé par un monitoring permanent ou au minimum par un contrôle périodique systématique.

L'antivirus installé sur le poste de travail effectue régulièrement un scan de l'ensemble des disques locaux afin de s'assurer de l'absence de virus sur le poste.

Détection et traitement des virus [VIR_03]

Tout virus détecté déclenche automatiquement une information des équipes locales chargées des SI, par alerte de surveillance et par enregistrement dans les journaux. Ces journaux doivent être examinés quotidiennement.

10. Sécurité du développement des systèmes

10.1. Objectif 29 : prise en compte de la sécurité dans le développement des SI.

Acquisition de solutions et externalisation des développements [PDM_03]

Les cahiers des charges rédigés pour l'acquisition d'une solution sensible (produit, système ou service) ou son développement tiennent compte de l'analyse de sécurité et incluent des clauses qui formulent les exigences et les conditions d'emploi prévues.

Ces cahiers des charges doivent inclure aussi des clauses destinées à assurer la pérennité de ces solutions et prendre en compte la maintenance et les contraintes d'évolution des systèmes et logiciels support dues à la mise en place de correctifs.

Bonnes pratiques de développement sécurisé [PDM_04]

Il convient de mettre en œuvre un ensemble de bonnes pratiques en matière de développement.

Ces bonnes pratiques prennent notamment en compte les points suivants :

- L'utilisation de la notion de profil métier pour le contrôle d'accès
- La journalisation des accès et de l'utilisation des différentes fonctions applicatives
- Le contrôle des données d'entrées et des procédures de saisie
- La limitation des durées de connexions et la vérification régulière de cette connexion
- La mise en place de mécanismes de reprise et de gestion des erreurs
- La sécurisation ou le durcissement des équipements, systèmes et configuration
- La mise en œuvre des derniers niveaux de correctifs
- La capacité de sauvegarder et de restaurer les données applicatives

Cloisonnement des environnements [PDM_06]

Les environnements de développement et de maintenance, de tests et de pré-production sont distincts de l'environnement exploitation.

Les données utilisées pour le développement et les tests ne sont jamais des données opérationnelles sensibles.

Cloisonnement des rôles [PDM_07]

Une séparation marquée des rôles entre tâches de développement, de tests et recette, et d'exploitation est mise en place.

Bon fonctionnement des applications [PDM_09]

Les applications sensibles sont hébergées sur des serveurs récents, dont la maintenance « constructeur » est toujours assurée. Il en va de même pour les systèmes d'exploitation.

Politique de journalisation [PDM_10]

Une politique de journalisation est mise en place, spécifiant, pour chaque application, les actions à auditer, permettant de collecter, en cas d'attaque ou de dysfonctionnement, les preuves et traces nécessaires au traitement de l'incident. Les délais de rétention des traces sont définis selon la sensibilité des applications. La politique de journalisation est conforme à la législation en vigueur.

10.2. Objectif 30 : prise en compte de la sécurité dans le développement des logiciels

Validation des données et fonctions applicatives [APP_04]

Une vérification des données transmises aux applications sensibles est effectuée afin d'empêcher des conditions pouvant porter atteinte à la sécurité des fonctions ou des informations des applications (valeurs hors intervalle, caractères invalides, données incomplètes, etc…)

La conception et la mise en œuvre des applications doivent réduire les risques de pertes d'intégrité. Les droits de lecture, écriture, exécution sont ajustés au besoin.

En fonction de leur sensibilité, les applications alimentées en sources externes de données contrôlent l'intégrité des messages et données reçues.

Les tests de recettes des applications sont réalisés de manière systématique afin de s'assurer que les bonnes pratiques de sécurité ont été prises en compte.

Limitation de durée de connexion [APP_05]

Les applications sensibles, dont l'accès est réservé sur une plage horaire ou sur un accès de courte durée (applications accessibles depuis des zones difficilement contrôlables par l'Etablissement), mettent en œuvre des limitations du temps de connexion, par tranche horaire, par durée de connexion, ou par durée d'inactivité. Les utilisateurs doivent alors se ré-authentifier pour continuer l'usage de ces applications sensibles.

Test des bonnes pratiques de développement [PDM_05]

Si le projet est considéré comme sensible, les fonctions et services de sécurité mis en œuvre sont testés et « recettés » avant toute mise en exploitation.

Gestion des sources, des évolutions et des modifications [PDM_08]

Les programmes sources, les scripts et les fichiers de paramètres sont gérés en configuration.

L'accès à ces fichiers comme aux données utilisées pour le développement est protégé.

Adhérence des applications à des produits ou technologies spécifiques [DEV-LOG-ADHER]

réduire l'adhérence des applications à des produits ou technologies spécifiques. Le fonctionnement d'une application s'appuie sur un environnement logiciel et matériel. En phases de conception et de spécification technique, il est nécessaire de s'assurer que les applications n'ont pas une trop forte adhérence vis-à-vis des environnements sur lesquels elles reposent. En effet, l'apparition de failles sur un environnement a de fait un impact sur la sécurité des applications qui en dépendent. En plus du maintien en condition de sécurité propre à l'application, il est donc nécessaire de pouvoir faire évoluer son environnement pour garantir sa sécurité dans la durée.

10.3. Objectif 31 : sécurisation des applications à risques

11. Traitement des incidents

11.1. Objectif 32 : chaînes opérationnelles

Procédure de gestion des incidents [INC_01]

L'Établissement met en œuvre une gestion des incidents liés à la sécurité.

- Les RSSIs évaluent, classent la nature de l'incident, assurent la centralisations des informations (dates, circonstances, actions correctrices).
- Les RSSIs transmettent les alertes aux CSSIs en charge du périmètre concerné et aux contacts en capacité d'intervenir.
- Les RSSIs se chargent de la diffusion des informations aux partenaires et autorités.

- Les équipements concernés par un incident de sécurité doivent être IMMÉDIATEMENT isolés du réseau.
- Avant toute intervention corrective, il faut déterminer la cause de l'incident.
- Les incidents doivent être signalés à la liste rssi@univ-lorraine.fr (INC_O4) ainsi que les conséquences de l'incident : impact de la coupure d'accès, fuite de données, attaque contre des tiers, ..[63].

[6]Document : Intervention sur incidents

[3]Document : Chaîne fonctionnelle d'alerte

Retour d'expérience [INC_02]

Tout incident de sécurité nécessite d'être analysé afin d'identifier les faiblesses exploitées et définir si nécessaire les mesures correctives permettant d'en limiter la répétition[6].

Conservation des traces [INC_03]

Tout incident de sécurité peut conduire à des sanctions, nécessiter des actions en justice ou conduire à un contentieux contractuel. Les traces et les éléments susceptibles de servir de preuve, comme de permettre une analyse a posteriori des incidents, sont recueillis et conservés en lieu sûr.

Un hash MD5 des fichiers collectés et conservés doit être transmis pour s'assurer de l'intégrité de ces fichiers[6].

Procédure de signalement [INC_04]

Les incidents doivent être signalés à la liste rssi@univ-lorraine.fr

Ces incidents concernent tout signe d'intrusion, d'utilisation frauduleuse d'un ordinateur ou d'infraction de sécurité, ainsi que tout comportement inhabituel ou inattendu.

Les incidents comme la perte ou le vol d'un ordinateur ou d'une clé USB doivent également être signalés s'ils contiennent des données potentiellement sensibles.

Surveillance du SI et détection des incidents [INC_05]

Des moyens organisationnels et des outils de supervision permettent un suivi de l'activité au niveau du système d'information et la détection des incidents :

- Supervision des éléments critiques sur le plan de la sécurité (virus, passerelles de messagerie, passerelles Internet, Wifi, connexions nomades…).
- Journalisation en temps réel des évènements liés à la sécurité du système d'information.
- De réaliser une surveillance continue des systèmes et des réseaux et de revoir périodiquement les différents journaux à la recherche d'anomalies pouvant être révélatrices d'incidents.
- D'analyser et traiter les anomalies détectées. Ces analyses doivent être formalisées et conservées.

Il appartient à la DN :

Cellule d'alerte et de traitement des incidents [INC_06]

Il appartient au Comité de Sécurité Opérationnelle de définir et mettre en place, avec le support de la DN, une cellule en charge du traitement des alertes et des incidents liés à la SSI, tels que :

- Les intrusions dans les réseaux et les systèmes.

[6]Document : Intervention sur incidents

[6]Document : Intervention sur incidents

- Les attaques par déni de service.
- Les violations de la politique de sécurité par les utilisateurs.

Il appartient à la cellule d'alerte de définir et mettre en œuvre les procédures d'urgence afin de formaliser les actions à prendre en cas de mise en alerte pour circonstances particulières (incident d'exploitation, détection attaque, violation contrôle d'accès…).

Signalement des incidents par le personnel [INC_08]

Le personnel de l'Établissement est tenu de signaler, le plus rapidement possible, tout événement ou faille de sécurité pouvant impacter la sécurité à son responsable hiérarchique ou au responsable sécurité désigné.

12. Continuité d'activité

12.1. Objectif 33 : gestion de la continuité d'activité

Organisation du PCA [PCA_01]

L'Établissement met en place une organisation permettant de répondre aux incidents majeurs pour revenir rapidement à un état fonctionnel acceptable.

Les rôles et responsabilités des intervenants dans le cadre du plan de continuité d'activité (PCA) sont identifiés, ainsi que les astreintes associées. Les modalités de déclenchement du PCA sont définies.

Existence du site de secours [PCA_04]

L'Établissement dispose, pour ses applications et informations les plus critiques, d'un site de secours qui permet le redémarrage des applications et services critiques dans les délais.

13. Conformité et contrôle

13.1. Objectif 34 : contrôles réguliers

Contrôle et suivi [AUD_01]

La conformité à la PSSIE et à la PSSI ministérielle est vérifiée par des contrôles réguliers. Les RSSI conduisent des actions locales d'évaluation de la conformité à la PSSIE et contribuent à la consolidation, dans un bilan annuel, de l'état d'avancement de sa mise en oeuvre.

Protection des outils d'audit [AUD_04]

Les outils d'audit (logiciels ou les fichiers de données) sont séparés des systèmes en exploitation et ne sont accessibles que par les personnes autorisées.

13.2. Conformité avec les exigences légales et réglementaires

Conformité avec les exigences légales et réglementaires [CONF_01]

Les procédures de sécurité, ainsi que leurs mises à jour, sont établies dans le respect des obligations légales, règlementaires et contractuelles.

Un corpus documentaire liste l'ensemble des textes de référence encadrant les obligations légales et réglementaires. Il convient de s'y référer en cas de besoin[5].

Identification de la législation en vigueur [CONF_02]

Une veille est assurée afin d'identifier les lois et règlements nationaux auxquels le SI de l'Établissement se conforme. Ces lois et règlements sont répertoriés et documentés. Les intervenants sont régulièrement informés au travers du comité de sécurité opérationnelle.

Respect des droits de propriété intellectuelle [CONF_03]

L'Établissement dispose de règles et procédures appropriées visant à garantir le respect de la propriété intellectuelle tant pour les biens possédés ou confiés à l'Établissement que pour les droits détenus par l'Établissement.

En particulier :

- L'Établissement s'engage à acquérir les logiciels uniquement à partir de sources connues et réputées.
- Les licences originales et les preuves d'achats des matériels et logiciels utilisés sont conservées en lieu sûr.
- Des contrôles sont régulièrement effectués afin de vérifier le respect de la législation et de régulariser les licences globales. En cas de manquement caractérisé, des sanctions peuvent être prise à l'encontre des contrevenants.

Obligation de protection des enregistrements de l'organisme [CONF_04]

Des mesures organisationnelles et techniques sont définies et mises en place afin de protéger les enregistrements importants sur un plan légal ou réglementaire (journaux de log, activités des dispositifs de contrôles d'accès, archives de vidéosurveillance) contre une perte, destruction et falsification, conformément aux exigences légales et réglementaires et aux contraintes métier.

[5]Document : Contexte légal et réglementaire

Protection des données à caractère personnel [CNIL_01]

L'établissement prend en compte les exigences de la CNIL relatives à la protection des données à caractère personnel. Pour cela les actions suivantes sont menées :

- Lister les traitements de données personnelles
- Déclarer les traitements auprès de la CNIL
- Mettre en œuvre les actions d'information et de sensibilisation des acteurs concernés par les traitements d'informations personnelles
- S'assurer du non détournement de la finalité des traitements (tels que le croisement de fichiers)
- S'assurer de l'effectivité des mesures de sécurité sur les traitements, garantissant la confidentialité des données

Déclaration des traitements [CNIL_02]

Tout nouveau projet traitant de données à caractère personnel fait l'objet d'une information auprès d'un correspondant juridique, une fiche de traitement est formalisée et validée.

Communication sur la protection des données à caractère personnel [CNIL_03]

Tout responsable qui souhaite mettre en œuvre un traitement de données personnelles doit préalablement contacter le comité de sécurité opérationnel afin de déterminer les formalités à accomplir et les mesures à mettre en œuvre pour protéger les informations traitées.

14. Annexe 1: Documents de référence

- Charte Informatique
- Référentiel des BC
- Chaîne fonctionnelle d'alerte
- Services par BC
- Contexte légal et réglementaire
- Intervention sur incidents