PREMIER MINISTRE
Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Sous-direction assistance, conseil et expertise
Bureau assistance et conseil

Expression des Besoins et Identification des Objectifs de Sécurité

EBIOS

BASES DE CONNAISSANCES

Version du 25 janvier 2010

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 65 - Fax 01 71 75 84 90

Historique des modifications

Date	Objet de la modification	Statut
02/1997	Publication par le service central de la sécurité des systèmes d'information (SCSSI) du guide d'expression des besoins et d'identification des objectifs de sécurité (EBIOS) et de ses bases de connaissances	Validé
05/02/2004	Publication par la direction centrale de la sécurité des systèmes d'information (DCSSI) de la version 2 du guide EBIOS et de ses bases de connaissances	Validé
25/01/2010	Publication par l'agence nationale de la sécurité des systèmes d'information (ANSSI) de la nouvelle version du guide EBIOS et de ses bases de connaissances : ❑ Restructuration complète (afin d'améliorer la structuration, la cohérence, l'exhaustivité et la compréhensibilité) : o des types de biens supports, o des menaces génériques, o des vulnérabilités génériques, o des mesures de sécurité génériques. ❑ Ajout (afin d'améliorer l'usage de la méthode de manière homogène et exhaustive) : o des types de sources de menaces, o des types d'impacts. ❑ Concernant les mesures de sécurité : o retrait de l'[ISO 15408], o ajout du référentiel général de sécurité.	Validé

Table des matières

Note : les libellés entre crochets […] correspondent à des références bibliographiques en annexe.

Avant-propos

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) élabore et tient à jour un important référentiel méthodologique destiné à aider les organismes du secteur public et du secteur privé à gérer la sécurité de leurs systèmes d'informations. Ce référentiel est composé de méthodes, de meilleures pratiques et de logiciels, diffusés gratuitement sur son site Internet (http://www.ssi.gouv.fr).

Le Club EBIOS est une association indépendante à but non lucratif (Loi 1901), composée d'experts individuels et d'organismes. Il regroupe une communauté de membres du secteur public et du secteur privé, français et européens. Il supporte et enrichit le référentiel de gestion des risques français depuis 2003, en collaboration avec l'ANSSI. Le Club organise des réunions périodiques pour favoriser les échanges d'expériences, l'homogénéisation des pratiques et la satisfaction des besoins des usagers. Il constitue également un espace pour définir des positions et exercer un rôle d'influence dans les débats nationaux et internationaux.

Ce document a été réalisé par le bureau assistance et conseil de l'ANSSI, avec la collaboration du Club EBIOS. La communauté des utilisateurs d'EBIOS enrichit régulièrement le référentiel complémentaire à ce document (techniques de mise en œuvre, bases de connaissances, guides d'utilisations spécifiques de la méthode, documents relatifs à la communication, à la formation, à la certification, logiciels…).

Introduction

Ce guide présente les bases de connaissances de la méthode EBIOS (expression des besoins et identification des objectifs de sécurité), concernant les types de :

- biens supports,
- impacts,
- sources de menaces,
- menaces et vulnérabilités,
- mesures de sécurité.

Elles ne sont pas nécessaires pour utiliser la méthode, mais constituent une aide précieuse pour gérer les risques de sécurité de l'information. En effet, elles reposent sur le retour d'expérience des usagers de la méthode. Et comme toute taxonomie, ces bases de connaissances visent :

- la structuration des connaissances (le classement doit permettre d'adopter une vision globale et de séparer les catégories de manière sémantique),
- le non recouvrement (les différentes catégories ne doivent pas se recouper pour qu'une attaque ne puisse pas être dans deux catégories à la fois),
- l'exhaustivité (toutes les attaques doivent pouvoir se trouver dans la classification),
- une clarté suffisante pour garantir la répétitivité (les instances doivent se ranger naturellement dans les catégories, indépendamment de qui effectue l'analyse ; deux analyses successives doivent conduire au même résultat), et
- l'acceptabilité (le caractère intuitif et utile du classement doit apparaître clairement).

Il est important de bien noter que ces bases de connaissances :

- ne constituent qu'une aide et ne sauraient remplacer le savoir et le savoir faire des experts,
- restent bien évidemment toujours améliorables (enrichissement, rectifications…),
- adoptent un niveau de détail qui ne convient pas directement à tous les usages d'EBIOS,
- traitent de sécurité de l'information, donc ne sont pas directement applicables à d'autres fins.

1 Types de biens supports

Les types de biens supports représentent les grandes catégories de composants d'un système d'information sur lesquels reposent les biens essentiels et/ou les mesures de sécurité.

Les biens supports sont :

- les systèmes informatiques et de téléphonie (SYS), qui peuvent être décomposés en :
  - matériels (MAT),
  - logiciels (LOG),
  - canaux informatiques et de téléphonie (RSX) ;
- les organisations (ORG), qui peuvent être décomposées en :
  - personnes (PER),
  - supports papier (PAP),
  - canaux interpersonnels (CAN) ;
- les locaux (LOC), qui hébergent les autres biens supports et fournissent les ressources ;

Note : les solutions de sécurité (procédures, produits…) ne sont pas considérées comme des biens supports ; elles sont en effet prises en compte en cours d'étude dans les "mesures de sécurité existantes" ou à la fin de l'étude dans les "mesures de sécurité" destinées à traiter les risques. Les risques liés à ces mesures de sécurité (induits du fait de leur intégration dans le système ou intrinsèques) doivent être gérés lors du traitement des risques afin de ne pas biaiser l'étude. De même, un type d'un haut niveau hiérarchique se verra affecté des biens essentiels liés aux types des niveaux inférieurs.

Chaque type fait l'objet d'une description. Les exemples figurent en *italique*.

SYS – Systèmes informatiques et de téléphonie[1]

Ce type de biens supports est constitué de la combinaison de matériels (MAT), de logiciels (LOG) et de canaux informatiques et de téléphonie (RSX) en interaction, organisés pour élaborer, traiter, stocker, acheminer, présenter ou détruire tout ou partie des biens essentiels.

Tel ordinateur isolé, tel réseau ou combinaison de réseaux (petit réseau local, réseau Ethernet d'entreprise, réseau local à jeton – token ring, réseau mobile, réseau sans fil en maillage complet, réseau sans fil à maillage partiel – point à point, point à multipoints, multipoints à multipoints ou métropolitain, réseau point à point, réseau en grille, réseau toroïdal ou en hypercube), telle interconnexion.

MAT – Matériels

Ce type de biens supports est constitué de l'ensemble des éléments physiques d'un système informatique (*hardware* et des supports de données électroniques) participant au stockage et au traitement de tout ou partie des biens essentiels.

Il peut être utile de différencier les matériels selon la typologie suivante.

Ordinateur

Matériel informatique permettant de traiter automatiquement des données et comprenant les organes nécessaires à son fonctionnement autonome, ses interfaces de communication (ports, connecteurs et adaptateurs), et ses périphériques indispensables (écran, clavier, souris…), qu'il soit fixe (conçu pour ne pas être déplacé manuellement et utilisé dans les locaux de l'organisme) ou mobile (conçu pour être déplacé manuellement et utilisé en des lieux différents).

Serveur, poste de travail, ordinateur central (mainframe), centre multimédia (media center), micro-ordinateur portable, assistant personnel (PDA), ardoise électronique.

Périphérique informatique

Matériel informatique, optionnel, que l'on doit connecter à un ordinateur par une interface de communication (ports, connecteurs et adaptateurs), et qui réalise l'entrée et/ou la sortie de données.

Imprimante, scanner, copieur multifonctions, périphérique de sauvegarde amovible (lecteur/graveur CD-ROM ou DVD-ROM…), microphone, caméra, télécommande.

Périphérique de téléphonie

Matériel de téléphonie qui réalise l'entrée et/ou la sortie de données.

Téléphone analogique fixe, téléphone analogique sans fil, téléphone IP, téléphone mobile.

Relais de communication

Dispositif intermédiaire ou relais, actif ou passif, informatique ou de téléphonie, qui transporte et aiguille des données.

Pont, routeur, hub, commutateur téléphonique (PABX, IPBX), modem.

Support électronique

Support électronique connectable à un ordinateur ou à un réseau informatique pour le stockage de données numériques. Il est susceptible de contenir de grand volume de données tout en restant de petite taille. Il est utilisable à partir d'équipement informatique standard.

Cédérom, DVD-Rom, clé USB, cartouche de sauvegarde, disque dur amovible, bande, carte mémoire (Compact Flash, Memory Stick, Multimedia Card, Secure Digital, Smartmedia…), disquette, cassettes.

[1] Ensemble des moyens informatiques et de télécommunication ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire des données. [IGI 1300]

LOG – Logiciels

Ce type de biens supports est constitué de l'ensemble des programmes participant au traitement de tout ou partie des biens essentiels (*software*).

Il peut être utile de différencier les logiciels selon la typologie suivante.

Application

Ensemble de composants logiciels (structure de stockage de données, librairies, interfaces conversationnelles…) fournissant des services aux utilisateurs (génériques ou spécifiques à leur métier) en automatisant des tâches, fonctions ou processus. Il peut s'agir d'un produit commercialisé, développé spécifiquement ou personnalisé.

Navigateur web, portail web, client de courrier électronique, suite bureautique, logiciel de comptabilité, téléprocédure administrative, application de pilotage de machine outil, forum de discussion, logiciel réseau.

Système de gestion de base de données

Ensemble de programmes permettant l'accès (séquentiel, par hachage ou indexé), l'ajout, la mise à jour et la recherche au sein d'une base de données.

Ingres, PostgreSQL, DB2, Oracle, SQL Server, Informix.

Intergiciel (middleware)

Logiciel de communication entre un système d'exploitation des applications, gérant les appels de fonctions de l'application ou de renvoi des résultats (par une interface de programmation), et mettant en forme des données pour la couche transport (par un protocole d'accès formaté).

EAI (Enterprise Application Integration), ETL (Extract-Transform-Load), CORBA (Common Object Request Broker Architecture), ODBC (Open DataBase Connectivity), NEXUS, ORB (Open Request Broker), moniteur transactionnel, MOM (Message Oriented Middleware).

Système d'exploitation

Logiciel d'un ordinateur constituant le socle opérationnel sur lequel vont s'exécuter l'ensemble des autres logiciels (services ou applications). Il comprend un noyau et des fonctions ou services de base. Selon les architectures, un système d'exploitation peut être monolithique ou constitué d'un micro-noyau et d'un ensemble de services systèmes. Le système d'exploitation contient principalement tous les services de gestion du matériel (CPU, mémoire, disques, périphériques et interfaces réseaux), ceux de gestions des taches ou processus et ceux de gestion des utilisateurs et de leurs droits.

GCOS, MVS, Solaris, Linux, Windows95, Windows2000, WindowsXP, PalmOS, WCX, MacOS.

Micrologiciel (firmware)

Logiciel (interne, embarqué ou d'exploitation) intégré dans un composant matériel au sein d'une mémoire volatile (effacée lorsqu'elle n'est plus alimentée en électricité) ou non.

BIOS (Basic Input Output System), gestionnaire de composants d'un téléphone mobile, programme stocké dans une clé USB équipée d'un microprocesseur, gestionnaire d'injection électronique d'un moteur à explosion.

RSX – Canaux informatiques et de téléphonie

Ce type de biens supports est constitué de l'ensemble des vecteurs physiques de communication et de télécommunication qui transportent tout ou partie des biens essentiels.

Il peut être utile de différencier les canaux informatiques et de téléphonie selon la typologie suivante.

Canal informatique

Vecteur de communications informatiques et téléphoniques sous forme numérique.

Cordon réseau, fibre optique, ondes radio, wifi.

Canal de téléphonie analogique

Vecteur de communications téléphoniques sous forme analogique.

Ligne téléphonique.

ORG – Organisations

Ce type de biens supports est constitué de la combinaison de personnes (PER), de supports papier (PAP) et des canaux interpersonnels (CAN) en interaction, organisées pour satisfaire les objectifs d'un organisme (en réalisant des activités métiers spécifiques) et manipulant tout ou partie des biens essentiels.

Telle personne morale[2], telle entreprise, tel ministère, tel organisme sous tutelle, tel partenaire, tel fournisseur, tel client, tel service, telle organisation projet, tel cadre organisationnel pour homologuer un système.

PER – Personnes

Ce type de biens supports est constitué de l'ensemble des individus, catégories d'individus ou groupes sociaux homogènes, qui ont accès à tout ou partie des biens essentiels.

On peut ainsi distinguer différentes fonctions (direction, encadrement, responsable, subordonné…), métiers (secrétaire, juriste, informaticien, commercial, ingénieur, comptable, dépanneurs…), ou statuts (contractuel, fonctionnaire, stagiaire, visiteur, contracté…).

Employés (développeur d'applications métiers, direction générale, chef de projet, manager, autorité d'homologation, utilisateur standard, exploitant, administrateur système ou de données, opérateur de sauvegarde, Help Desk…), personnes ne faisant pas partie de l'organisme mais placées sous sa responsabilité (stagiaire, thésard, prestataire en régie…), groupe projet.

PAP – Supports papier

Ce type de biens supports est constitué de l'ensemble des Support statique non électronique contenant des données.

Document manuscrit, document imprimé, diapositive, transparent, documentation, fax, photographie, radiographie.

CAN – Canaux interpersonnels

Ce type de biens supports est constitué de l'ensemble des circuits organisationnels (canaux et processus organisationnels) et des échanges verbaux en face à face, qui transportent tout ou partie des biens essentiels.

Circuit de validation par parapheur, processus de décision, circuit courrier, réunions, discussions de couloir.

[2] Entité, généralement constituée par un groupement de personnes physiques ou morales ou de biens, dotée de la personnalité juridique, et au sein de laquelle des biens essentiels sont manipulés. Selon sa forme, elle peut être de droit public, de droit privé ou de droit mixte.

LOC – Locaux

Ce type de biens supports est constitué des infrastructures immobilières hébergeant, et nécessaires au bon fonctionnement, des systèmes informatiques (SYS) et des organisations (ORG), dans lesquels sont utilisés tout ou partie des biens essentiels.

Site de Rennes, site d'exploitation au Maroc, usine au Pays-Bas, siège à Paris, locaux de l'organisme, périmètre particulier au sein des locaux, bureaux, bâtiment ou partie de bâtiment à usage de bureaux, de stockage, industriel, d'habitation ou mixte, *pièce de stockage, salle serveur, salle de conférence, salle de réunion.*

2 Types d'impacts

Les types impacts constituent les catégories de conséquences, directes et indirectes, sur l'organisme et sur les tiers, de la réalisation d'un sinistre.

Chaque type d'impacts fait l'objet d'une description. Les exemples figurent en *italique*.

Impacts sur le fonctionnement

Impacts sur les missions

Conséquences directes ou indirectes sur la réalisation des missions (production d'un bien ou d'un service).

Incapacité à fournir un service, perte de savoir-faire, changement de stratégie, impossibilité d'assurer un service, conséquences sur la production ou la distribution de biens ou de services considérés comme vitaux (atteinte à la satisfaction des besoins essentiels des populations, à l'exercice de l'autorité de l'État, au fonctionnement de l'économie, au maintien du potentiel de défense, à la sécurité de la nation).

Impacts sur la capacité de décision

Conséquences directes ou indirectes sur la liberté de décider ou diriger.

Perte de souveraineté, perte ou limitation de l'indépendance de jugement ou de décision, limitation des marges de négociation, perte de capacité d'influence, prise de contrôle de l'organisme

Impacts humains

Impacts sur la sécurité des personnes

Conséquences directes ou indirectes sur l'intégrité physique de personnes.

Accident du travail, maladie professionnelle, perte de vies humaines, mise en danger.

Impacts sur le lien social interne

Conséquences directes ou indirectes sur la qualité des liens sociaux au sein de l'organisme.

Perte de confiance des employés dans la pérennité de l'entreprise, exacerbation d'un ressentiment ou de tensions entre groupes sociaux (direction / employés, nationaux / étrangers, fonctionnaires / non-fonctionnaires, jeunes / seniors), affaiblissement de l'engagement d'employés vis-à-vis de l'entreprise, affaiblissement des valeurs éthiques communes au personnel (humanitaire, service public pour tous, progrès social, contribution à la santé dans le monde…)

Impacts sur les biens

Impacts sur le patrimoine intellectuel ou culturel

Conséquences directes ou indirectes sur les connaissances non-explicites accumulées par l'organisme, sur le savoir-faire, les capacités d'innovation, sur les références culturelles communes.

Perte de mémoire de l'entreprise (anciens projets, succès ou échecs…), perte de connaissances implicites (savoir-faire transmis entre générations, optimisations dans l'exécution de tâches ou de processus, captation d'idées novatrices, perte de patrimoine culturel (références esthétiques, modèles, styles…) ou scientifique (espèces biologiques rares ou disparues…).

Impacts financiers

Conséquences pécuniaires, directes ou indirectes.

Perte de chiffre d'affaire, dépenses imprévues, chute de valeur en bourse, baisse de revenus, pénalités.

Impacts sur l'image

Conséquences directes ou indirectes sur l'image de marque, la notoriété, la renommée, la capacité d'influence de l'organisme (lobby, relation avec des acteurs et décideurs politiques ou économiques) ou sur l'éthique (transparence, non corruption, respect de la dignité humaine, argent propre…).

Publication d'un article satirique dans la presse, perte de crédibilité vis-à-vis de clients, mécontentement des actionnaires, perte d'avance concurrentielle, perte de notoriété.

Autres impacts

Impacts de non-conformité

Conséquences directes ou indirectes sur l'obtention ou la maintenance d'un label (certification, qualification…) de conformité à des normes.

Refus d'obtention ou perte de labels du fait de non conformités à l'ISO 27001, Sarbanes-Oxley.

Impacts juridiques

Conséquences procédurales, pénales, civiles ou administratives, directes ou indirectes.

Procès, amende, condamnation d'un dirigeant, dépôt de bilan, avenant, amendements de contrats.

Impacts sur l'environnement

Conséquences écologiques à court ou long terme, directes ou indirectes.

Nuisances dues à des déchets ou des rejets sources de pollution (chimique, bactériologique, radiologique, sonore, visuelle, olfactive, …) générée par l'organisme et touchant son périmètre, son voisinage ou une zone.

3 Types de sources de menaces

Les sources de menaces représentent une typologie des choses ou personnes à l'origine des risques.

On distingue les sources par :
- leur origine humaine ou non humaine,
- leur facilité d'accès au sujet de l'étude (interne ou externe),
- dans le cas de sources humaines :
  - leur caractère intentionnel ou accidentel,
  - leurs capacités (force intrinsèque, selon leurs ressources, expertise, dangerosité…),
- dans le cas de sources non humaines :
  - leur type (naturelle, animale, contingence…).

Chaque type de source de menace fait l'objet d'exemples, qui figurent en *italique*.

Sources humaines agissant de manière délibérée

Personnes ou groupes de personnes mal intentionnées, qu'elles soient physiques ou morales, et qui peuvent être à l'origine de risques. Elles peuvent être internes ou externes au sujet de l'étude. Leurs capacités (force intrinsèque) dépendent principalement de leurs ressources, de leur expertise et du temps qu'elles peuvent accorder. Leur motivation peut être le jeu, la cupidité, la vengeance, une idéologie, le chantage, l'égo, la recherche d'un avantage concurrentiel, le terrorisme…

Source humaine interne, malveillante, avec de faibles capacités

Collaborateur malveillant avec des possibilités d'action limitées sur le système d'information (personnel en fin de contrat ou voulant se venger de son employeur ou de ses collègues…), stagiaire agissant de manière ludique, client désirant obtenir des avantages, personnel d'entretien.

Source humaine interne, malveillante, avec des capacités importantes

Collaborateur malveillant avec d'importantes connaissances et possibilités d'action sur le système d'information (manager ambitieux en fin de contrat ou voulant se venger de son employeur ou de ses collègues, développeur agissant par égo ou de manière ludique, fraudeur, actionnaires…), sous-traitant ou prestataire, personnel de maintenance ou d'assistance à distance.

Source humaine interne, malveillante, avec des capacités illimitées

Collaborateur malveillant avec des connaissances et possibilités d'action illimitées sur le système d'information (administrateur système ou réseau agissant par vengeance, dirigeant…).

Source humaine externe, malveillante, avec de faibles capacités

Script-kiddies, vandale.

Source humaine externe, malveillante, avec des capacités importantes

Militant agissant de manière idéologique ou politique, pirate passionné, casseur ou fraudeur, ancien employé désirant se venger d'un licenciement, concurrent, groupement professionnel, organisation de lobbying, syndicat, journaliste, organisation non gouvernementale.

Source humaine externe, malveillante, avec des capacités illimitées

Organisation criminelle, agence gouvernementale ou organisation sous le contrôle d'un État étranger, espions, organisation terroriste.

Sources humaines agissant de manière accidentelle

Personnes ou groupes de personnes sans intention de nuire, qu'elles soient physiques ou morales, et qui peuvent être à l'origine de risques. Ceci comprend tout type d'activités humaines. Elles peuvent être internes ou externes au sujet de l'étude. Leurs capacités (force intrinsèque) dépendent principalement de leurs ressources, de leur expertise et du temps qu'elles peuvent accorder. Leur action involontaire peut être due à une faute d'attention, à une erreur de manipulation, à un manque d'investissement, à la malchance…

Source humaine interne, sans intention de nuire, avec de faibles capacités

Collaborateur maladroit ou inconscient avec des possibilités d'action limitées sur le système d'information, personnel à faible conscience d'engagement, peu sensibilisé ou peu motivé dans sa relation contractuelle avec l'organisme, personnel d'entretien maladroit, stagiaire, thésard, intérimaire, utilisateur, fournisseur, prestataire, sous-traitant, client, actionnaires.

Source humaine interne, sans intention de nuire, avec des capacités importantes

Collaborateur maladroit ou inconscient avec d'importantes connaissances et possibilités d'action sur le système d'information (manager, développeur…).

Source humaine interne, sans intention de nuire, avec des capacités illimitées

Collaborateur maladroit ou inconscient avec des connaissances et possibilités d'action illimitées sur le système d'information (administrateur système ou réseau, dirigeant…).

Source humaine externe, sans intention de nuire, avec de faibles capacités

Entourage du personnel, personne réalisant des travaux dans le voisinage, manifestants, visiteur maladroit, forte ambiance sonore.

Source humaine externe, sans intention de nuire, avec des capacités importantes

Matériels émettant des ondes, des vibrations, activités industrielles dégageant des substances chimiques toxiques ou susceptibles de provoquer des sinistres mineurs, trafic routier ou aérien pouvant générer des accidents.

Source humaine externe, sans intention de nuire, avec des capacités illimitées

Matériels émettant des radiations ou des impulsions électromagnétiques, activités industrielles susceptibles de provoquer des sinistres majeurs, explosion dans le voisinage.

Sources non humaines

Choses ou objets qui peuvent être à l'origine de risques. Elles peuvent être internes au sujet de l'étude ou externe à celui-ci. Il ne peut s'agir que de contingences ou de malchance. Leurs capacités dépendent principalement de leurs ressources disponibles et de leur dangerosité.

Code malveillant d'origine inconnue

Virus informatique, code malveillant non ciblé, ou ciblé mais d'origine inconnue.

Phénomène naturel

Phénomène météorologique ou climatique aléatoire (foudre, canicule…), chute de roches, infiltration de sable, usure (temps qui s'écoule), phénomène naturel imprévisible mais récurrent.

Catastrophe naturelle ou sanitaire

Phénomène géologique (affaissement de terrain, séisme, éruption volcanique…), météorologique (tempête, ouragan…), naturel (feu de forêt, crue…), sanitaire (pandémie) de grande ampleur.

Activité animale

Présence d'animaux susceptibles de provoquer des dégâts aux infrastructures (rongeurs…), présence d'animaux dangereux pour l'homme.

Événement interne

Présence de matières corrosives, combustion de matières inflammables, incendie des locaux, explosion de matières explosives, fuite de canalisation, accident de chantier, fuite de substances chimiques, réorganisation, changement d'architecture réseau, branchement d'un composant réseau ou d'une machine incompatible, travaux de réaménagement des locaux.

4 Menaces et vulnérabilités génériques

Les menaces génériques représentent les incidents ou les sinistres types qui peuvent affecter les biens supports.

Elles peuvent être classées selon :

- le type de biens supports sur lequel elles portent (MAT, LOG, CAN, PER) ;
- le critère de sécurité des biens essentiels qu'elles sont susceptibles d'affecter (disponibilité, intégrité, confidentialité) ;
- leur mode opératoire :
  - les détournements d'usages (USG) : les biens supports sont détournés de leur cadre d'utilisation nominal (usage des fonctionnalités possibles, prévues ou autorisées) sans être modifiés ni endommagés ;
  - l'espionnage (ESP) : les biens supports sont observés, avec ou sans équipement supplémentaire, sans être endommagés ;
  - les dépassements de limites de fonctionnement (DEP) : les biens supports sont surchargés ou utilisés au-delà de leurs limites de fonctionnement ;
  - les détériorations (DET) : les biens supports sont endommagés, partiellement ou totalement, temporairement ou définitivement ;
  - les modifications (MOD) : les biens supports sont transformés ;
  - les pertes de propriété (PTE) : les biens supports sont aliénés (perdus, volés, vendus, donnés…), sans être modifiés ni endommagés, de telle sorte qu'il n'est plus possible d'exercer les droits de propriété.

Chaque menace générique fait l'objet d'une description et d'exemples, qui figurent en *italique*. Les critères de sécurité directement concernés, les principales vulnérabilités exploitables et les pré-requis pour la source de menace complètent la description.

La correspondance entre la typologie précédente et la présente typologie est présentée en annexe.

Concernant les principales vulnérabilités exploitables, celles-ci représentent les caractéristiques génériques des biens supports qui peuvent être exploitées pour que les menaces puissent se réaliser. Elles ne sont pas exhaustives et devraient systématiquement être adaptées pour être intelligibles pour les personnes à qui elles sont destinées et que leur niveau de détail soit approprié au sujet étudié et à l'objectif poursuivi.

Menaces sur les matériels

M1. MAT-USG – Détournement de l'usage prévu d'un matériel

Le matériel est utilisé à d'autres fins que celles prévues, sans être modifié ni endommagé. Ses ressources peuvent ainsi être réduites ou rendues indisponibles.

Usage d'une imprimante à des fins personnelles au détriment d'autrui, stockage de fichiers personnels sur l'ordinateur de bureau, utilisation de la vitesse de traitement, utilisation de matériels inappropriés à la sensibilité des informations stockées (disque dur, clé USB…).

Critère(s) de sécurité concerné(s) :	**Disponibilité**	**Intégrité**	**Confidentialité**

Principales vulnérabilités exploitables :

- Utilisable en dehors de l'usage prévu (exploitation nominale des biens essentiels)

Pré-requis pour la source de menace :

- Connaissance de l'existence et de la localisation du matériel
- Accès physique au matériel (franchissement légitime ou non, ou contournement)

M2. MAT-ESP – Espionnage d'un matériel

Le matériel, généralement un périphérique, est observé ou écouté, sans être endommagé, avec ou sans équipement d'amplification sensorielle ou de capture, depuis l'intérieur ou l'extérieur de locaux. Les informations et traitements peuvent ainsi être compromis.

Observation d'un écran, écoute de hauts parleurs, observation des caractéristiques de fonctionnement d'un matériel (analyse d'émanations électromagnétiques telles que des signaux parasites compromettants issus de l'affichage ou des touches du clavier, observation de caractéristiques électriques telles que la consommation, attaque temporelle, cryptanalyse acoustique, attaque par faute, attaque par perturbation telle qu'un changement rapide de la tension d'alimentation ou au laser, ingénierie inverse), géolocalisation d'un matériel (à partir de son adresse IP ou par le réseau téléphonique), extraction de données par refroidissement brutal (cold boot), interception de signaux compromettants (via des tuyaux ou des câbles de fourniture de ressources, en utilisant une antenne d'interception…).

Critère(s) de sécurité concerné(s) :	Disponibilité	Intégrité	**Confidentialité**

Principales vulnérabilités exploitables :

- Permet d'observer des données interprétables
- Émet des signaux compromettants

Pré-requis pour la source de menace :

- Connaissance de l'existence et de la localisation du matériel
- Accès physique au matériel (franchissement légitime ou non, ou contournement)

M3. MAT-DEP – Dépassement des limites de fonctionnement d'un matériel

Les capacités physiques du matériel sont dépassées. Il peut ainsi tomber en panne ou dysfonctionner de manière temporaire.

Surexploitation des capacités de stockage et de traitement (surcharge des capacités, volume d'information à traiter supérieur au flux alloué…), exploitation aux limites de fonctionnement (forte sollicitation ou saturation pour provoquer des effets de bord), mise en conditions extrêmes (perturbations électriques ou électromagnétiques, échauffement, glaciation), défaut de fourniture énergétique d'un matériel (surexploitation de l'alimentation électrique par rapport à l'approvisionnement prévu, remplacement de matériels dont la consommation est supérieure à la fourniture énergétique, incompatibilité, surcharge, court-circuit dû à la foudre, une erreur de branchement ou un incident électrique, courant qui disjoncte, rupture de câbles électriques…).

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

Principales vulnérabilités exploitables :
- Dimensionnement inapproprié des capacités de stockage
- Dimensionnement inapproprié des capacités de traitement
- N'est pas approprié aux conditions d'utilisation
- Requiert en permanence de l'électricité pour fonctionner
- Sensible aux variations de tension

Pré-requis pour la source de menace :
- Accès à la fourniture de ressources essentielles
- Détournement d'usage d'un logiciel pour surcharger les fonctionnalités du matériel

M4. MAT-DET – Détérioration d'un matériel

Le matériel est endommagé, partiellement ou totalement, temporairement ou définitivement, à l'intérieur ou à l'extérieur des locaux. Il peut ainsi tomber en panne ou casser et ne plus pouvoir être utilisé.

Usure d'un matériel par vieillissement (naturel, accéléré en raison de l'usage de mauvais matériaux, d'une construction défectueuse, de mouvements du terrain, de sape des fondations, d'infiltration d'eau dans le sol…), corrosion (agression chimique, pollution, humidification…), dégradation, casse (vandalisme, code malveillant sollicitant fortement la tête de lecture d'un disque dur), destruction des composants électroniques (impulsion électromagnétique, déclenchement d'une bombe à impulsion électromagnétique ou engendrant un effet électromagnétique), embrasement, explosion (bombe, missile, accident…), effacement d'un matériel (action d'un aimant sur un disque dur, impulsion électromagnétique sur les matériels électroniques, action de vibrations…).

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

Principales vulnérabilités exploitables :
- Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement…)
- N'est pas approprié aux conditions d'utilisation (sensible à l'humidité…)
- Effaçable (vulnérable aux effets électromagnétiques ou vibratoires…)

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du matériel
- Accès physique au matériel (franchissement légitime ou non, ou contournement)

M5. MAT-MOD – Modification d'un matériel

Le matériel est modifié par le retrait, l'ajout, la substitution ou la désactivation d'un élément à l'intérieur ou à l'extérieur des locaux. Il peut ainsi tomber en panne, dysfonctionner ou fonctionner autrement que son fonctionnement nominal.

Branchement de périphériques ou de supports amovibles incompatibles, changement d'éléments lors d'une maintenance, piégeage d'un matériel (keylogger).

Critère(s) de sécurité concerné(s) :	**Disponibilité**	**Intégrité**	**Confidentialité**

Principales vulnérabilités exploitables :
- Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions…) via des connecteurs (ports, slots…)
- Permet de désactiver des éléments (port USB…)

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du matériel
- Accès physique au matériel (franchissement légitime ou non, ou contournement)

M6. MAT-PTE – Perte d'un matériel

Le matériel est perdu, sans être endommagé, à l'intérieur ou à l'extérieur des locaux. Son contenu peut ainsi ne plus être disponible et l'être pour autrui.

Vol, perte ou don d'un ordinateur, d'un périphérique, d'un PABX, d'un composant du réseau ou d'un support de données électronique, revente, recyclage ou mise au rebus d'un matériel obsolète, perte de matériel lors d'un déménagement.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	**Confidentialité**

Principales vulnérabilités exploitables :

- Portable
- Attractif (valeur marchande)

Pré-requis pour la source de menace :

- Connaissance de l'existence et de la localisation du matériel
- Accès physique au matériel (franchissement légitime ou non, ou contournement)

Menaces sur les logiciels

M7. LOG-USG – Détournement de l'usage prévu d'un logiciel

Les fonctionnalités du logiciel sont utilisées, sans le modifier ni l'endommager, pour réaliser des actions autres que celles prévues.

Lecture ou copie inappropriée via un logiciel : lecture ou copie de données de configuration ou de données métiers, fouille de contenu stocké, collecte de données métiers partagées.

Suppression inappropriée via un logiciel : effacement d'enregistrements, de fichiers ou de répertoires, qu'ils soient sur une mémoire, un disque dur ou un support, effacement de traces de journaux d'événements, effacement de fichiers ou de répertoires partagés sur un réseau.

Création ou modification inappropriée via un logiciel : saisie de messages ne respectant pas la charte d'utilisation d'un espace d'échange non modéré (forum, blog…), élévation de privilèges d'un compte utilisateur, modification du contenu ou du nom de fichiers ou de répertoires, partagés ou non, ou de la configuration d'un système, qu'ils soient sur une mémoire, un disque dur ou un support (insertion d'une page web sur un site Internet, défiguration de site Internet, élévation de privilèges, modification des traces de journaux d'événements, fraude…), croisement d'informations dont le résultat est confidentiel, utilisation de canaux cachés pour traiter ou véhiculer des données discrètement (stéganographie).

Usage inapproprié de fonctionnalités d'un logiciel : usage d'un logiciel professionnel pour des besoins personnels, détournement de fonctionnalités de réseaux (envoi massif d'informations par courrier électronique – spam, envoi de données ou de fichiers partagés, détournement de services d'un réseau…), utilisation de logiciels contrefaits ou copiés.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	**Intégrité**	**Confidentialité**

Principales vulnérabilités exploitables :
- Donne accès à des données
- Permet de manipuler des données (supprimer, modifier, déplacer…)
- Peut être détourné de son usage nominal (offre la possibilité d'envois massifs…)
- Permet d'utiliser des fonctionnalités avancées

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du logiciel
- Accès logique au logiciel (franchissement légitime ou non, ou contournement)

M8. LOG-ESP – Analyse d'un logiciel

Le logiciel est analysé (code source, fonctionnement, fonctionnalités…), sans être endommagé, depuis l'intérieur ou l'extérieur du système d'information. Des données et du savoir faire peuvent ainsi être compromis.

Collecte de données de configuration d'un réseau, balayage d'adresses réseau ou de ports, observation des caractéristiques de fonctionnement d'un logiciel (observation de l'espace mémoire d'un logiciel depuis un débogueur, ingénierie inverse…).

Critère(s) de sécurité concerné(s) :	Disponibilité	Intégrité	**Confidentialité**

Principales vulnérabilités exploitables :
- Accessibilité et intelligibilité du code source
- Possibilité d'observer le fonctionnement du logiciel

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du logiciel
- Accès logique au logiciel (franchissement légitime ou non, ou contournement)

M9. LOG-DEP – Dépassement des limites d'un logiciel

Les capacités de stockage ou de traitement du logiciel sont dépassées sans qu'il soit modifié. Le logiciel peut ainsi dysfonctionner, permettre de réaliser des fonctions non prévues ou tomber en panne.

Surexploitation (dépassement du dimensionnement des enregistrements d'une base de données ou de la longueur des variables…), injection de données en dehors des valeurs prévues (fuzzing), attaque en déni de service, lancement d'une boucle infinie, débordement de tampon (buffer overflow), exploitation aux limites de fonctionnement (forte sollicitation ou saturation pour provoquer des effets de bord), saturation des services réseaux, création d'incompatibilités entre logiciels.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

Principales vulnérabilités exploitables :
- Permet de saisir n'importe quelle donnée
- Permet de saisir n'importe quel volume de données
- Permet de réaliser n'importe quelle action avec les données entrantes
- Peu interopérable

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du logiciel
- Accès logique au logiciel (franchissement légitime ou non, ou contournement)

M10. LOG-DET – Suppression de tout ou partie d'un logiciel

Le logiciel est endommagé, partiellement ou totalement, temporairement ou définitivement. Il peut ainsi ne plus pouvoir être utilisé (tout ou partie des fonctionnalités attendues a disparu).

Effacement d'un exécutable en production, effacement de code sources, effacement ou suppression d'un logiciel par un code malveillant (bombe logique…).

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

Principales vulnérabilités exploitables :
- Possibilité d'effacer ou de supprimer des programmes
- Exemplaire unique
- Utilisation complexe (mauvaise ergonomie, peu d'explications…)

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du logiciel

M11. LOG-MOD – Modification d'un logiciel

Le logiciel est modifié. Il peut ainsi dysfonctionner ou ne plus fonctionner (substitution ou ajout de fonctionnalités).

Manipulation inopportune lors de la mise à jour, de la configuration ou de la maintenance (activation ou désactivation de fonctions, changement de paramétrage du réseau, règles de routage ou de résolution de nom, modification ou ajout de fonctionnalités ou de code…), piégeage logiciel (keylogger, contagion par un code malveillant, substitution d'un composant par un autre…).

Critère(s) de sécurité concerné(s) :	**Disponibilité**	**Intégrité**	**Confidentialité**

Principales vulnérabilités exploitables :
- Modifiable (améliorable, paramétrable…)
- Maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes…)
- Ne fonctionne pas correctement ou conformément aux attentes

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du logiciel

M12. LOG-PTE – Disparition d'un logiciel

Le logiciel n'est plus en possession de son propriétaire, sans être endommagé. Il ne peut ainsi plus rendre ses services et peut éventuellement les rendre à autrui.

Revente d'un logiciel, perte ou non renouvellement de licence, cession de droits sur une licence.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	**Confidentialité**

Principales vulnérabilités exploitables :

- Exemplaire unique (des contrats de licence ou du logiciel, développé en interne…)
- Attractif (rare, novateur, grande valeur commerciale…)
- Cessible (clause de cessibilité totale dans la licence…)

Pré-requis pour la source de menace :

- Connaissance de l'existence et de la localisation du logiciel

Menaces sur les canaux informatiques et de téléphonie

M13. RSX-USG – Attaque du milieu sur un canal informatique ou de téléphonie

Le canal informatique ou de téléphonie est utilisé à d'autres fins que celles prévues, sans le modifier ni l'endommager. Le flux d'information qui transite peut ainsi être altéré, ralenti ou bloqué (suppression, modification, ajout, ralentissement, brouillage…).

Attaque du milieu (man in the middle) sur un canal informatique ou téléphonique, rejeu (réémission d'un flux intercepté)…

Critère(s) de sécurité concerné(s) :	**Disponibilité**	**Intégrité**	Confidentialité

Principales vulnérabilités exploitables :
- Permet d'altérer les flux communiqués (interception puis réémission, éventuellement après altération…)
- Seule ressource de transmission pour le flux
- Permet de modifier les règles de partage du canal informatique ou de téléphonie (protocole de transmission qui autorise le rajout de nœuds et l'accès…)

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du canal informatique ou de téléphonie
- Accès physique ou logique au canal informatique ou de téléphonie (intégration légitime ou non d'un élément sur le canal[3])

M14. RSX-ESP – Écoute passive d'un canal informatique ou de téléphonie

Le canal informatique ou de téléphonie est observé, sans être endommagé, avec ou sans matériel d'interception, depuis l'intérieur ou l'extérieur du système d'information. Le flux d'information peut ainsi être écouté.

Acquisition de données par écoute passive, interception téléphonique.

Critère(s) de sécurité concerné(s) :	Disponibilité	Intégrité	**Confidentialité**

Principales vulnérabilités exploitables :
- Unique
- Perméable (émission de rayonnements, parasites ou non…)
- Permet d'observer des données interprétables
- Observable

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du canal informatique ou de téléphonie
- Accès physique ou logique au canal informatique ou de téléphonie (intégration légitime ou non d'un élément sur le canal)

M15. RSX-DEP – Saturation d'un canal informatique ou de téléphonie

Le canal informatique ou de téléphonie est surchargé, partiellement ou totalement. Le flux d'information peut ainsi être ralentit ou bloqué.

Surexploitation de la bande passante d'un réseau, assourdissement de signal, détournement de la bande passante d'un canal de transmission (exploitation distante d'un réseau sans fil, occupation de bande passante, téléchargement non autorisé…).

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

[3] Intégration d'une machine non maîtrisée sur un réseau, branchement d'un dispositif (d'interception, de brouillage…) en coupure d'un câble réseau ou téléphonique, infiltration d'une personne malveillante au sein de l'organisation, interconnexion maîtrisée ou non (cette situation devrait requérir une mise à jour de l'étude)…

Principales vulnérabilités exploitables :

- Dimensionnement fixe des capacités de transmission (dimensionnement insuffisant de la bande passante, plage de numéros téléphoniques limitée…)

Pré-requis pour la source de menace :

- Connaissance de l'existence et de la localisation du canal informatique ou de téléphonie
- Accès physique ou logique au canal informatique ou de téléphonie (intégration légitime ou non d'un élément sur le canal)

M16. RSX-DET – Dégradation d'un canal informatique ou de téléphonie

Le canal informatique ou de téléphonie est endommagé, partiellement ou totalement, temporairement ou définitivement. Le flux d'information peut ainsi être ralentit ou bloqué.

Sectionnement de câblages, dégradation ou coupure d'une ligne téléphonique, pincement de câble, torsion de fibre optique.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

Principales vulnérabilités exploitables :

- Altérable (fragile, cassable, câble de faible structure, à nu, gainage disproportionné …)
- Unique

Pré-requis pour la source de menace :

- Connaissance de l'existence et de la localisation du canal informatique ou de téléphonie
- Accès physique ou logique au canal informatique ou de téléphonie (intégration légitime ou non d'un élément sur le canal)

M17. RSX-MOD – Modification d'un canal informatique ou de téléphonie

Le canal informatique ou de téléphonie est modifié. Le flux d'information qu'il supporte peut ainsi être ralentit ou bloqué.

Remplacement d'un câble par un autre inapproprié (incompatible, de moins grande capacité…), rallonge de câble, modification du chemin d'un câble, changement de gamme de fréquences hertziennes.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

Principales vulnérabilités exploitables :

- Modifiable (remplaçable…)

Pré-requis pour la source de menace :

- Connaissance de l'existence et de la localisation du canal informatique ou de téléphonie
- Accès physique ou logique au canal informatique ou de téléphonie (intégration légitime ou non d'un élément sur le canal)

M18. RSX-PTE – Disparition d'un canal informatique ou de téléphonie

Le canal informatique ou de téléphonie n'est plus présent, sans avoir été altéré. Le flux d'information ne peut plus transiter.

Vol de câbles de transmission.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

Principales vulnérabilités exploitables :

- Attractif (valeur marchande des câbles…)
- Transportable (léger, dissimulable…)
- Peu visible (oubliable, insignifiant, peu remarquable…)

Pré-requis pour la source de menace :

- Connaissance de l'existence et de la localisation du canal informatique ou de téléphonie
- Accès physique ou logique au canal informatique ou de téléphonie (intégration légitime ou non d'un élément sur le canal)

Menaces sur les personnes

M19. PER-USG – Dissipation de l'activité d'une personne

Les ressources de la personne sont employées à faire autre chose que ce qu'elle devrait faire, sans la faire changer ni l'affecter physiquement. Ses performances peuvent ainsi être diminuées.

Exploitation du temps de travail (réception et tri ou lecture de pourriel – spam, retransmission d'un canular – hoax, retransmission d'une escroquerie – scam…), exploitation d'une personne en dehors de ses prérogatives ou détournement des services rendus par une personne (utilisation illégitime des ressources d'une personne par d'autres services, travail en dehors des missions fixées dans un contrat…), blocage de l'accès d'une personne à son lieu de travail (occupation, grève, squattage, manifestation, routes coupées suite à des inondations, pandémie, zone de guerre, manifestations sur la route d'accès ou blocage du site, zone interdite pour cause de contamination bactérienne, utilisation de locaux à d'autres fins que celles prévues…).

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

Principales vulnérabilités exploitables :

- Sujet à la dissipation (distraction, difficulté à cadrer ses activités…)

Pré-requis pour la source de menace :

- Connaissance de l'existence et de la localisation de la personne
- Établissement d'une relation (hiérarchique, professionnelle, d'autorité, personnelle, sociale…) avec la personne

M20. PER-ESP – Espionnage d'une personne à distance

Observation ou écoute d'une personne, avec ou sans équipement d'amplification sensorielle ou de capture, depuis l'intérieur ou l'extérieur des locaux, sans être affectée physiquement.

Divulgation involontaire, observation du comportement et des habitudes.

Critère(s) de sécurité concerné(s) :	Disponibilité	Intégrité	**Confidentialité**

Principales vulnérabilités exploitables :

- Peu discret (loquace, sans réserve…)
- Routinier (habitudes facilitant l'espionnage récurrent)

Pré-requis pour la source de menace :

- Connaissance de l'existence et de la localisation de la personne
- Proximité physique de la personne

M21. PER-DEP – Surcharge des capacités d'une personne

Les capacités (compétences, ressources, capacités physiques ou psychologiques) de la personne sont dépassées. Elle peut ainsi ne plus agir correctement et ses performances peuvent diminuer.

Surcharge (une personne est poussée à trop travailler et ne peut plus réaliser ses actions correctement, baisse de performance, fatigue, problèmes personnels…), stress, perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée, mauvaise utilisation des compétences.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	**Intégrité**	Confidentialité

Principales vulnérabilités exploitables :

- Ressources (capacités de travail et disponibilités) insuffisantes pour les tâches assignées
- Capacités physiques inappropriées aux conditions de travail (travail en pleine chaleur, avec une lumière insuffisante, dépassement de la capacité de locaux pour l'activité du personnel, utilisation de locaux à d'autres fins que celles prévues, inadéquation de locaux pour l'usage réel, contamination par des fumées d'incendie ou des produits nocifs ou désagréables…)
- Capacités psychologiques inappropriées aux conditions de travail (faible résistance au stress ou à la pression permanente liée à l'activité, sujet à l'influence de la démotivation ambiante…)
- Compétences inappropriées aux conditions d'exercice de ses fonctions (compétences insuffisantes ou mal employées, méthode de travail inadaptée, changement de la langue de travail…)
- Incapacité à s'adapter au changement (nouveaux outils, nouvelles méthodes de travail…)

Pré-requis pour la source de menace :

- Connaissance de l'existence et de la localisation de la personne
- Établissement d'une relation (hiérarchique, professionnelle, d'autorité, personnelle, sociale…) avec la personne

M22. PER-DET – Dégradation d'une personne

La personne est affectée physiquement ou psychologiquement, partiellement ou totalement, temporairement ou définitivement, à l'intérieur ou à l'extérieur des locaux. Elle peut ainsi exercer sa fonction de manière moins performante, voire ne plus pouvoir exercer sa fonction.

Accident du travail, maladie professionnelle, autre blessure ou maladie (agression, empoisonnement, intoxication, infection bactériologique, biologique, radiologique, chimique, épidémie, pandémie…), assassinat, décès, surmenage, affection neurologique, psychologique ou psychiatrique, suicide.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

Principales vulnérabilités exploitables :

- Limites physiques, psychologiques ou mentales

Pré-requis pour la source de menace :

- Connaissance de l'existence et de la localisation de la personne
- Proximité physique de la personne

M23. PER-MOD – Influence sur une personne

Les conditions d'exercice du libre arbitre de la personne sont modifiées, à l'intérieur ou à l'extérieur des locaux. Elle peut ainsi être amenée à agir de manière inopportune ou à divulguer des informations.

Pression, corruption ou manipulation (via argent, idéologie, chantage, ego, plaisirs…), hameçonnage, filoutage, ingénierie sociale, harcèlement moral, torture, désinformation, embrigadement, rumeur.

Critère(s) de sécurité concerné(s) :	Disponibilité	**Intégrité**	**Confidentialité**

Principales vulnérabilités exploitables :

- Influençable (naïf, crédule, obtus, faible estime de soi, faible loyauté…)
- Manipulable (vulnérable à une pression sur elle-même ou son entourage)

Pré-requis pour la source de menace :

- Connaissance de l'existence et de la localisation de la personne
- Établissement d'une relation (hiérarchique, professionnelle, d'autorité, personnelle, sociale…) avec la personne

M24. PER-PTE – Départ d'une personne

La personne est perdue pour l'organisme, sans être affectée. Son savoir et son savoir faire ne sont plus disponibles pour l'organisme mais le deviennent pour autrui.

Départ, changement d'affectation, licenciement, enlèvement, rachat de tout ou partie de l'organisation.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	**Confidentialité**

Principales vulnérabilités exploitables :

- Faible loyauté vis-à-vis de l'organisme
- Faible satisfaction des besoins personnels (reconnaissance, salaire, motivation, ambiance, pérennité de l'emploi, incompatibilités déontologiques, déception professionnelle…)
- Facilité de rupture du lien contractuel

Pré-requis pour la source de menace :

- Connaissance de l'existence et de la localisation de la personne
- Établissement d'une relation (hiérarchique, professionnelle, d'autorité, personnelle, sociale…) avec la personne

Menaces sur les supports papier

M25. PAP-USG – Détournement de l'usage prévu d'un support papier

Le support papier est utilisé à d'autres fins que celles prévues, sans être modifié ni endommagé. Son contenu peut ainsi être réduit ou rendu indisponible.

Falsification d'un support papier (création ou modification du contenu d'un document papier…), effacement de données sur un support papier (usage d'un produit effaçant, disparition de contenus avec le temps…), utilisation du verso d'impressions papier en tant que brouillons ou afin d'économiser le papier.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	**Intégrité**	Confidentialité

Principales vulnérabilités exploitables :
- Utilisable en dehors de l'usage prévu (exploitation nominale des biens essentiels)
- Falsifiable (support papier au contenu modifiable ou effaçable)

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du matériel
- Accès physique au matériel (franchissement légitime ou non, ou contournement)

M26. PAP-ESP – Espionnage d'un support papier

Le support papier est observé, sans être endommagé, avec ou sans équipement de capture, depuis l'intérieur ou l'extérieur de locaux. Les informations contenues peuvent ainsi être compromises.

Lecture de supports papiers, photocopillage, photographie de dossiers papier.

Critère(s) de sécurité concerné(s) :	Disponibilité	Intégrité	**Confidentialité**

Principales vulnérabilités exploitables :
- Permet d'observer des données interprétables

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du support papier
- Accès physique au support papier (franchissement légitime ou non, ou contournement)

M27. PAP-DET – Détérioration d'un support papier

Le support papier est endommagé, partiellement ou totalement, temporairement ou définitivement, à l'intérieur ou à l'extérieur des locaux. Il peut ainsi ne plus pouvoir être utilisé.

Usure d'un support papier par vieillissement (naturel, accéléré en raison de l'usage de mauvais matériaux…), corrosion (agression chimique, pollution, humidification…), dégradation (vandalisme, accident…), embrasement.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

Principales vulnérabilités exploitables :
- Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement…)
- N'est pas approprié aux conditions d'utilisation (sensible à l'humidité…)

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du support papier
- Accès physique au support papier (franchissement légitime ou non, ou contournement)

M28. PAP-PTE – Perte d'un support papier

Le support papier est perdu, sans être endommagé, à l'intérieur ou à l'extérieur des locaux. Son contenu peut ainsi ne plus être disponible et l'être pour autrui.

Vol, perte ou prêt d'un support papier, revente ou mise au rebus d'un document papier, perte de document papier lors d'un déménagement.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	**Confidentialité**

Principales vulnérabilités exploitables :

- Portable

Pré-requis pour la source de menace :

- Connaissance de l'existence et de la localisation du support papier
- Accès physique au support papier (franchissement légitime ou non, ou contournement)

Menaces sur les canaux interpersonnels

M29. CAN-USG – Manipulation via un canal interpersonnel

Le canal interpersonnel est utilisé à d'autres fins que celles prévues, sans le modifier ni l'endommager. Le flux d'information qui transite peut ainsi être altéré, ralenti ou bloqué (suppression, modification, ajout, ralentissement, brouillage…).

Changement du contenu d'une note dans un circuit courrier, changement d'un parapheur par un autre, disparition d'une note dans un circuit courrier, disparition d'un parapheur, rumeur, désinformation, appropriation de temps de réunion à d'autres fins que celles prévues…

Critère(s) de sécurité concerné(s) :	**Disponibilité**	**Intégrité**	Confidentialité

Principales vulnérabilités exploitables :
- Permet d'altérer les flux communiqués (interception puis réémission, éventuellement après altération…)
- Seule ressource de transmission pour le flux
- Permet la modification du circuit organisationnel

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du canal interpersonnel
- Accès physique ou logique au canal interpersonnel (intégration légitime ou non d'un élément sur le canal)

M30. CAN-ESP – Espionnage d'un canal interpersonnel

Le canal interpersonnel est observé, sans être endommagé, avec ou sans matériel d'interception, depuis l'intérieur ou l'extérieur des locaux. Le flux d'information peut ainsi être écouté.

Récupération d'information au milieu d'un processus organisationnel, écoute de conversations lors de réunions ou à l'extérieur des locaux, pose d'un microphone dans un bureau.

Critère(s) de sécurité concerné(s) :	Disponibilité	Intégrité	**Confidentialité**

Principales vulnérabilités exploitables :
- Unique
- Observable

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du canal interpersonnel
- Accès physique ou logique au canal interpersonnel (intégration légitime ou non d'un élément sur le canal)

M31. CAN-DEP – Saturation d'un canal interpersonnel

Le canal interpersonnel est surchargé, partiellement ou totalement. Le flux d'information peut ainsi être ralentit ou bloqué.

Surcharge d'un processus de validation (ce qui peut mener à une perte ou à un ralentissement du flux d'informations), communication impossible du fait du bruit ambiant.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

Principales vulnérabilités exploitables :
- Existence de limites quantitatives ou qualitatives

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du canal interpersonnel
- Accès physique ou logique au canal interpersonnel (intégration légitime ou non d'un élément sur le canal)

M32. CAN-DET – Dégradation d'un canal interpersonnel

Le canal interpersonnel est endommagé, partiellement ou totalement, temporairement ou définitivement. Le flux d'information peut ainsi être ralentit ou bloqué.

Coupure d'un processus organisationnel du fait d'une réorganisation.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

Principales vulnérabilités exploitables :
- Instable
- Unique

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du canal interpersonnel
- Accès physique ou logique au canal interpersonnel (intégration légitime ou non d'un élément sur le canal)

M33. CAN-MOD – Modification d'un canal interpersonnel

Le canal interpersonnel est modifié. Le flux d'information qu'il supporte peut ainsi être ralentit ou bloqué.

Évolution inappropriée d'un processus organisationnel, changement de langue professionnelle.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

Principales vulnérabilités exploitables :
- Modifiable (remplaçable…)

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du canal interpersonnel
- Accès physique ou logique au canal interpersonnel (intégration légitime ou non d'un élément sur le canal)

M34. CAN-PTE – Disparition d'un canal interpersonnel

Le canal interpersonnel n'est plus présent, sans avoir été altéré. Le flux d'information ne peut plus transiter.

Disparition d'un processus organisationnel lors d'une réorganisation, disparition de réunions d'échanges d'informations.

Critère(s) de sécurité concerné(s) :	**Disponibilité**	Intégrité	Confidentialité

Principales vulnérabilités exploitables :
- Utilité non reconnue

Pré-requis pour la source de menace :
- Connaissance de l'existence et de la localisation du canal interpersonnel
- Accès physique ou logique au canal interpersonnel (intégration légitime ou non d'un élément sur le canal)

5 Mesures de sécurité génériques

Mesures de sécurité issues du [RGS]

Les mesures suivantes proviennent des chapitres du [RGS] intégrant des clauses qui peuvent être interprétées comme des mesures de sécurité. Les lignes de défense auxquelles elles contribuent ont été déterminées.

2. Un cadre pour gérer la sécurité des systèmes d'information

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
2.2. Six grands principes de gestion de la SSI	2.2.1.	Adopter une démarche globale	Voir [RGS]	X	X	X
2.2. Six grands principes de gestion de la SSI	2.2.2.	Adapter la SSI selon les enjeux	Voir [RGS]	X	X	X
2.2. Six grands principes de gestion de la SSI	2.2.3.	Gérer les risques SSI	Voir [RGS]	X	X	X
2.2. Six grands principes de gestion de la SSI	2.2.4.	Élaborer une politique SSI	Voir [RGS]	X	X	X
2.2. Six grands principes de gestion de la SSI	2.2.5.	Utiliser les produits et prestataires labellisés SSI	Voir [RGS]	X	X	
2.2. Six grands principes de gestion de la SSI	2.2.6.	Viser une amélioration continue	Voir [RGS]	X	X	X
2.3. Intégration de la SSI dans le cycle de vie des systèmes d'information	2.3.1.	Des efforts proportionnés aux enjeux SSI	Voir [RGS]	X	X	X
2.3. Intégration de la SSI dans le cycle de vie des systèmes d'information	2.3.2.	Un engagement systématique : l'homologation de sécurité	Voir [RGS]	X	X	X
2.3. Intégration de la SSI dans le cycle de vie des systèmes d'information	2.3.3.	Des outils ciblés pour les projets de système d'information	Voir [RGS]	X	X	X

3. Fonctions de sécurité

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
3.2. Authentification	3.2.1.	Utilisation de mécanismes cryptographiques	Voir [RGS]	X	X	
3.2. Authentification	3.2.2.	Utilisation des identifiants / mots de passe statiques	Voir [RGS]	X	X	
3.2. Authentification	3.2.3.	Authentification d'une personne par certificat électronique	Voir [RGS]	X	X	
3.2. Authentification	3.2.4.	Authentification d'un serveur par certificat électronique	Voir [RGS]	X	X	
3.3. Signature électronique	3.3.1.	Utilisation de mécanismes cryptographiques	Voir [RGS]	X	X	
3.3. Signature électronique	3.3.2.	Signature d'une personne par certificat électronique	Voir [RGS]	X	X	X
3.3. Signature électronique	3.3.3.	Cachet d'un serveur par certificat électronique	Voir [RGS]	X	X	X
3.4. Confidentialité	3.4.1.	Utilisation de mécanismes cryptographiques	Voir [RGS]	X	X	
3.4. Confidentialité	3.4.2.	Confidentialité par certificat électronique	Voir [RGS]	X	X	
3.4. Confidentialité	3.4.3.	Habilitations	Voir [RGS]	X		

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
3.5. Horodatage	3.5.1.	Utilisation des mécanismes cryptographiques	Voir [RGS]	X	X	X
3.5. Horodatage	3.5.2.	Horodatage par contremarques de temps	Voir [RGS]	X	X	X

4. Accusé d'enregistrement et de réception

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
4.2. Règles de sécurité	4.2.	Règles de sécurité	Voir [RGS]	X		X

5. Qualification

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
5.1. Qualification de produits de sécurité	5.1.2.	Qualification élémentaire	Voir [RGS]	X	X	
5.1. Qualification de produits de sécurité	5.1.3.	Qualification standard	Voir [RGS]	X	X	
5.1. Qualification de produits de sécurité	5.1.4.	Qualification renforcée	Voir [RGS]	X	X	

6. Les infrastructures de gestion de clés (IGC)

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
6.1. Règles et recommandations générales	6.1.	Règles et recommandations générales	Voir [RGS]	X	X	X
6.2. Cas particulier de la validation des certificats par l'État	6.2.2.	Règles de sécurité	Voir [RGS]	X	X	X

Mesures de sécurité issues de l'Annexe A de l'[ISO 27001] ou [ISO 27002]

Les mesures de sécurité suivantes proviennent des mesures de l'Annexe A de l'[ISO 27001] (ou de l'[ISO 27002]). Les lignes de défense auxquelles elles contribuent ont été déterminées.

5. Politique de sécurité

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
5.1. Politique de sécurité de l'information	5.1.1.	Document de politique de sécurité de l'information	Il convient qu'un document de politique de sécurité de l'information soit approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés.	X	X	X
5.1. Politique de sécurité de l'information	5.1.2.	Réexamen de la politique de sécurité de l'information	Pour garantir la pertinence, l'adéquation et l'efficacité de la politique de sécurité de l'information, il convient de réexaminer la politique à intervalles fixés préalablement ou en cas de changements majeurs.	X	X	X

6. Organisation de la sécurité de l'information

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
6.1. Organisation interne	6.1.1.	Engagement de la direction vis-à-vis de la sécurité de l'information	Il convient que la direction soutienne activement la politique de sécurité au sein de l'organisme au moyen de directives claires, d'un engagement franc, d'attribution de fonctions explicites et d'une reconnaissance des responsabilités liées à la sécurité de l'information.	X	X	X
6.1. Organisation interne	6.1.2.	Coordination de la sécurité de l'information	Il convient que les activités relatives à la sécurité de l'information soient coordonnées par des intervenants ayant des fonctions et des rôles appropriés représentatifs des différentes parties de l'organisme.	X	X	X
6.1. Organisation interne	6.1.3.	Attribution des responsabilités en matière de sécurité de l'information	Il convient de définir clairement toutes les responsabilités en matière de sécurité de l'information.	X	X	X
6.1. Organisation interne	6.1.4.	Système d'autorisation concernant les moyens de traitement de l'information	Il convient de définir et de mettre en oeuvre un système de gestion des autorisations pour chaque nouveau moyen de traitement de l'information.	X		
6.1. Organisation interne	6.1.5.	Engagements de confidentialité	Il convient d'identifier et de réexaminer régulièrement les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins de l'organisme.	X	X	
6.1. Organisation interne	6.1.6.	Relations avec les autorités	Il convient de mettre en place des relations appropriées avec les autorités compétentes.	X		X
6.1. Organisation interne	6.1.7.	Relations avec des groupes de spécialistes	Il convient d'entretenir des contacts appropriés avec des groupes de spécialistes, des forums spécialisés dans la sécurité et des associations professionnelles.	X	X	
6.1. Organisation interne	6.1.8.	Revue indépendante de la sécurité de l'information	Il convient de procéder à des revues régulières et indépendantes de l'approche retenue par l'organisme pour gérer et mettre en oeuvre sa sécurité (à savoir le suivi des objectifs de sécurité, les politiques, les procédures et les processus relatifs à la sécurité de l'information); de telles revues sont également nécessaires lorsque des changements importants sont intervenus dans la mise en oeuvre de la sécurité.	X	X	X
6.2. Tiers	6.2.1.	Identification des risques provenant des tiers	Il convient d'identifier les risques pesant sur l'information et les moyens de traitement de l'organisme qui découlent d'activités impliquant des tiers, et de mettre en oeuvre des mesures appropriées avant d'accorder des accès.	X	X	
6.2. Tiers	6.2.2.	La sécurité et les clients	Tous les besoins de sécurité doivent être traités avant d'accorder aux clients l'accès à l'information ou aux biens de l'organisme.	X	X	
6.2. Tiers	6.2.3.	La sécurité dans les accords conclus avec des tiers	Il convient que les accords conclus avec des tiers qui portent sur l'accès, le traitement, la communication ou la gestion de l'information, ou des moyens de traitement de l'information de l'organisme, ou qui portent sur l'ajout de produits ou de services aux moyens de traitement de l'information, couvrent l'ensemble des exigences applicables en matière de sécurité.	X	X	X

7. Gestion des biens

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
7.1. Responsabilités relatives aux biens	7.1.1.	Inventaire des biens	Il convient de clairement identifier tous les biens, de réaliser et de gérer un inventaire de tous les biens importants.	X	X	X
7.1. Responsabilités relatives aux biens	7.1.2.	Propriété des biens	Il convient d'attribuer la propriété de chaque information et moyens de traitement de l'information à une partie définie de l'organisme.	X	X	X
7.1. Responsabilités relatives aux biens	7.1.3.	Utilisation correcte des biens	Il convient d'identifier, de documenter et de mettre en oeuvre des règles permettant l'utilisation correcte de l'information et des biens associés aux moyens de traitement de l'information.	X	X	
7.2. Classification des informations	7.2.1.	Lignes directrices pour la classification	Il convient de classer les informations en termes de valeur, d'exigences légales, de sensibilité et de criticité.	X		
7.2. Classification des informations	7.2.2.	Marquage et manipulation de l'information	Il convient d'élaborer et de mettre en oeuvre un ensemble approprié de procédures pour le marquage et la manipulation de l'information, conformément au plan de classification adopté par l'organisme.	X	X	

8. Sécurité liée aux ressources humaines

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
8.1. Avant le recrutement	8.1.1.	Rôles et responsabilités	Il convient de définir et de documenter les rôles et responsabilités en matière de sécurité des salariés, contractants et utilisateurs tiers, conformément à la politique de sécurité de l'information de l'organisme.	X	X	
8.1. Avant le recrutement	8.1.2.	Sélection	Qu'il s'agisse de postulants, de contractants ou d'utilisateurs tiers, il convient que les vérifications des informations concernant tous les candidats soient réalisées conformément aux lois, aux règlements et à l'étique et qu'elles soient proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés.	X		
8.1. Avant le recrutement	8.1.3.	Conditions d'embauche	Dans le cadre de leurs obligations contractuelles, il convient que les salariés, contractants et utilisateurs tiers se mettent d'accord sur les modalités du contrat d'embauche les liant et le signent. Il convient que ce contrat définisse les responsabilités de l'organisme et de l'autre partie quant à la sécurité de l'information.	X		
8.2. Pendant la durée du contrat	8.2.1.	Responsabilités de la direction	Il convient que la direction demande aux salariés, contractants et utilisateurs tiers d'appliquer les règles de sécurité conformément aux politiques et procédures établies de l'organisme.	X	X	
8.2. Pendant la durée du contrat	8.2.2.	Sensibilisation, qualification et formations en matière de sécurité de l'information	Il convient que l'ensemble des salariés d'un organisme et, le cas échant, les contractants et utilisateurs tiers suivent une formation adaptée sur la sensibilisation et reçoivent régulièrement les mises à jour des politiques et procédures de l'organisme, pertinentes pour leurs fonctions.	X	X	
8.2. Pendant la durée du contrat	8.2.3.	Processus disciplinaire	Il convient d'élaborer un processus disciplinaire formel pour les salariés ayant enfreint les règles de sécurité.	X	X	
8.3. Fin ou modification de contrat	8.3.1.	Responsabilités en fin de contrat	Il convient que les responsabilités relatives aux fins ou aux modifications de contrats soient clairement définies et attribuées.	X	X	
8.3. Fin ou modification de contrat	8.3.2.	Restitution des biens	Il convient que tous les salariés, contractants et utilisateurs tiers restituent la totalité des biens de l'organisme qu'ils ont en leur possession à la fin de leur période d'emploi, contrat ou accord.	X		
8.3. Fin ou modification de contrat	8.3.3.	Retrait des droits d'accès	Il convient que les droits d'accès de l'ensemble des salariés, contractants et utilisateurs tiers à l'information et aux moyens de traitement de l'information soient supprimés à la fin de leur période d'emploi, ou modifiés en cas de modification du contrat ou de l'accord.	X	X	

9. Sécurité physique et environnementale

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
9.1. Zones sécurisées	9.1.1.	Périmètre de sécurité physique	Il convient de protéger les zones contenant des informations et des moyens de traitement de l'information par des périmètres de sécurité (obstacles tels que des murs, des portes avec un contrôle d'accès par cartes, ou des bureaux de réception avec personnel d'accueil).	X	X	
9.1. Zones sécurisées	9.1.2.	Contrôles physiques des accès	Il convient de protéger les zones sécurisées par des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis.	X	X	
9.1. Zones sécurisées	9.1.3.	Sécurisation des bureaux, des salles et des équipements	Il convient de concevoir et d'appliquer des mesures de sécurité physique pour les bureaux, les salles et les équipements.	X	X	
9.1. Zones sécurisées	9.1.4.	Protection contre les menaces extérieures et environnementales	Il convient de concevoir et d'appliquer des mesures de protection physique contre les dommages causés par les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et autres formes de catastrophes naturelles ou de sinistres provoqués par l'homme.	X	X	
9.1. Zones sécurisées	9.1.5.	Travail dans les zones sécurisées	Il convient de concevoir et d'appliquer des mesures de protection physique et des directives pour le travail en zone sécurisée.	X	X	
9.1. Zones sécurisées	9.1.6.	Zones d'accès public, de livraison et de chargement	Il convient de contrôler les points d'accès tels que les zones de livraison/chargement et les autres points par lesquels des personnes non habilitées peuvent pénétrer dans les locaux. Il convient également d'isoler les points d'accès, si possible, des moyens de traitement de l'information, de façon à éviter les accès non autorisés.	X	X	
9.2. Sécurité du matériel	9.2.1.	Choix de l'emplacement et protection du matériel	Il convient de situer et de protéger le matériel de manière à réduire les risques de menaces et de dangers environnementaux et les possibilités d'accès non autorisé.	X	X	
9.2. Sécurité du matériel	9.2.2.	Services généraux	Il convient de protéger le matériel des coupures de courant et autres perturbations dues à une défaillance des services généraux.	X	X	X
9.2. Sécurité du matériel	9.2.3.	Sécurité du câblage	Il convient de protéger les câbles électriques ou de télécommunications transportant des données contre toute interception ou dommage.		X	
9.2. Sécurité du matériel	9.2.4.	Maintenance du matériel	Il convient d'entretenir le matériel correctement pour garantir sa disponibilité permanente et son intégrité.	X	X	
9.2. Sécurité du matériel	9.2.5.	Sécurité du matériel hors des locaux	Il convient d'appliquer la sécurité au matériel utilisé hors des locaux de l'organisme en tenant compte des différents risques associés au travail hors site.	X		
9.2. Sécurité du matériel	9.2.6.	Mise au rebut ou recyclage sécurisé(e) du matériel	Il convient de vérifier tout le matériel contenant des supports de stockage soient vérifiées pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut.	X	X	
9.2. Sécurité du matériel	9.2.7.	Sortie d'un bien	Il convient de ne pas sortir un matériel, des informations ou des logiciels des locaux de l'organisme sans autorisation préalable.	X	X	

10. Gestion de l'exploitation et des télécommunications

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
10.1. Procédures et responsabilités liées à l'exploitation	10.1.1.	Procédures d'exploitation documentées	Il convient que les procédures d'exploitation soient documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.	X	X	X
10.1. Procédures et responsabilités liées à l'exploitation	10.1.2	Gestion des modifications	Il convient de contrôler les changements apportés aux systèmes et moyens de traitement de l'information.	X	X	
10.1. Procédures et responsabilités liées à l'exploitation	10.1.3.	Séparation des tâches	Il convient de séparer les tâches et les domaines de responsabilité pour réduire les occasions de modification ou de mauvais usage non autorisé(e) ou involontaire des biens de l'organisme.	X	X	
10.1. Procédures et responsabilités liées à l'exploitation	10.1.4.	Séparation des équipements de développement, de test et d'exploitation	Il convient de séparer les équipements de développement, de test et d'exploitation pour réduire les risques d'accès ou de changements non autorisés dans le système en exploitation.	X	X	
10.2. Gestion de la prestation de service par un tiers	10.2.1.	Prestation de service	Il convient de s'assurer que les mesures de sécurité, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers sont mis en œuvre, appliqués et tenus à jour par le tiers.	X	X	X
10.2. Gestion de la prestation de service par un tiers	10.2.2.	Surveillance et réexamen des services tiers	Il convient que les services, rapports et enregistrements fournis par les tiers soient régulièrement contrôlés et réexaminés, et que des audits soient régulièrement réalisés.		X	
10.2. Gestion de la prestation de service par un tiers	10.2.3.	Gestion des modifications dans les services tiers	Il convient de gérer les changements effectués dans la prestation de service, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, en tenant compte de la criticité des systèmes et processus de gestion concernés et de la réévaluation du risque.	X	X	
10.3. Planification et acceptation du système	10.3.1.	Dimensionnement	Il convient de surveiller et d'ajuster au plus près l'utilisation des ressources et il convient de faire des projections sur les dimensionnements futurs pour assurer les performances requises pour le système.	X		
10.3. Planification et acceptation du système	10.3.2.	Acceptation du système	Il convient de fixer les critères d'acceptation pour les nouveaux systèmes d'information, les nouvelles versions et les mises à niveau, et de réaliser les tests adaptés du (des) système(s) au moment du développement et préalablement à leur acceptation.		X	
10.4. Protection contre les codes malveillant et mobile	10.4.1.	Mesures contre les codes malveillants	Il convient de mettre en œuvre des mesures de détection, de prévention et de récupération pour se protéger des codes malveillants ainsi que des procédures appropriées de sensibilisation des utilisateurs.	X	X	X
10.4. Protection contre les codes malveillant et mobile	10.4.2	Mesures contre le code mobile	Lorsque l'utilisation de code mobile est autorisée, il convient que la configuration garantisse que le code mobile fonctionne selon une politique de sécurité clairement définie et il convient d'empêcher tout code mobile non autorisé de s'exécuter.	X	X	
10.5. Sauvegarde	10.5.1.	Sauvegarde des informations	Il convient de réaliser des copies de sauvegarde des informations et logiciels et de les soumettre régulièrement à essai conformément à la politique de sauvegarde convenue.	X	X	X
10.6. Gestion de la sécurité des réseaux	10.6.1.	Mesures sur les réseaux	Il convient de gérer et de contrôler les réseaux de manière adéquate pour qu'ils soient protégés des menaces et de maintenir la sécurité des systèmes et des applications utilisant le réseau, notamment les informations en transit.		X	
10.6. Gestion de la sécurité des réseaux	10.6.2.	Sécurité des services réseau	Pour tous les services réseau, il convient d'identifier les fonctions réseau, les niveaux de service et les exigences de gestion, et de les intégrer dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.	X	X	
10.7. Manipulation des supports	10.7.1.	Gestion des supports amovibles	Il convient de mettre en place des procédures pour la gestion des supports amovibles.	X	X	
10.7. Manipulation des supports	10.7.2.	Mise au rebut des supports	Il convient de mettre au rebut de façon sûre les supports qui ne servent plus, en suivant des procédures formelles.	X	X	
10.7. Manipulation des supports	10.7.3.	Procédures de manipulation des informations	Il convient d'établir des procédures de manipulation et de stockage des informations pour protéger ces informations d'une divulgation non autorisée ou d'un mauvais usage.	X	X	
10.7. Manipulation des supports	10.7.4.	Sécurité de la documentation système	Il convient de protéger la documentation système contre les accès non autorisés.		X	
10.8. Échange des informations	10.8.1.	Politiques et procédures d'échange des informations	Il convient de mettre en place des politiques, procédures et mesures d'échange formelles pour protéger les échanges d'informations transitant par tous types d'équipements de télécommunication.	X	X	
10.8. Échange des informations	10.8.2.	Accords d'échange	Il convient de conclure des accords pour l'échange d'informations et de logiciels entre l'organisme et la partie externe.	X	X	

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
10.8. Échange des informations	10.8.3.	Supports physiques en transit	Il convient de protéger les supports contenant des informations contre les accès non autorisés, le mauvais usage ou l'altération lors du transport hors des limites physiques de l'organisme.	X	X	
10.8. Échange des informations	10.8.4.	Messagerie électronique	Il convient de protéger de manière adéquate les informations transitant par la messagerie électronique.	X	X	
10.8. Échange des informations	10.8.5.	Systèmes d'information d'entreprise	Il convient d'élaborer et de mettre en œuvre des politiques et procédures pour protéger l'information liée à l'interconnexion de systèmes d'informations d'entreprise.	X	X	X
10.9. Services de commerce électronique	10.9.1.	Commerce électronique	Il convient de protéger l'information transitant par le commerce électronique transmise sur les réseaux publics contre les activités frauduleuses, les litiges sur les contrats et la divulgation et la modification non autorisées.	X	X	
10.9. Services de commerce électronique	10.9.2.	Transactions en ligne	Il convient de protéger les informations transitant par les transactions en ligne pour empêcher la transmission incomplète, les erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou la réémission.	X	X	
10.9. Services de commerce électronique	10.9.3.	Informations à disposition du public	Il convient de protéger l'intégrité des informations mises à disposition sur un système accessible au public pour empêcher toute modification non autorisée.		X	
10.10. Surveillance	10.10.1.	Rapport d'audit	Il convient que les rapports d'audit, qui enregistrent les activités des utilisateurs, les exceptions et les événements liés à la sécurité soient produits et conservés pendant une période préalablement définie afin de faciliter les investigations ultérieures et la surveillance du contrôle d'accès.	X	X	X
10.10. Surveillance	10.10.2.	Surveillance de l'exploitation du système	Il convient d'établir des procédures permettant de surveiller l'utilisation des moyens de traitement de l'information et de réexaminer périodiquement les résultats des activités de surveillance.	X	X	X
10.10. Surveillance	10.10.3.	Protection des informations journalisées	Il convient de protéger les équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés.	X	X	
10.10. Surveillance	10.10.4.	Journal administrateur et journal des opérations	Il convient de journaliser les activités de l'administrateur système et de l'opérateur système.	X	X	
10.10. Surveillance	10.10.5.	Rapports de défaut	Il convient de journaliser et d'analyser les éventuels défauts et de prendre les mesures appropriées.		X	X
10.10. Surveillance	10.10.6.	Synchronisation des horloges	Il convient de synchroniser les horloges des différents systèmes de traitement de l'information d'un organisme ou d'un domaine de sécurité à l'aide d'une source de temps précise et préalablement définie.	X	X	

11. Contrôle d'accès

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
11.1. Exigences métier relatives au contrôle d'accès	11.1.1.	Politique de contrôle d'accès	Il convient d'établir, de documenter et de réexaminer une politique de contrôle d'accès sur la base des exigences d'exploitation et de sécurité.	X	X	
11.2. Gestion de l'accès utilisateur	11.2.1.	Enregistrement des utilisateurs	Il convient de définir une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à accorder et à supprimer l'accès à tous les systèmes et services d'information.	X		
11.2. Gestion de l'accès utilisateur	11.2.2.	Gestion des privilèges	Il convient de restreindre et de contrôler l'attribution et l'utilisation des privilèges.	X	X	
11.2. Gestion de l'accès utilisateur	11.2.3.	Gestion du mot de passe utilisateur	Il convient que l'attribution de mots de passe soit réalisée dans le cadre d'un processus formel.		X	
11.2. Gestion de l'accès utilisateur	11.2.4.	Réexamen des droits d'accès utilisateurs	Il convient que la direction revoie les droits d'accès utilisateurs à intervalles réguliers par le biais d'un processus formel.	X	X	
11.3. Responsabilités utilisateurs	11.3.1.	Utilisation du mot de passe	Il convient de demander aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.	X	X	
11.3. Responsabilités utilisateurs	11.3.2.	Matériel utilisateur laissé sans surveillance	Il convient que les utilisateurs s'assurent que tout matériel laissé sans surveillance est doté d'un dispositif de protection approprié.	X	X	
11.3. Responsabilités utilisateurs	11.3.3.	Politique du bureau propre et de l'écran vide	Il convient d'adopter une politique du bureau propre pour les documents papier et les supports de stockage amovibles, et une politique de l'écran vide pour les moyens de traitement de l'information.	X	X	
11.4. Contrôle d'accès au réseau	11.4.1.	Politique relative à l'utilisation des services en réseau	Il convient que les utilisateurs aient uniquement accès aux services pour lesquels ils ont spécifiquement reçu une autorisation.	X	X	
11.4. Contrôle d'accès au réseau	11.4.2.	Authentification de l'utilisateur pour les connexions externes	Il convient d'utiliser des méthodes d'authentification appropriées pour contrôler l'accès d'utilisateurs distants.	X	X	
11.4. Contrôle d'accès au réseau	11.4.3.	Identification des matériels en réseau	Il convient de considérer l'identification automatique de matériels comme un moyen d'authentification des connexions à partir de lieux et matériels spécifiques.	X	X	
11.4. Contrôle d'accès au réseau	11.4.4.	Protection des ports de diagnostic et de configuration à distance	Il convient de contrôler l'accès physique et logique aux ports de diagnostic et de configuration à distance.	X	X	
11.4. Contrôle d'accès au réseau	11.4.5.	Cloisonnement des réseaux	Il convient que les groupes de services d'information, d'utilisateurs et de systèmes d'information soient séparés sur le réseau.	X	X	
11.4. Contrôle d'accès au réseau	11.4.6.	Mesure relative à la connexion réseau	Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme, il convient de restreindre la capacité de connexion réseau des utilisateurs, conformément à la politique de contrôle d'accès et les exigences relatives aux applications de gestion.	X	X	
11.4. Contrôle d'accès au réseau	11.4.7.	Contrôle du routage réseau	Il convient de mettre en oeuvre des mesures du routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	X	X	
11.5. Contrôle d'accès au système d'exploitation	11.5.1.	Ouverture de sessions sécurisées	Il convient que l'accès aux systèmes d'exploitation soit soumis à une procédure sécurisée d'ouverture de session.	X	X	
11.5. Contrôle d'accès au système d'exploitation	11.5.2.	Identification et authentification de l'utilisateur	Il convient d'attribuer à chaque utilisateur un identifiant unique et exclusif et de choisir une technique d'authentification permettant de vérifier l'identité déclarée par l'utilisateur.	X	X	
11.5. Contrôle d'accès au système d'exploitation	11.5.3.	Système de gestion des mots de passe	Il convient que les systèmes qui gèrent les mots de passe soient interactifs et fournissent des mots de passe de qualité.	X	X	
11.5. Contrôle d'accès au système d'exploitation	11.5.4.	Emploi des utilitaires système	Il convient de limiter et de contrôler étroitement l'emploi des programmes utilitaires permettant de contourner les mesures d'un système ou d'une application.		X	
11.5. Contrôle d'accès au système d'exploitation	11.5.5.	Déconnexion automatique des sessions inactives	Il convient que les sessions inactives soient déconnectées après une période d'inactivité définie.	X	X	X
11.5. Contrôle d'accès au système d'exploitation	11.5.6.	Limitation du temps de connexion	Il convient de restreindre les temps de connexion afin d'apporter un niveau de sécurité supplémentaire aux applications à haut risque.	X		
11.6. Contrôle d'accès aux applications et à l'information	11.6.1.	Restriction d'accès à l'information	Pour les utilisateurs et le personnel chargé de l'assistance technique, il convient de restreindre l'accès aux informations et aux fonctions applicatives conformément à la politique de contrôle d'accès.	X	X	

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
11.6. Contrôle d'accès aux applications et à l'information	11.6.2.	Isolement des systèmes sensibles	Il convient que les systèmes sensibles disposent d'un environnement informatique dédié (isolé).	X	X	
11.7. Informatique mobile et télétravail	11.7.1.	Informatique mobile et télécommunications	Il convient de mettre en place une procédure formelle et des mesures de sécurité appropriées pour assurer une protection contre le risque lié à l'utilisation d'appareils informatiques et de communication mobiles.		X	
11.7. Informatique mobile et télétravail	11.7.2.	Télétravail	Il convient d'élaborer et de mettre en oeuvre une politique, des procédures et des programmes opérationnels spécifiques au télétravail.		X	

12. Acquisition, développement et maintenance des systèmes d'information

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
12.1. Exigences de sécurité applicables aux systèmes d'information	12.1.1.	Analyse et spécification des exigences de sécurité	Il convient que les exigences métier relatives aux nouveaux systèmes d'information ou que les améliorations apportées aux systèmes d'information existants spécifient les exigences de sécurité.	X		
12.2. Bon fonctionnement des applications	12.2.1.	Validation des données d'entrée	Il convient de valider les données entrées dans les applications afin de vérifier si elles sont correctes et appropriées.	X		
12.2. Bon fonctionnement des applications	12.2.2.	Mesure relative au traitement interne	Il convient d'inclure des mesures de validation dans les applications afin de détecter les éventuelles altérations de l'information dues à des erreurs de traitement ou des actes délibérés.		X	
12.2. Bon fonctionnement des applications	12.2.3.	Intégrité des messages	Il convient d'identifier les exigences relatives à l'authentification et à la protection de l'intégrité des messages. Il convient également d'identifier et de mettre en œuvre les mesures appropriées.	X		
12.2. Bon fonctionnement des applications	12.2.4.	Validation des données de sortie	Il convient de valider les données de sortie d'une application pour vérifier que le traitement des informations stockées est correct et adapté aux circonstances.		X	
12.3. Mesures cryptographiques	12.3.1.	Politique d'utilisation des mesures cryptographiques	Il convient d'élaborer et de mettre en œuvre une politique d'utilisation des mesures cryptographiques en vue de protéger l'information.	X		
12.3. Mesures cryptographiques	12.3.2.	Gestion des clés	Il convient qu'une procédure de gestion des clés vienne à l'appui de la politique de l'organisme en matière de chiffrement.	X		
12.4. Sécurité des fichiers système	12.4.1.	Mesure relative aux logiciels en exploitation	Il convient de mettre des procédures en place pour contrôler l'installation du logiciel sur les systèmes en exploitation.	X		
12.4. Sécurité des fichiers système	12.4.2.	Protection des données système d'essai	Il convient que les données d'essai soient sélectionnées avec soin, protégées et contrôlées.		X	
12.4. Sécurité des fichiers système	12.4.3.	Contrôle d'accès au code source du programme	Il convient de restreindre l'accès au code source du programme.	X	X	
12.5. Sécurité en matière de développement et d'assistance technique	12.5.1.	Procédures de contrôle des modifications	Il convient de contrôler la mise en œuvre des modifications par le biais de procédures formelles.	X		
12.5. Sécurité en matière de développement et d'assistance technique	12.5.2.	Réexamen technique des applications après modification du système d'exploitation	Lorsque des modifications sont apportées aux systèmes d'exploitation, il convient de réexaminer et de soumettre à essai les applications critiques de gestion afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.		X	
12.5. Sécurité en matière de développement et d'assistance technique	12.5.3.	Restrictions relatives à la modification des progiciels	Il convient de ne pas encourager la modification des progiciels et de se limiter aux changements nécessaires. Il convient également d'exercer un contrôle strict sur ces modifications.	X	X	
12.5. Sécurité en matière de développement et d'assistance technique	12.5.4.	Fuite d'informations	Il convient d'empêcher toute possibilité de fuite d'informations.	X	X	
12.5. Sécurité en matière de développement et d'assistance technique	12.5.5.	Externalisation du développement logiciel	Il convient que l'organisme encadre et contrôle le développement logiciel externalisé.	X	X	
12.6. Gestion des vulnérabilités techniques	12.6.1.	Mesure relative aux vulnérabilités techniques	Il convient d'être informé en temps voulu de toute vulnérabilité technique des systèmes d'information en exploitation, d'évaluer l'exposition de l'organisme audites vulnérabilités et d'entreprendre les actions appropriées pour traiter le risque associé.	X		

13. Gestion des incidents liés à la sécurité de l'information

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
13.1. Signalement des événements et des failles liés à la sécurité de l'information	13.1.1.	Signalement des événements liés à la sécurité de l'information	Il convient de signaler, dans les meilleurs délais, les événements liés à la sécurité de l'information, par les voies hiérarchiques appropriées.		X	X
13.1. Signalement des événements et des failles liés à la sécurité de l'information	13.1.2.	Signalement des failles de sécurité	Il convient de demander à tous les salariés, contractants et utilisateurs tiers des systèmes et services d'information de noter et de signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.	X	X	
13.2. Gestion des améliorations et incidents liés à la sécurité de l'information	13.2.1.	Responsabilités et procédures	Il convient d'établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.			X
13.2. Gestion des améliorations et incidents liés à la sécurité de l'information	13.2.2.	Exploitation des incidents liés à la sécurité de l'information déjà survenus	Il convient de mettre en place des mécanismes permettant de quantifier et surveiller les différents types d'incidents liés à la sécurité de l'information ainsi que leur volume et les coûts associés.	X		X
13.2. Gestion des améliorations et incidents liés à la sécurité de l'information	13.2.3.	Collecte de preuves	Lorsqu'une action en justice civile ou pénale est engagée contre une personne physique ou un organisme, à la suite d'un incident lié à la sécurité de l'information, il convient de recueillir, conserver et présenter les informations conformément aux dispositions légales relatives à la présentation de preuves régissant la ou les juridiction(s) compétente(s).	X	X	X

14. Gestion du plan de continuité de l'activité

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité	14.1.1.	Intégration de la sécurité de l'information dans le processus de gestion du plan de continuité de l'activité	Il convient d'élaborer et de gérer un processus de continuité de l'activité dans l'ensemble de l'organisme qui satisfait aux exigences en matière de sécurité de l'information requises pour la continuité de l'activité de l'organisme.	X		X
14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité	14.1.2.	Continuité de l'activité et appréciation du risque	Il convient d'identifier les événements pouvant être à l'origine d'interruptions des processus métier tout comme la probabilité et l'impact de telles interruptions et leurs conséquences pour la sécurité de l'information.	X		X
14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité	14.1.3.	Élaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	Il convient d'élaborer et de mettre en œuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.			X
14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité	14.1.4.	Cadre de la planification de la continuité de l'activité	Il convient gérer un cadre unique pour les plans de continuité de l'activité afin de garantir la cohérence de l'ensemble des plans, de satisfaire de manière constante aux exigences en matière de sécurité de l'information et d'identifier les priorités en matière de mise à l'essai et de maintenance.			X
14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité	14.1.5.	Mise à l'essai, gestion et appréciation constante des plans de continuité de l'activité	Il convient de soumettre à essai et de mettre à jour régulièrement les plans de continuité de l'activité afin de s'assurer qu'ils sont actualisés et efficaces.			X

15. Conformité

Sous-chapitre	N°	Mesure de sécurité	Description	Prév.	Prot.	Récu.
15.1. Conformité avec les exigences légales	15.1.1.	Identification de la législation en vigueur	Pour chaque système d'information et pour l'organisme, il convient de définir, documenter et mettre à jour explicitement toutes les exigences légales, réglementaires et contractuelles en vigueur, ainsi que la procédure utilisée par l'organisme pour satisfaire à ces exigences.		X	
15.1. Conformité avec les exigences légales	15.1.2.	Droits de propriété intellectuelle	Il convient de mettre en oeuvre des procédures appropriées visant à garantir la conformité avec les exigences légales, réglementaires et contractuelles concernant l'utilisation du matériel pouvant être soumis à des droits de propriété intellectuelle et l'utilisation des logiciels propriétaires.		X	
15.1. Conformité avec les exigences légales	15.1.3.	Protection des enregistrements de l'organisme	Il convient de protéger les enregistrements importants de la perte, destruction et falsification conformément aux exigences légales, réglementaires et aux exigences métier.		X	X
15.1. Conformité avec les exigences légales	15.1.4.	Protection des données et confidentialité des informations relatives à la vie privée	Il convient de garantir la protection et la confidentialité des données telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant.		X	
15.1. Conformité avec les exigences légales	15.1.5.	Mesure préventive à l'égard du mauvais usage des moyens de traitement de l'information	Il convient de dissuader les utilisateurs de toute utilisation de moyens de traitement de l'information à des fins illégales.	X	X	
15.1. Conformité avec les exigences légales	15.1.6.	Réglementation relative aux mesures cryptographiques	Il convient de prendre des mesures cryptographiques conformément aux accords, lois et réglementations applicables.		X	
15.2. Conformité avec les politiques et normes de sécurité et conformité technique	15.2.1.	Conformité avec les politiques et les normes de sécurité	Il convient que les responsables s'assurent de l'exécution correcte de l'ensemble des procédures de sécurité placées sous leur responsabilité en vue de garantir leur conformité avec les politiques et normes de sécurité.	X	X	
15.2. Conformité avec les politiques et normes de sécurité et conformité technique	15.2.2.	Vérification de la conformité technique	Il convient de vérifier régulièrement la conformité des systèmes d'information avec les normes relatives à la mise en oeuvre de la sécurité.			X
15.3. Prises en compte de l'audit du système d'information	15.3.1.	Contrôles de l'audit du système d'information	Il convient que les exigences d'audit et les activités impliquant des contrôles des systèmes en exploitation soient planifiées de manière précise et qu'elles soient le résultat d'un accord afin de réduire le plus possible le risque de perturbations des processus métier.	X	X	
15.3. Prises en compte de l'audit du système d'information	15.3.2.	Protection des outils d'audit du système d'information	Il convient de protéger l'accès aux outils d'audit du système d'information afin d'empêcher tous mauvais usage ou compromission éventuels.		X	

Annexes

Correspondance entre les nouvelles menaces et celles d'EBIOSv2

Le tableau suivant montre que les méthodes d'attaque de la méthode EBIOSv2 sont parfaitement prises en compte dans les menaces génériques des présentes bases de connaissances.

Nouvelles menaces / Méthodes d'attaque EBIOSv2	M1. MAT-USG	M2. MAT-ESP	M3. MAT-DEP	M4. MAT-DET	M5. MAT-MOD	M6. MAT-PTE	M7. LOG-USG	M8. LOG-ESP	M9. LOG-DEP	M10. LOG-DET	M11. LOG-MOD	M12. LOG-PTE	M13. RSX-USG	M14. RSX-ESP	M15. RSX-DEP	M16. RSX-DET	M17. RSX-MOD	M18. RSX-PTE	M19. PER-USG	M20. PER-ESP	M21. PER-DEP	M22. PER-DET	M23. PER-MOD	M24. PER-PTE	M25. PAP-USG	M26. PAP-ESP	M27. PAP-DET	M28. PAP-PTE	M29. CAN-USG	M30. CAN-ESP	M31. CAN-DEP	M32. CAN-DET	M33. CAN-MOD	M34. CAN-PTE
1. Incendie				X												X						X					X							
2. Dégâts des eaux				X												X			X								X							
3. Pollution				X																		X					X							
4. Sinistre majeur				X												X						X					X							
5. Destruction de matériels ou de supports				X																							X							
6. Phénomène climatique			X	X											X	X					X	X					X							
7. Phénomène sismique				X												X			X			X					X							
8. Phénomène volcanique				X												X			X			X					X							
9. Phénomène météorologique			X	X											X	X			X		X	X					X							
10. Crue				X												X			X			X					X							
11. Défaillance de la climatisation			X																		X													
12. Perte d'alimentation énergétique			X																															
13. Perte des moyens de télécommunication													X		X	X	X	X																
14. Rayonnements électromagnétiques			X																															
15. Rayonnements thermiques			X																		X													
16. Impulsions électromagnétiques				X																														
17. Interception de signaux parasites compromettants		X												X																				
18. Espionnage à distance		X												X						X						X				X				
19. Écoute passive														X																X				

Nouvelles menaces / Méthodes d'attaque EBIOSv2	M1. MAT-USG	M2. MAT-ESP	M3. MAT-DEP	M4. MAT-DET	M5. MAT-MOD	M6. MAT-PTE	M7. LOG-USG	M8. LOG-ESP	M9. LOG-DEP	M10. LOG-DET	M11. LOG-MOD	M12. LOG-PTE	M13. RSX-USG	M14. RSX-ESP	M15. RSX-DEP	M16. RSX-DET	M17. RSX-MOD	M18. RSX-PTE	M19. PER-USG	M20. PER-ESP	M21. PER-DEP	M22. PER-DET	M23. PER-MOD	M24. PER-PTE	M25. PAP-USG	M26. PAP-ESP	M27. PAP-DET	M28. PAP-PTE	M29. CAN-USG	M30. CAN-ESP	M31. CAN-DEP	M32. CAN-DET	M33. CAN-MOD	M34. CAN-PTE
20. Vol de supports ou de documents						X																						X						
21. Vol de matériels						X																												
22. Récupération de supports recyclés ou mis au rebut						X																						X						
23. Divulgation																				X			X						X					
24. Informations sans garantie de l'origine							X																						X					
25. Piégeage du matériel					X																													
26. Piégeage du logiciel											X																							
27. Géolocalisation		X																																
28. Panne matérielle	X		X	X	X																													
29. Dysfonctionnement du matériel	X		X	X	X																													
30. Saturation du système d'information			X						X						X						X										X			
31. Dysfonctionnement logiciel							X		X	X	X																							
32. Atteinte à la maintenabilité du système d'information	X		X	X	X		X		X	X	X		X		X	X	X																	
33. Utilisation illicite des matériels	X																																	
34. Copie frauduleuse de logiciels							X	X				X																						
35. Utilisation de logiciels contrefaits ou copiés							X																											
36. Altération des données							X		X	X	X		X						X		X		X						X					
37. Traitement illicite des données							X																		X				X					
38. Erreur d'utilisation	X		X	X	X		X		X	X	X		X		X	X	X																	
39. Abus de droits	X						X						X						X										X					
40. Usurpation de droits	X		X		X		X		X		X								X		X		X						X					
41. Reniement d'actions	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
42. Atteinte à la disponibilité du personnel																			X		X	X	X	X										

Références bibliographiques

[ISO 15408] *Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information*, International Organization for Standardization – ISO (2005).

[ISO 27001] *Information technology – Security Techniques – Information security management systems – Requirements*, International Organization for Standardization – ISO (2005).

[ISO 27002] *Information technology – Code of practice for information security management*, International Organization for Standardization – ISO (2005).

[RGS] *Référentiel général de sécurité* – ANSSI (2010).