Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

Office fédéral de la cybersécurité OFCS

20 novembre 2025

Méthode de cybersécurité et de résilience (MCSR)

Une approche structurée pour renforcer la cybersécurité et la résilience

Table des matières

1 Introduction

Dans le présent document, l'Office fédéral de la cybersécurité (OFCS) propose une approche structurée dont le but est de renforcer la cybersécurité et la résilience des organisations et des entreprises, indépendamment de leur taille et de leur secteur d'activité. Cette approche est désignée ci-après sous les termes de *méthode de cybersécurité et de résilience (MCSR)* ou, simplement, de *méthode*.[1]

La MCSR repose sur les normes, les recommandations et les bonnes pratiques pertinentes, notamment sur le *NIST Cybersecurity Framework* (*CSF)* [2] et les directives de sécurité informatique mises en œuvre avec succès dans l'administration fédérale[2]. Elle renonce à une analyse complète des risques, telle qu'elle est prévue dans de nombreux modèles-cadres de gestion des cyberrisques[3], et vise à renforcer la cybersécurité et la résilience de la manière la plus simple et la plus pragmatique possible [6 – 8]. À cette fin, elle suit une approche de protection de base élargie, celle-ci étant définie par un ensemble de bonnes pratiques formulées sous forme d'exigences fondamentales (cf. annexe C) qui doivent en principe toujours être mises en œuvre. En fonction du besoin de protection, d'autres mesures techniques et organisationnelles (MTO) doivent également être introduites. Ces besoins de protection résultent d'une évaluation des répercussions des menaces potentielles pour la sécurité informatique sur les activités importantes ainsi que sur les processus d'affaires et de production de l'organisation ou de l'entreprise.

La méthode se distingue par les propriétés et les caractéristiques ci-dessous.

- La MCSR repose sur des normes internationales (en particulier le NIST CSF) et sur une procédure de sécurité informatique dont les prescriptions ont fait leurs preuves au sein de l'administration fédérale suisse.
- Ses objectifs fondamentaux sont la garantie des activités importantes, des processus d'affaires et de production correspondants, la protection des biens de l'organisation ou de l'entreprise, le respect des lois et des autres prescriptions réglementaires, ainsi que la protection contre les pannes, les dysfonctionnements et les défaillances. Si nécessaire, des MTO supplémentaires doivent être mises en œuvre en plus de celles qui répondent aux exigences fondamentales.
- Bien que la méthode renonce à une analyse complète des risques et, plus particulièrement, à leur quantification, elle se base sur les risques et se fonde sur une évaluation qualitative des menaces pour la sécurité informatique et de leurs répercussions.

[1] Pour les termes « cybersécurité » et « résilience », veuillez-vous reporter à l'annexe A et [1].

[2] https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/sicherheitsvorgaben-bund.html

[3] On peut citer en exemples *ISO/CEI 27005* [3], *NIST Risk Management Framework* (*RMF*, https://csrc.nist.gov/Projects/risk-management/) [4] et *NIST SP 800-30* [5] ainsi que les outils correspondants. L'agence de l'Union européenne pour la cybersécurité (ENISA) a élaboré une vue d'ensemble plus complète des modèles-cadres actuellement disponibles et utilisés dans la pratique pour la gestion des cyberrisques. Ce document est disponible à l'adresse https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework.

- Elle part du principe qu'un nombre illimité de composants matériels et logiciels peuvent être regroupés en objets informatiques à protéger[4]. Cette possibilité d'agrégation représente une extension et une précision importantes des modèles-cadres courants pour la gestion des cyberrisques, en particulier en ce qui concerne l'utilisation pratique. Elle favorise par ailleurs une allocation cohérente et compréhensible des ressources pour la mise en œuvre de MTO appropriées.
- La méthode permet un reporting offrant aux organisations et aux entreprises la possibilité de présenter de manière transparente les caractéristiques de sécurité et de résilience par processus d'affaires, par processus de production ou par produit, ce qui crée un sentiment de confiance auprès de la clientèle et de la société.

À moyen terme, la MCSR devrait offrir une alternative à la norme minimale en matière de TIC [9] développée par l'Office fédéral pour l'approvisionnement économique du pays (OFAE) et rendue contraignante par les régulateurs concernés pour certains secteurs de l'économie suisse, notamment pour les exploitants d'infrastructures critiques actifs dans les domaines de l'électricité et du gaz.

Figure 1 Cadre de cybersécurité du NIST (© N. Hanacek/NIST)

Le NIST CSF, représenté schématiquement à la figure 1, est mentionné à plusieurs reprises ci-après, en particulier en lien avec les exigences fondamentales figurant dans l'annexe C. Il s'agit avant tout de faciliter la transition vers la MCSR pour les utilisateurs de la norme minimale en matière de TIC [10].

Le prochain chapitre présente une vue d'ensemble de la méthode, avant d'en approfondir les différentes étapes dans les chapitres ultérieurs [3 – 7]. Le chapitre 8 présente les objectifs de contrôle pour une évaluation et une comparaison des

[4] À ce stade, le terme d'*objet informatique à protéger* n'est pas encore défini. Comme expliqué ultérieurement, un objet informatique à protéger désigne un ensemble de moyens informatiques (tels que des composants matériels et logiciels) poursuivant un objectif commun et défini et qui, de ce fait, constituent un tout cohérent.

performances, et le chapitre 9 décrit les travaux en cours et à venir concernant la MCSR. Enfin, les termes utilisés, les niveaux de sécurité des procédures, des moyens et des services d'authentification, ainsi que les exigences fondamentales sont répertoriés dans les annexes A, B et C.

2 Aperçu

Comme mentionné précédemment, la MCSR repose sur une approche de protection de base élargie. Cela signifie que des exigences fondamentales sont posées dans le cadre d'une protection de base et qu'elles doivent en principe être mises en œuvre pour chaque objet informatique à protéger à l'aide de MTO appropriées (cf. annexe C)[5].

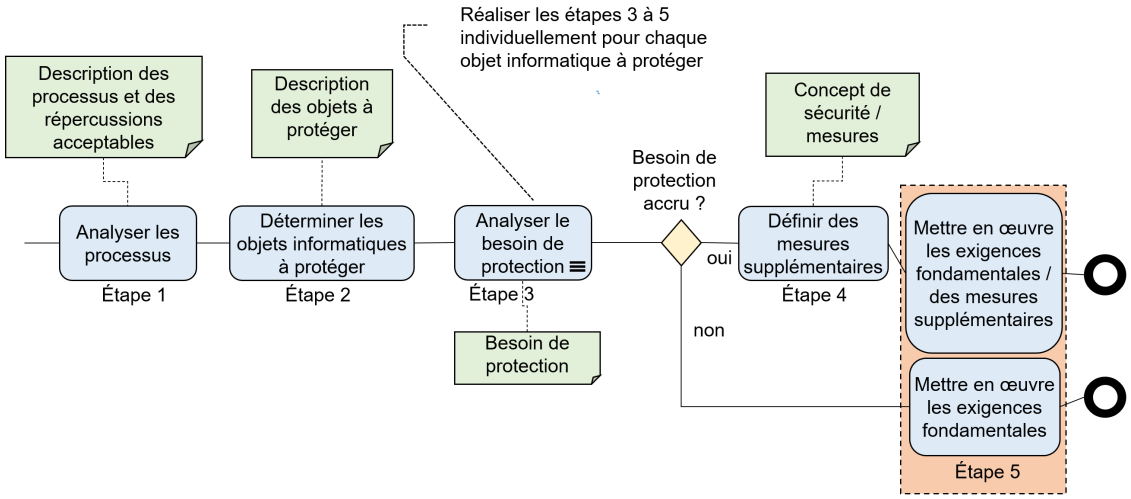

Figure 2 Spécification BPMN de la MCSR

Au-delà de la protection de base, la méthode repose sur une approche en cinq étapes qui se limite toutefois à des considérations architecturales de sécurité pour les objets informatiques à protéger[6]. Ces étapes sont spécifiées à la figure 2 à l'aide du *Business Process Model and Notation* (BPMN). Elles peuvent être résumées et décrites comme suit.

- **Étape 1 (analyse des activités principales) :** pour que la méthode puisse être utilisée de façon judicieuse, l'organisation ou l'entreprise doit avoir une connaissance approfondie de ses activités principales ainsi que des processus d'affaires

[5] La mise en œuvre des exigences fondamentales est en principe contraignante pour tous les objets informatiques à protéger. Des exceptions justifiées et documentées sont possibles en fonction de l'organisation ou de l'entreprise. Toutefois, les procédures et processus d'autorisation de déroger correspondants doivent être transparents et clairement définis.

[6] Les vulnérabilités et les faiblesses d'implémentations et de produits spécifiques doivent être examinées et traitées séparément et indépendamment de la méthode, p. ex. dans le cadre d'une gestion des vulnérabilités. Cette dernière doit être prise en charge au niveau opérationnel et ne relève pas de la MCSR.

et de production qui les rendent possibles, avec leurs objectifs et leurs interdépendances. Cette analyse constitue donc la première étape de la MCSR.

- **Étape 2 (détermination des objets informatiques à protéger) :** l'infrastructure informatique utilisée pour les activités et les processus analysés lors de la première étape doit être répartie en un ensemble d'objets informatiques à protéger. Ces objets seront ensuite analysés et documentés individuellement dans les étapes suivantes de la MCSR. Un objet informatique à protéger peut se composer de différents moyens informatiques, tels que des composants matériels[7] et logiciels ainsi que les données qui y sont stockées, traitées ou transmises. Tous ces éléments poursuivent un objectif commun et défini, ce qui en fait un tout cohérent (p. ex. une application spécialisée pour le traitement d'un processus d'affaires ou de production, ou une plateforme en amont de divers processus). Les étapes 3 à 5 de la MCSR s'appliquent ensuite individuellement à chaque objet informatique à protéger et doivent donc être réalisées séparément pour chacun d'eux.
- **Étape 3 (analyse des besoins de protection) :** pour chaque objet informatique à protéger identifié lors de la deuxième étape, il convient de déterminer s'il affiche un besoin de protection accru en se basant sur les données stockées, traitées et transmises et en tenant compte de l'objectif réel de l'objet en question. Il s'agit en principe d'une décision binaire qui doit être prise indépendamment des exigences fondamentales de la protection de base.
- **Étape 4 (concept de sécurité) :** pour chaque objet informatique à protéger présentant un besoin de protection accru, tel qu'identifié lors de l'analyse des besoins de protection, il faut définir les MTO supplémentaires nécessaires ou pertinentes au-delà des exigences fondamentales de la protection de base, ainsi que les modalités de leur mise en œuvre. Le choix de ces MTO repose sur une analyse approfondie de l'objet informatique à protéger et de ses caractéristiques spécifiques (de préférence sur la base d'une modélisation des menaces). Cette démarche aboutit à un concept de sécurité dans lequel sont documentés à la fois l'objet informatique à protéger, son besoin de protection ainsi que le dispositif de sécurité prévu à cet effet.
- **Étape 5 (mise en œuvre) :** pour chaque objet informatique à protéger, il convient de mettre en œuvre rapidement les MTO nécessaires et de les intégrer dans l'exploitation régulière. Ces dernières servent à satisfaire aux exigences fondamentales de la protection de base ou ont été indiquées comme MTO supplémentaires dans le concept de sécurité informatique.

La structure organisationnelle et administrative de la MCSR ainsi que les compétences et les responsabilités qui en découlent dépendent de l'organisation ou de l'entreprise considérée et ne peuvent donc être définies de manière générale dans le présent document. Il est toutefois certainement judicieux et conseillé que la direction adopte une charte de sécurité recommandant ou imposant l'application de la méthode. Le concept de sécurité élaboré devrait être présenté à la direction concernée sous

[7] Le terme « composants matériels » englobe également les périphériques, c'est-à-dire les appareils externes connectés à un système informatique afin d'étendre ses fonctionnalités, tels que les claviers, les souris, les imprimantes, les écrans et les supports de stockage externes.

une forme appropriée et validé par celle-ci. Cette approche permet en particulier de tenir compte du fait que la responsabilité globale en matière de cybersécurité incombe, dans tous les cas, à la direction.

Les chapitres qui suivent approfondissent et détaillent les cinq étapes de la MCSR, à savoir l'analyse des activités importantes, la détermination des objets informatiques à protéger, l'analyse des besoins de protection, le concept de sécurité et la mise en œuvre.

3 Étape 1 : Analyse des activités principales

L'analyse des activités principales de l'organisation ou de l'entreprise ainsi que des processus d'affaires et de production correspondants constitue le point de départ de la MCSR. Par exemple, la fabrication et la distribution de médicaments sont des activités principales d'une entreprise pharmaceutique, tandis que dans le secteur informatique, ce sont plutôt le développement et la maintenance de logiciels ainsi que le conseil à la clientèle qui prédominent. Dans tous les cas, les activités principales doivent être soutenues par des processus d'affaires et de production appropriés (désignés ci-après sous le terme de *processus*), les processus d'affaires portant sur la fourniture de services et les processus de production sur la fabrication de biens. Ces processus varient d'une organisation et d'une entreprise à l'autre et doivent donc être adaptés et compris au mieux afin que la MCSR puisse être utilisée de façon judicieuse.

3.1 Réalisation

L'analyse des activités importantes (étape 1) se compose essentiellement de deux étapes partielles : il faut d'abord identifier les processus[8] pertinents pour l'exercice des activités importantes de l'organisation ou de l'entreprise (étape partielle 1) et, dans un deuxième temps, les analyser et les documenter sous les angles de la cybersécurité et de la résilience (étape partielle 2).

Étape partielle 1 : identification des processus pertinents

Cette étape vise à identifier les processus pertinents pour l'exercice des activités principales de l'organisation ou de l'entreprise, et donc indispensables à la réalisation des objectifs stratégiques et économiques. Pour ce faire, on peut recourir aux descriptions ou documentations des processus existantes, aux manuels et aux procédures opérationnelles normalisées (*standard operating procedures*, SOP) et mener des entrevues et des ateliers avec le personnel (impliqué dans ces processus). Il est en outre possible d'évaluer et de simuler les procédures et les phases de travail des processus existants[9]. Le nombre de ces processus, qui doit rester raisonnable, varie en fonction de l'organisation ou de l'entreprise. En principe, il va de quelques processus à une douzaine, voire à davantage dans les grandes organisations ou entreprises.

Étape partielle 2 : analyse et documentation des processus

[8] Bien que la formulation soit écrite au pluriel, il se peut que certaines organisations ou entreprises ne disposent que d'un seul processus d'affaires ou de production pertinent.

[9] Dans ce cas, la validité (actualité) des processus existants peut également être vérifiée.

Les processus définis à l'étape partielle 1 doivent être approfondis – c'est-à-dire analysés et documentés – sous les angles de la cybersécurité et de la résilience. L'analyse et la documentation doivent principalement porter sur les objectifs (de processus) et les données (de processus), qui doivent tous deux être systématiquement saisis.

- Les **objectifs de processus** indiquent ce qu'un processus doit concrètement atteindre. Ils comprennent un objectif principal ou primaire et plusieurs objectifs secondaires. L'objectif primaire se trouve au centre du processus examiné et, les objectifs secondaires doivent garantir des conditions-cadres essentiels au processus. Par exemple, un processus d'affaires aura pour objectif principal la fourniture efficace d'un service, tandis que dans un processus de production, il s'agira de fabriquer des biens en quantités requises. Par ailleurs, un objectif secondaire peut concerner la sécurité du processus[10], la protection contre les perturbations et les incidents (sûreté), la protection de la propriété intellectuelle ou le respect des lois, des réglementations, des normes et des bonnes pratiques (dans le cadre de la conformité). Outre les objectifs primaires et secondaires de processus, il convient également de définir les écarts maximaux admissibles en vue de l'analyse des besoins de protection (étape 3). La marge de manœuvre pour les écarts peut être faible, voire nulle (p. ex. dans le contexte de la conformité).
- Les **données de processus** sont des métadonnées relatives à un processus, destinées à le décrire de manière brève mais aussi complète que possible, afin de permettre ou de simplifier les étapes ultérieures de la MCSR. Il s'agit notamment de données se rapportant aux composants de processus suivants :
  - entrées (p. ex. matériaux, fournisseurs, services) ;
  - ressources nécessaires (systèmes informatiques, machines, appareils, etc.) ;
  - étapes de travail et processus concrets ;
  - conditions-cadres (délais, temps de traitement, etc.) et règles à respecter (prescriptions légales et internes, normes, spécifications de qualité, etc.) ;
  - dépendances (p. ex. par rapport à d'autres processus) ;
  - problèmes et dysfonctionnements pouvant survenir et auxquels il faut s'attendre (dommages environnementaux, accidents, divulgation de secrets d'entreprise, etc.)[11] ;
  - dépenses et résultats (p. ex. services ou biens à produire).

  Dans certains cas, les données de processus peuvent déjà être mentionnées comme objectif primaire (p. ex. les biens à produire dans un processus de production) ou secondaire (p. ex. la minimisation des dommages environnementaux). Les données de processus sont toujours pertinentes et doivent être collectées lorsqu'elles sont essentielles à la sécurité du processus.

[10] Les objectifs secondaires liés à la sécurité des processus d'affaires ou de production sont désignés ci-après sous le terme générique d'*objectifs de protection*. Les contributions informatiques aux objectifs de protection sont désignées sous le terme d'*objectifs de protection informatique*.

[11] Il ne s'agit pas de réaliser une analyse des risques, mais d'évaluer si les problèmes et dysfonctionnements mentionnés peuvent en principe survenir au cours du processus, indépendamment des menaces éventuelles.

3.2 Résultats

Les processus issus des activités importantes, analysés plus en détail, doivent être décrits et documentés de manière compréhensible. Pour chaque processus, la documentation comprend une représentation graphique (p. ex. diagramme de flux ou BPMN) ainsi qu'une description structurée (p. ex. tableau) des objectifs de processus (avec les écarts maximaux admissibles) et des données de processus, conformément au ch. 3.1. Il est bien entendu possible d'ajouter des informations supplémentaires non structurées à cette documentation, notamment si elles sont susceptibles de soutenir ou de simplifier les étapes suivantes de la MCSR.

4 Étape 2 : Définition des objets informatiques à protéger

Sur la base des activités importantes analysées lors de la première étape, la deuxième étape consiste à définir les objets informatiques à protéger indispensables aux processus correspondants. La répartition nécessaire de l'infrastructure informatique (constituée de composants matériels et logiciels, de données et d'autres moyens informatiques) en un ensemble d'objets informatiques à protéger représente une tâche architecturale complexe. D'une part, elle doit en effet partir des processus pertinents et d'une architecture d'entreprise explicite ou implicite (approche *top-down*). D'autre part, elle doit tenir compte du fait qu'une agrégation judicieuse des différents composants matériels et logiciels en un objet informatique à protéger peut aussi résulter de leur interaction dans l'accomplissement d'une fonction commune (p. ex. plateformes, services *cloud*, banques de données, etc. ; approche *bottom-up*). Il est difficile de prendre en compte et d'évaluer ces deux approches. De plus, les modèles-cadres courants pour la gestion des cyberrisques n'abordent pas cet aspect. En général, ils mentionnent plutôt le terme d'*assets*, c'est-à-dire de biens à inventorier, sans préciser s'il s'agit de moyens informatiques individuels ou d'objets informatiques agrégés à protéger. La définition des objets informatiques à protéger constitue donc également une extension et une précision importantes de ces modèles-cadres en ce qui concerne l'utilisation pratique. Elle permet surtout de passer d'un nombre excessif de moyens informatiques et d'*assets* à un nombre gérable d'objets informatiques (agrégés) à protéger, ce qui optimise la charge de travail globale.

Il convient de noter qu'il n'y a pas qu'une seule solution correcte pour définir les objets informatiques à protéger, mais plusieurs possibilités avec chacune ses avantages et ses inconvénients. La répartition des moyens informatiques entre les objets informatiques à protéger n'est pas explicite, ce qui signifie que de nombreux moyens informatiques feront simultanément partie de différents objets informatiques à protéger, entraînant ainsi des recoupements entre les objets informatiques à protéger. L'objectif est de réduire au minimum le nombre de ces recoupements, plus exactement le nombre de moyens informatiques faisant simultanément partie de différents objets informatiques à protéger (notamment parce que les recoupements compliquent la cohérence de la procédure de sélection et de mise en œuvre des MTO). Par ailleurs, dans une organisation ou entreprise de petite taille, il est possible que l'ensemble de l'infrastructure informatique soit considéré comme un seul et même objet informatique à protéger.

4.1 Réalisation

Il existe en principe différentes possibilités et approches pour définir les objets informatiques à protéger. Toutefois, une procédure judicieuse comprendra toujours, sous une forme ou une autre, les trois étapes décrites ci-dessous.

Étape partielle 1 : détermination des applications (par processus)

Pour chaque processus, il y a lieu de déterminer les applications nécessaires à la réalisation des objectifs primaires et secondaires correspondants. Il peut s'agir, au niveau des objectifs primaires, d'applications liées à la gestion des fournisseurs ou au commerce électronique, les objectifs secondaires se rapportant plutôt à des applications relevant du domaine du personnel ou des progiciels de gestion intégrés (*enterprise resource planning*, ERP). Cette étape aboutit, dans tous les cas, à l'établissement d'une liste d'applications par processus.

Étape partielle 2 : détermination des moyens informatiques (par application)

Il convient de déterminer les moyens informatiques nécessaires à chacune des applications identifiées à la première étape. Un moyen informatique peut être un composant matériel et/ou logiciel ou des données[12]. La manière dont ces moyens informatiques sont agrégés dépend de l'application concernée. Ainsi, une application ERP recourra à des moyens informatiques davantage simplifiés et agrégés qu'une application dédiée au contrôle des processus. En principe, les personnes chargées de la détermination des moyens informatiques doivent posséder des connaissances techniques approfondies et une grande expertise.

Étape partielle 3 : vérification et simplification des objets informatiques à protéger

Enfin, il faut vérifier que tous les composants matériels et logiciels soient rattachés à au moins une application et que chaque application soit attribuée à au moins un processus. Ces attributions doivent être compréhensibles et faire l'objet d'une évaluation afin d'identifier des possibilités supplémentaires d'agrégation et de simplification, comme le regroupement de plusieurs applications au sein d'une même plateforme. En général, une plateforme offre une série de fonctionnalités transversales pouvant être utilisées simultanément par plusieurs applications. Chaque application ou plateforme ainsi définie constitue un objet informatique (agrégé) à protéger indépendant. Le nombre d'objets informatiques à protéger devrait se limiter à quelques dizaines au maximum.

4.2 Résultats

Les objets informatiques à protéger déterminés à cette étape doivent être agrégés et documentés de façon pertinente. La documentation devrait au moins comporter les informations ci-dessous concernant l'objet informatique à protéger :

(1) nom ou identifiant unique ;

[12] Le composant logiciel peut être l'application elle-même. Il peut être également pertinent de décrire les composants et les modules du logiciel nécessaire à l'application.

(2) brève description (y c., le cas échéant, les schémas architecturaux disponibles et les plateformes utilisées) ;
(3) liste des processus d'affaires et de production auxquels l'objet informatique à protéger sert ;
(4) liste récapitulative du matériel informatique et des logiciels utilisés ;
(5) liste des données d'entrée et de sortie regroupées et agrégées de façon judicieuse, ainsi que les flux de données ;
(6) liste des personnes et des groupes pour lesquels l'objet informatique à protéger est ou peut être pertinent ;
(7) aspects physiques (bâtiments, machines, etc.) pouvant être pertinents pour la cybersécurité ;
(8) informations disponibles concernant les conditions-cadres (p. ex. fournisseurs, exigences géographiques).

Il est bien entendu possible d'ajouter des informations supplémentaires à la documentation relative à l'objet informatique à protéger si elles sont utiles pour la suite des réflexions et des étapes.

5 Étape 3 : Analyse des besoins de protection

La troisième étape consiste à analyser et à définir les besoins de protection pour chacun des objets informatiques à protéger déterminés lors de la deuxième étape. Cette analyse se base sur les objectifs primaires et secondaires des processus, identifiés lors de la première étape, auxquels un objet informatique à protéger sert, ainsi que sur les écarts maximaux admissibles correspondants. Le besoin de protection de l'objet informatique à protéger est considéré comme accru si la violation d'un ou de plusieurs objectifs peut entraîner au moins un écart non admissible. Ce n'est qu'en cas de besoin de protection accru qu'il y a lieu d'analyser en détail les menaces pour la sécurité informatique (quatrième étape) et d'élaborer un concept de sécurité. En l'absence de besoin de protection accru, cette étape n'est pas obligatoire : le respect des exigences fondamentales et la mise en œuvre de MTO correspondantes suffisent.

5.1 Réalisation

Pour être judicieuse, l'analyse des besoins de protection d'un objet informatique à protéger requiert la création d'un répertoire de données. Il possible de s'appuyer sur les données d'entrée et de sortie identifiées à la deuxième étape (au pt 5 du ch. 4.2 concernant la documentation relative à l'objet informatique à protéger). Ce répertoire doit contenir les données principales qui sont soit générées, stockées, traitées et/ou transmises par l'objet informatique à protéger, soit nécessaires à sa mise à disposition. Les données doivent être regroupées de manière logique et accompagnées d'attributs. Un attribut peut par exemple préciser que le groupe de données contient des données à caractère personnel et qu'il est donc soumis à la protection des données.

Il convient d'évaluer les conséquences d'une compromission sur les différents objectifs de protection informatique, au moins pour chaque groupe de données (du répertoire de données) et, si nécessaire, pour d'autres moyens informatiques (tels que les composants matériels ou logiciels). Concrètement, il s'agit de répondre aux questions suivantes : que se passerait-il en cas de violation d'un objectif de protection

informatique spécifique (p. ex. confidentialité, intégrité, disponibilité) et dans quelle mesure cette violation serait-elle compatible avec les objectifs fixés pour le processus sous-jacent, compte tenu des écarts admissibles ? Il est pertinent de compiler les réponses à ces questions sous forme de tableau. Les groupes de données et les autres moyens informatiques sont disposés en lignes, tandis que les attributs et les conséquences d'une violation des objectifs de protection informatique sont indiqués en colonnes. Les entrées du tableau peuvent contenir des textes explicatifs ou des mots-clés. Il convient de mettre en évidence les endroits où les écarts admissibles sont dépassés et où un besoin de protection accru en découle. Une seule entrée dans le tableau suffit pour qu'un objet informatique à protéger bénéficie d'un besoin de protection accru. Si le tableau contient des explications détaillées, celles-ci peuvent contribuer à améliorer le concept de sécurité ultérieur.

À la fin, il convient de vérifier la plausibilité et la cohérence de l'analyse des besoins de protection. Il faut notamment contrôler que les effets possibles identifiés sont réalistes et que les évaluations correspondantes sont compréhensibles et bien fondées. Dans ce but, il peut être nécessaire de faire appel à d'autres instances, telles que le conseiller à la protection des données, lorsque des données à caractère personnel sont utilisées.

5.2 Résultats

En principe, le résultat d'une analyse des besoins de protection se traduit par une décision binaire qui indique si un objet informatique à protéger présente ou non un besoin de protection accru. Comme mentionné précédemment, en cas de résultat positif, un tableau rempli de manière aussi complète que possible constitue également une aide à l'élaboration du futur concept de sécurité. Le choix de MTO appropriées dépendra donc largement des objectifs de protection informatique menacés et de la nature concrète de ces menaces. Dans tous les cas, il est judicieux d'ajouter les conclusions de l'analyse des besoins de protection, sous une forme adéquate, à la documentation relative à l'objet informatique à protéger tel que défini lors de la deuxième étape (définition des objets informatiques à protéger).

6 Étape 4 : Concept de sécurité

Lors de la quatrième étape, un concept de sécurité doit être élaboré pour chaque objet informatique à protéger présentant un besoin de protection accru. Il doit notamment définir les MTO supplémentaires requises ou utiles au-delà des exigences fondamentales de la protection de base et la façon dont ces mesures seront mises en œuvre, sans compromettre l'objectif des processus sous-jacents. Le choix de ces MTO nécessite une analyse approfondie de l'objet informatique à protéger et de ses spécificités.

La première étape consiste en particulier à identifier les objectifs de protection à atteindre pour un processus et, par conséquent, pour un objet informatique à protéger, ainsi que les écarts et les répercussions correspondantes qui sont inadmissibles. L'analyse des besoins de protection effectuée lors de la troisième étape permet par ailleurs de déterminer quelles répercussions sont en principe envisageables. Élaboré lors de la quatrième étape, le concept de sécurité vise à choisir des MTO appropriées

permettant d'éliminer ou de réduire à un niveau acceptable les répercussions envisageables mais non admissibles.

6.1 Réalisation

Le concept de sécurité comporte essentiellement trois étapes : la modélisation des menaces, le choix de MTO appropriées et l'élaboration d'un concept de sécurité. Il existe plusieurs approches méthodologiques possibles pour les deux premières étapes, et celles décrites ci-après ne doivent être considérées que comme des recommandations. Une organisation ou une entreprise qui aurait déjà expérimenté d'autres approches peut bien sûr également les utiliser.

Élément	S	T	R	I	D	E	LM
Acteur	x		x				
Processus	x	x	x	x	x	x	x
Flux de données		x		x	x		
Stockage de données		x		x	x		
Mesures fondamentales	Authentification	Contrôle d'intégrité Renforcement Authentification des messages	Procès-verbal	Cryptage Autorisation Segmentation	Redondance Haute disponibilité	Autorisation Moindre privilège	Protection autonome des composants

Tableau 1 Catégories de menaces pertinentes selon STRIDE-LM (comportant des mesures fondamentales)

Étape partielle 1 : modélisation des menaces

STRIDE(-LM)[13] est une approche de modélisation des menaces qui s'est imposée et a fait ses preuves dans la pratique et qui est donc aussi recommandée dans le cadre

[13] STRIDE est un modèle de risques de sécurité initialement développé par Loren Kohnfelder et Praerit Garg pour la modélisation des menaces chez Microsoft. Il est aujourd'hui utilisé à l'échelle mondiale [11]. Cet acronyme (néologisme) se compose des premières lettres des six catégories initiales de menaces de sécurité distinguées dans le cadre de STRIDE : *Spoofing* (usurpation d'identité), *Tampering* (falsification), *Repudiation* (répudiation), *Information disclosure* (violation de la vie privée ou fuite de données), *Denial of service* (déni de service) et *Elevation of privilege* (élévation des privilèges). Dans le contexte du CSF et pour mieux répondre aux menaces actuelles sur les réseaux, le modèle a été étendu à STRIDE-LM avec l'ajout de la catégorie *Lateral Movement* (mouvement latéral,

de la MCSR. En principe, il s'agit de procéder à un examen systématique visant à déterminer quels éléments architecturaux d'un objet informatique à protéger sont exposés à quelles catégories de menaces et comment ces dernières peuvent être contrées[14]. Comme le montre la partie supérieure (sur fond bleu) du tableau 1[15], les éléments architecturaux peuvent être représentés sur les lignes d'une matrice et les catégories de menaces en colonnes. Les éléments architecturaux fondamentaux (p. ex. les acteurs, les processus, les flux de données et le stockage de données) proviennent de la documentation relative à l'objet informatique à protéger. Ils peuvent être exposés à différentes catégories de menaces du modèle STRIDE-LM. Ainsi, les acteurs peuvent par exemple être concernés par les menaces de type *Spoofing* et *Repudiation*. Les catégories de menaces qui peuvent toucher un élément architectural donné sont marquées d'un « x » dans le tableau 1.

Étape partielle 2 : choix de MTO appropriées

Pour chaque catégorie de menaces à laquelle à un élément architectural donné peut être exposé, il convient de déterminer les mesures fondamentales (figurant en fond orange dans tableau 1) ou les MTO concrètes correspondantes permettant d'y parer. Ce choix ne nécessite ni estimations probabilistes ni calculs de risques, mais uniquement des considérations qualitatives et technologiques sous forme d'heuristiques[16]. Par exemple, si une menace pertinente consiste en une possible interception de certaines données lors de leur transmission, alors l'utilisation systématique de technologies de cryptage est une mesure technique appropriée et judicieuse pour contrer cette menace. Une heuristique similaire s'applique à une connexion à internet : par exemple, si une application spécialisée considérée comme un objet informatique à protéger peut être consultée par le biais d'internet, alors l'utilisation d'un pare-feu constitue dans tous les cas une mesure technique judicieuse.

Il faut donc évaluer, en s'appuyant sur des considérations heuristiques, si le recours à des MTO appropriées découlant des mesures fondamentales du tableau 1 permet de réduire à un niveau acceptable la surface d'attaque de l'objet informatique à protéger et de ses éléments critiques. À cet égard, il convient d'utiliser des MTO préventives

---

qui pourrait toutefois aussi être attribué à la catégorie *Elevation of privilege*). STRIDE-LM est utilisé ci-après.

[14] Dans de nombreux modèles de procédure, les risques sont modélisés au moyen d'une liste de menaces réelles (p. ex. rançongiciels ou attaques par déni de service distribuées). La liste des catégories de menaces postulée dans le cadre de STRIDE simplifie cette modélisation. En effet, les menaces réelles peuvent être rattachées à l'une de ces catégories. Par exemple, les rançongiciels peuvent être classés dans les catégories *Information Disclosure* et *Denial of Service*.

[15] Cette partie du tableau 1, reprise de https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach, a été complétée d'une dernière colonne.

[16] Le terme *heuristique* est dérivé du mot grec *heuriskein*, qui peut être traduit par *trouver* ou *découvrir*. Il s'agit de chercher une solution à un problème qui ne peut être formulé mathématiquement et résolu avec précision à l'aide d'algorithmes appropriés, mais seulement de manière approximative au moyen de valeurs et de règles empiriques, de simplifications ciblées et de raccourcis. Une procédure (de résolution) est donc qualifiée d'heuristique lorsqu'elle permet, au moyen de connaissances restreintes et d'un temps limité, de trouver une solution à un problème qui est au moins suffisamment bonne ou plausible.

et, en particulier, des MTO détectives et réactives de façon à ce qu'elles se complètent mutuellement de manière judicieuse.

Étape partielle 3 : élaboration d'un concept de sécurité

Les MTO ainsi choisies doivent être affinées et spécifiées dans le cadre d'un concept de sécurité. Les situations et les cas d'utilisation permettront probablement de dériver des combinaisons de MTO appropriées pouvant être standardisées sous forme de bonnes pratiques.

6.2 Résultats

À l'issue de cette étape, les MTO choisies doivent être documentées et spécifiées dans le concept de sécurité, en vue de leur mise en œuvre lors de l'étape suivante. Ces spécifications doivent être suffisamment précises pour que les MTO puissent être utilisées et exploitées judicieusement aux échelons tactique et opérationnel.

7 Étape 5 : Mise en œuvre

Au cours de la cinquième et dernière étape de la MCSR, les MTO doivent être mises en œuvre le plus rapidement possible (de l'extérieur vers l'intérieur)[17] pour chaque objet informatique à protéger et transmises de manière compréhensible au service chargé de l'exploitation ou de la sécurité informatique opérationnelle. Elles doivent soit satisfaire aux exigences fondamentales de la protection de base, soit être documentées et spécifiées dans le concept de sécurité. Pour les MTO répondant aux exigences fondamentales de la protection de base, un document séparé doit décrire les modalités de leur concrétisation ou expliquer comment celle-ci est effectuée. La responsabilité de la mise en œuvre doit être clairement indiquée pour chaque MTO : il convient de préciser si la réalisation incombe à l'organisation ou à l'entreprise elle-même, ou à un fournisseur ou à un client. Dans tous les cas, la sécurité informatique opérationnelle doit assurer la protection de ses propres processus d'exploitation visant notamment à gérer les incidents, les vulnérabilités, les fournisseurs, les autorisations et les programmes de sensibilisation et de formation du personnel. Ces processus opérationnels sont d'une grande importance pour la sécurité informatique.

L'exploitation doit toujours être comprise comme un processus circulaire incluant une surveillance et une amélioration permanentes des MTO. Idéalement, elle suit un modèle d'exploitation explicite ou implicite, dont la forme et le contenu ne sont toutefois pas l'objet principal de la MCSR et donc du présent document. Ce modèle, dans sa version la plus simple, peut se composer de prescriptions ou de directives[18] relatives aux processus opérationnels, lesquelles prennent la forme de procédures, de responsabilités et de règles, ou encore d'une liste de tâches à réaliser régulièrement. Les

[17] Selon cette heuristique, les mesures ayant pour but de protéger l'objet informatique à protéger contre les attaques extérieures doivent être mises en œuvre en premier lieu, avant celles visant à assurer une protection interne. Cette heuristique se réfère donc à la hiérarchisation des priorités lors de la mise en œuvre.

[18] Ces directives ne sont pas des stratégies ou des principes directeurs, mais des directives concrètes de mise en œuvre ou d'utilisation (politiques d'utilisation acceptable). Elles ne nécessitent pas d'être redéveloppées par chaque organisation, vu qu'elles ne diffèrent guère pour des processus similaires. Il est possible de développer et de partager des modèles applicables à tout un secteur.

MTO qui s'avèrent inefficaces au niveau de l'exploitation doivent être retirées ou supprimées dans les plus brefs délais.

8 Évaluation et comparaison des performances

La sécurité informatique est une caractéristique qui ne peut être mesurée et vérifiée que de manière limitée [12, 13]. Bien que cela soit similaire pour la cybersécurité et la cyberrésilience [1], cette dernière est en principe mieux adaptée comme fonction objective et base d'évaluation et de comparaison des performances au sens d'un benchmarking. La raison en est que, contrairement à la sécurité informatique, la cyberrésilience se compose en grande partie d'éléments vérifiables (tels que les capacités, les processus, l'organisation et les mécanismes de redémarrage) qui peuvent être convertis en objectifs de contrôle définis et évalués (voir ci-dessous).

L'évaluation et la comparaison de la cyberrésilience d'une organisation ou d'une entreprise avec celle d'organisations et d'entreprises comparables permettent de mettre en évidence les forces et les faiblesses en matière de technologie, d'organisation, de processus et de culture d'entreprise. Elles aident les responsables à hiérarchiser les investissements, à mettre en œuvre des améliorations de manière ciblée et à s'aligner sur les normes reconnues et les exigences réglementaires. Elles renforcent ainsi la fiabilité des services fournis aux clients, aux partenaires et à la société dans son ensemble.

L'évaluation de la cyberrésilience d'une organisation ou d'une entreprise doit s'orienter de manière judicieuse vers les (six) objectifs de contrôle suivants :

1. Les processus commerciaux et de production importants doivent être connus, documentés et compris, ainsi que leurs dépendances vis-à-vis des objets informatiques à protéger.

2. Les compétences et les responsabilités doivent être clarifiées, les ressources nécessaires mises à disposition et ancrées durablement dans le cadre d'une culture de la sécurité.

3. Pour tous les objets informatiques à protéger, la menace doit être analysée et les besoins de protection doivent être clarifiés.

4. Des mesures techniques et organisationnelles appropriées doivent être mises en œuvre pour tous les objets informatiques à protéger et regroupées dans un concept de sécurité cohérent.

5. Il faut s'assurer que les incidents liés à la sécurité puissent être détectés et maîtrisés rapidement. En particulier, les systèmes et applications concernés doivent pouvoir être restaurés rapidement.

6. Toutes les dépendances et tous les risques découlant de la collaboration avec des tiers (par exemple, dans le cadre de chaînes d'approvisionnement ou avec des partenaires) doivent pouvoir être contrôlés afin d'éviter les effets dominos et de garantir la résilience des chaînes de valeur.

Ces objectifs de contrôle constituent le cadre d'une comparaison globale des performances en matière de cyberrésilience. Ils garantissent que les aspects techniques, organisationnels, procéduraux et culturels sont pris en compte de manière égale. Dans cette optique, l'OFCS a élaboré des questionnaires d'évaluation de la cybersécurité et de la résilience, qui sont actuellement développés et testés avec des organisations et des entreprises intéressées, notamment en vue de créer des outils et des ressources d'aide pour la MCSR.

9 Perspective

La MCSR peut être considérée comme un système de gestion de la cybersécurité et de la résilience qui s'inscrit dans une série de systèmes de gestion similaires mais néanmoins différents dans leur orientation, tels que les systèmes de gestion de la protection des données (DSMS), les systèmes de gestion de la continuité des activités (BCMS), les systèmes de gestion de la cybersécurité[19] (CSMS) et surtout les systèmes de gestion de la sécurité de l'information (SMSI). Selon [14], un SMSI peut être défini comme « un système composé de procédures et de règles » qui « peut être mis en œuvre dans une organisation ou une entreprise afin de garantir la sécurité de l'information, c'est-à-dire de définir des objectifs concrets en matière de sécurité de l'information et de planifier, piloter et garantir leur réalisation ».

Le tableau 2 présente les différents systèmes de gestion en fonction de leur couverture des objectifs de contrôle de la cyberrésilience énumérés au chapitre 8 [10]. Toutefois, même dans le cas de la MCSR, la couverture n'est pas complète dans tous les domaines, comme le montre par exemple l'objectif de contrôle numéro 6. Les fonctions classiques du BCM, telles que la planification du redémarrage et la coordination sectorielle en cas de crise, ne sont pas pleinement prises en compte dans la MCSR. Dans ce domaine, les organisations doivent recourir en complément à des méthodes BCM établies.

L'un des atouts particuliers de la MCSR est toutefois qu'elle considère les processus commerciaux et de production comme un point de départ essentiel pour évaluer les besoins de protection. Les risques doivent toujours être évalués dans le contexte de ces processus. Cela permet également de prendre en compte les exigences en matière de protection des données et de sécurité des opérations (au sens de « Safety ») tout au long du processus.

Alors que la MCSR fournit le cadre méthodologique, les systèmes de gestion mentionnés se spécialisent dans des domaines spécifiques : un SMSI, par exemple, est moins ancré dans les processus et vise les systèmes informatiques (par opposition aux systèmes OT industriels). Il est donc moins à même de contrer les effets des perturbations et des pannes. Un DSMS, en revanche, vise – indépendamment des processus commerciaux et de production proprement dits – à protéger les données personnelles, à signaler les violations de la protection des données et à garantir le respect des dispositions contractuelles relatives à la protection des données personnelles. Un BCMS, quant à lui, agit principalement sur les objectifs de contrôle 5 et 6,

[19] Il s'agit en particulier des systèmes de gestion dans le domaine de l'OT qui sont alignés sur les normes pertinentes (par exemple, IEC 62443).

ainsi que sur la connaissance des processus commerciaux et de production proprement dits.

La MCSR offre ici une convergence et permet la mise en place d'un système de gestion qui combine le SMSI, le CSMS, le DSMS et même, en partie, le BCMS. Mais surtout, il peut permettre une mise en œuvre simple et pragmatique d'un SMSI.

Système de gestion	**Objectifs de contrôle de la cyberrésilience**					
	1	**2**	**3**	**4**	**5**	**6**
MCSR Méthode de cybersécurité et de résilience		[20]				[21]
SMSI Système de gestion de la sécurité de l'information			[22]	[23]		
DSMS Système de gestion de la protection des données						
BCMS Système de gestion de la continuité des activités						

entièrement couvert

partiellement couvert

non couvert

Tableau 2 : Couverture de la cyberrésilience (c'est-à-dire des objectifs de contrôle de la cyberrésilience) par les systèmes de gestion courants.

L'OFCS accompagne l'utilisation de la MCSR dans certaines organisations et entreprises choisies, le but étant d'améliorer en permanence la méthode sur la base des expériences réalisées et de la compléter par des recommandations et des aides relatives à sa concrétisation. L'objectif principal reste son applicabilité universelle. Les spécificités propres à chaque secteur et les cas particuliers ne sont pas couverts par défaut par la MCSR et feront l'objet, le cas échéant, d'extensions et de recommandations de mise en œuvre sectorielles.

[20] La méthode, tout comme les autres systèmes de gestion, stipule que, dans l'idéal, l'exploitation doit suivre un modèle d'exploitation explicite ou implicite, dont la forme et le contenu ne constituent toutefois pas l'objet principal de la MCSR.

[21] La gestion des risques fournisseurs est attendue par la MCSR comme une exigence de base de la protection fondamentale, mais n'en fait pas explicitement partie.

[22] L'identification des risques dans un SMSI repose sur les objectifs de protection informatique tels que la confidentialité, la disponibilité et l'intégrité, et non sur les conséquences acceptables concernant les processus commerciaux et de production.

[23] Un SMSI a pour objectif de protéger les informations et non d'empêcher les violations de la protection des données ou de prévenir les perturbations et les pannes. Il ne s'agit donc pas d'une approche holistique.

Abréviations

AAL	*Authentication assurance level* (niveau de confiance de l'authentification)
BCM	Business Continuity Management
BCMS	BCM-System
CCTV	Closed Circuit Television
CEI	Commission électrotechnique internationale
CI/CD	*Continuous integration/continuous delivery* (intégration/livraison continues)
CSF	*Cybersecurity framework* (référentiel de cybersécurité)
CSMS	Système de management de la cybersécurité
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DSMS	Système de management de la protection des données
ENISA	Agence de l'Union européenne pour la cybersécurité
ERP	*Enterprise resource planning* (progiciel de gestion intégré)
FIDO2	*Fast identity online 2* (norme pour l'authentification des utilisateurs)
IEEE	*Institute of Electrical and Electronics Engineers* (Institut des ingénieurs électriciens et électroniciens)
ISO	Organisation internationale de normalisation
JSON	*JavaScript Object Notation* (format de données textuel)
JWT	*JSON Web Token* (standard ouvert pour l'échange sécurisé de jetons)
LM	*Lateral movement* (mouvement latéral)
MCSR	Méthode de cybersécurité et de résilience
MITM	*Man in the middle* (attaque de l'homme du milieu)
MTO	Mesures techniques et organisationnelles
MVSP	*Minimum viable secure product* (produit minimal viable et sécurisé)
NIST	*National Institute of Standards and Technology* (Institut national des normes et de la technologie)
OAuth	*Open Authorization* (protocole de délégation d'autorisation)
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFCS	Office fédéral de la cybersécurité
OIDC	*OpenID Connect* (dispositif d'autorisation)
OTP	*One-time password* (mot de passe à usage unique)
RFC	*Request for comments* (définition de protocoles et de normes)
RMF	*Risk management framework* (cadre de gestion des risques)
SaaS	*Software as a service* (logiciel en tant que service)
SAML	*Security assertion markup language* (protocole pour échanger des informations liées à la sécurité)
SMS	*Short message service* (service de transmission de courts messages)
SMSI	Système de management de la sécurité de l'information
SOC	*Security operations center* (centre des opérations de sécurité)
SOP	*Standard operating procedure* (procédures opérationnelles normalisées)
SP	*Special publication* (publication spéciale)
SSO	*Single sign-on* (authentification unique)
STRIDE	*Spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege* (usurpation d'identité, falsification, répudiation, violation de la vie privée ou fuite de données, déni de service, élévation des privilèges)
TI	Technologies de l'information

TIC	Technologies de l'information et de la communication
TNI	Transformation numérique et gouvernance de l'informatique
TO	Technologies opérationnelles
TPM	*Trusted platform module* (module de plateforme de confiance)
XML	*Extensible markup language* (langage de balisage extensible)

Références

[1] OFCS, Considérations technologiques « Cybersécurité et résilience », novembre 2025

[2] NIST, The NIST Cyber Security Framework (CSF) 2.0, 26 février 2024

[3] ISO/CEI 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks

[4] NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations — A System Life Cycle Approach for Security and Privacy, décembre 2018

[5] NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, septembre 2012

[6] Rolf Oppliger et Andreas Grünert, How to Manage Cyber Risks: Lessons Learnt from Medical Science, IEEE Computer, vol. 56, nº 1, janvier 2023, pages 117 à 119

[7] Rolf Oppliger et Andreas Grünert, How to Measure Cybersecurity and Why Heuristics Matter, IEEE Computer, vol. 57, nº 2, février 2024, pages 111 à 115

[8] Andreas Grünert, James Bret Michael, Rolf Oppliger et Ruedi Rytz, Why Probabilities Cannot Be Used in Cyber Risk Management, IEEE Computer, vol. 57, nº 10, octobre 2024, pages 86 à 89

[9] OFAE, Norme minimale pour améliorer la résilience informatique, 2023

[10] OFCS, la MCSR en comparaison à d'autres systèmes de management, novembre 2025

[11] Loren Kohnfelder et Praerit Garg, « The threats to our products », 1er avril 1999

[12] Andreas Grünert, James Bret Michael, Rolf Oppliger et Ruedi Rytz, On the Measurability and Testability of IT Security, IEEE Computer, vol. 58, nº 3, mars 2025, pages 120 à 126

[13] OFCS, Mesure et vérification de la sécurité informatique : méthodes et limites, 10 juin 2025

[14] OFCS, Analyse de technologie « Gestion de la sécurité de l'information et SMSI », 2 juillet 2025

[15] NIST SP 800-63B, Digital Identity Guidelines – Authentication and Lifecycle Management, juin 2017

[16] OFCS, Considérations technologiques « Clés d'accès », septembre 2025

Annexe A Terminologie

En informatique, on désigne par pyramide du savoir le modèle représenté dans la figure 3. Celui-ci illustre schématiquement comment les données, une fois organisées et traitées, se transforment en informations et en connaissance (direction ascendante), et comment la connaissance peut être décomposée en informations et en données (direction descendante). Parfois, la base du modèle est complétée par un niveau contenant des *caractères*, tandis qu'un niveau supplémentaire, placé au sommet de la pyramide, mentionne la *sagesse* ou la *compréhension*. Ainsi, les données sont composées de caractères, et la sagesse ou la compréhension découle également de la connaissance. En lisant de haut en bas, on peut dire que la connaissance peut être codée sous forme d'informations, et les informations sous forme de données. Les données sont donc une forme d'informations codées spécialement conçue pour les processus de traitement automatisés.

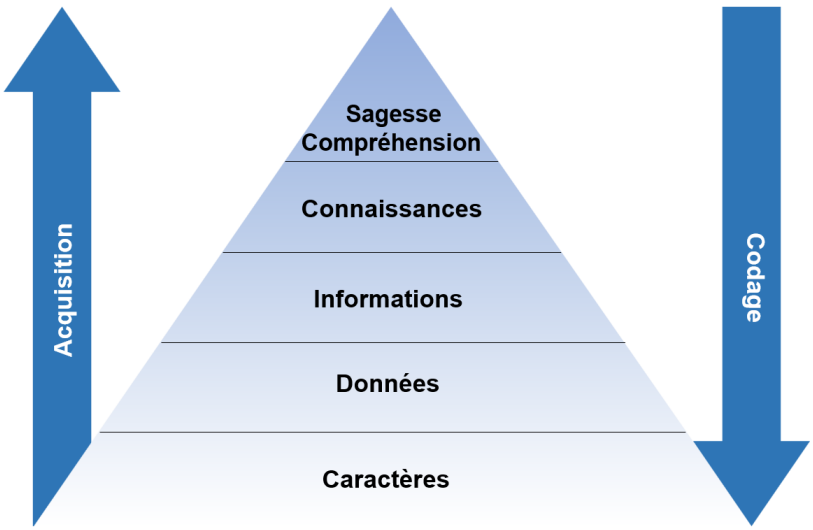

Figure 3 Pyramide du savoir

Bien que les termes *information* et *donnée* soient souvent utilisés comme des synonymes au quotidien, cette assimilation est incorrecte et peut, dans certaines circonstances, provoquer des ambiguïtés, voire des malentendus. En effet, toutes les informations ne sont pas codées sous forme de données. Par exemple, lors d'une conversation personnelle, les mots choisis, les expressions faciales et les gestes transmettent des informations qui ne sont pas codées, ou alors sommairement consignées dans un procès-verbal. On observe également d'autres situations informatives de la vie quotidienne que l'on ne peut ni enregistrer ni coder sous forme de données. Inversement, il existe des données dont aucune information ne peut être tirée. C'est le cas des données générées aléatoirement ou des données cryptées. Dans ce deuxième cas, il est même possible de prouver mathématiquement, sous certaines conditions, qu'aucune information ne peut être extraite de données cryptées sans connaître les clés utilisées[24].

[24] Dans ce contexte, on parle également de *sécurité informationnelle* du cryptage.

En raison de ces différences, il convient de distinguer les termes *information* et *donnée*. Cette distinction s'applique également aux concepts de *sécurité des données* et de *sécurité de l'information*.

- **La sécurité des données** consiste à sécuriser les données qui sont stockées, traitées de manière automatisée et transmises dans le cadre de l'informatique ou dans des systèmes TI et TO. Dans ce contexte, la sécurité peut également se référer à différents objectifs de protection informatique, tels que la confidentialité, l'intégrité et la disponibilité des données.
- La **sécurité de l'information**, quant à elle, consiste à sécuriser les informations, lesquelles peuvent, comme mentionné précédemment, aussi exister hors du domaine informatique sous une forme non conçue pour des processus de traitement automatisés (c'est-à-dire codées sous forme de données). Les conversations personnelles et les scènes de la vie quotidienne ont déjà été citées comme exemples. Un autre exemple est celui des archives papier contenant des notes manuscrites. Ces documents ainsi archivés sont certes codés, mais ce codage n'est pas conçu pour des processus de traitement automatisés (même si, aujourd'hui, un nombre croissant de ces documents sont numérisés et codés sous forme de données en vue d'un traitement automatisé).

Le concept de **sécurité informatique** ou de **sécurité des technologies de l'information** est similaire, mais un peu plus large que celui de sécurité des données. Il ne s'agit par uniquement de garantir la sécurité des données, mais également d'assurer la sécurité d'autres moyens informatiques, comme les composants matériels ou logiciels. Cet aspect joue un rôle significatif notamment dans le domaine des technologies opérationnelles (TO) et dans l'utilisation d'appareils intelligents, aussi appelés internet des objets (IdO)[25]. Il convient de noter que si les TO et l'IdO utilisent des composants, des protocoles et des architectures informatiques « normaux », les conséquences d'une violation des objectifs de protection de la confidentialité, de la disponibilité ou de l'intégrité peuvent non seulement affecter les processus d'affaires et de production (qui peuvent ne pas être maintenus), mais avoir aussi un impact sur le monde réel (physique) : ouverture de soupapes ou de fenêtres, déclenchement d'un processus mécanique, etc. Ces incidents peuvent causer des accidents et des blessures. La MCSR permet de protéger les systèmes TO et TI et de les rendre résilients. Elle favorise ainsi la convergence méthodologique des TI et des TO en matière de cybersécurité[26].

---

[25] Les menaces pesant sur les appareils IdO, qui peuvent être autonomes et exposés, diffèrent de celles affectant les appareils et composants TO. Ces derniers devraient en effet faire partie d'un environnement redondant et équipé de systèmes de sécurité supplémentaires. Cela a aussi une incidence sur la mise en œuvre des exigences fondamentales.

[26] La MCSR est conçue pour être appliquée non seulement à la logique d'affaires, mais aussi aux systèmes de production et d'exploitation ainsi qu'aux systèmes de contrôle des processus, de commande et de surveillance. Elle s'applique également aux actionneurs numériques et aux capteurs utilisés dans les processus de fabrication industriels. À cette fin, la première étape prend en compte les objectifs de protection contre les perturbations et les incidents et la deuxième étape, les composants des systèmes TO en tant que partie intégrante des objets à protéger. La troisième étape évalue si une violation des objectifs de protection informatique peut compromettre les objectifs de processus, y compris la protection contre les perturbations et les incidents. Enfin, le concept de sécurité

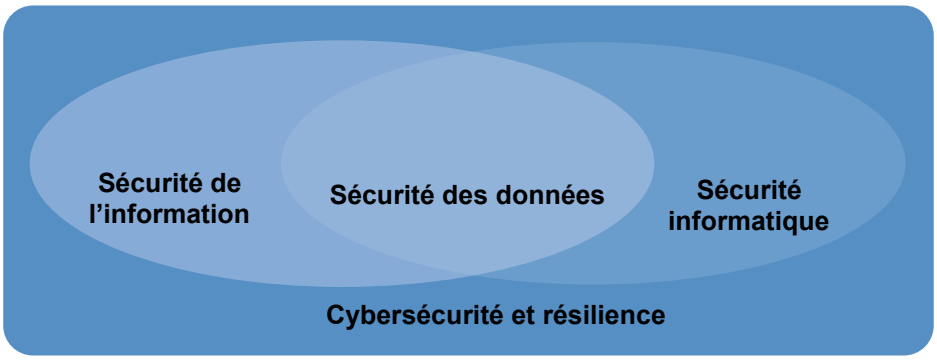

Figure 4 Termes liés à la sécurité

L'interaction entre la sécurité de l'information, la sécurité des données et la sécurité informatique ou des TI est représentée schématiquement à la figure 4. À ces notions de sécurité s'ajoute le nouveau terme de cybersécurité et résilience [1]. Le terme **cybersécurité** n'est toutefois pas défini avec exactitude et ne se distingue pas facilement des autres notions relatives à la sécurité. En fin de compte, la cybersécurité concerne toujours la protection des infrastructures TI et des informations et données qui leur sont directement liées. En revanche, la **cyberrésilience** décrit la capacité d'une organisation ou d'une entreprise à maintenir ses processus commerciaux et de production essentiels malgré les cybermenaces et les incidents informatiques, ou à les reprendre le plus rapidement possible après un incident informatique. Il est non seulement essentiel de prévenir les incidents informatiques (y compris les attaques), mais aussi de savoir quels effets sont inacceptables et d'être capable de rester opérationnel à tout moment, de limiter efficacement les dommages et de revenir rapidement à un fonctionnement normal.

élaboré lors de la quatrième étape et les exigences fondamentales doivent également être mises en œuvre dans les systèmes TO. Une comparaison de cette méthode avec les modèles de la norme CEI 62443 est en cours d'élaboration.

Annexe B Niveaux de sécurité pour les procédures, moyens et services d'authentification

Il existe aujourd'hui sur le marché un grand nombre de procédures, moyens et services pouvant être utilisés pour authentifier de manière directe ou indirecte[27] des personnes ou des processus. Leurs caractéristiques en matière de sécurité peuvent parfois différer considérablement. Sans entrer dans les détails, la présente annexe propose une classification simplifiée qui comporte uniquement trois niveaux de sécurité (*faible*, *moyen* et *élevé*). Elle repose sur les *authentication assurance levels* (*AAL*) 1 à 3 [15] et se limite aux approches basées sur les connaissances[28]. Cette classification se veut aussi simple que possible et ne prévoit actuellement aucune possibilité de reconnaissance ou de contrôle formels.

- **Faible :** les informations sur la base desquelles une authentification directe ou indirecte peut être effectuée sont statiques et identiques pour chaque processus d'authentification (p. ex. un mot de passe ou une clé cryptographique). Lorsque ces informations sont compromises, notamment en cas d'hameçonnage ou par l'enregistrement du trafic des données sur un réseau, elles peuvent également être utilisées à des fins d'usurpation d'identité. Les exemples typiques sont le nom d'utilisateur et le mot de passe, ainsi que les jetons au porteur (p. ex. les cookies) qui ne sont pas sécurisés par cryptographie. Le niveau de sécurité reste faible même si la transmission s'effectue via une connexion cryptée (p. ex. TLS). Pour des raisons de sécurité, ces procédures d'authentification ne devraient plus être utilisées de nos jours, ou seulement dans des cas exceptionnels.
- **Moyen :** les informations sur la base desquelles une authentification directe ou indirecte peut être effectuée sont dynamiques et générées à nouveau à chaque processus d'authentification. En cas de compromission, elles ne peuvent donc pas être facilement utilisées à des fins d'usurpation d'identité. Le nom d'utilisateur et le mot de passe peuvent être utilisés pour l'authentification directe, mais ils doivent être sécurisés par un mécanisme de sécurité supplémentaire, tel qu'une restriction à un appareil[29]. Il est préférable d'utiliser des solutions logicielles OTP (p. ex. *Google Authenticator* ou *Microsoft Authenticator*), des authentifications basées sur des certificats logiciels dans le cadre de TLS et des implémentations de FIDO2 avec des possibilités de synchronisation et d'exportation de clés (p. ex. *Passkeys* [16]). Pour l'authentification indirecte, les certificats doivent être sécurisés par cryptographie (p. ex. cryptés et/ou signés numériquement) et liés au contexte

[27] Une authentification est dite directe lorsqu'elle s'effectue directement entre l'entité qui s'authentifie (p. ex. une personne ou un processus) et une autre entité (d'authentification). Elle est qualifiée d'indirecte si elle est gérée par un tiers (p. ex. un fournisseur d'identité). Dans ce cas, le tiers remet un certificat – appelé dans ce contexte *ticket* ou *jeton* (*token*) – portant sur une ou plusieurs conditions (p. ex. l'identité*).* Ces tickets ou jetons sont idéalement eux-mêmes sécurisés par cryptographie. L'authentification auprès du tiers doit satisfaire aux exigences du niveau de sécurité correspondant.

[28] Par conséquent, cette classification ne tient pas compte d'autres approches d'authentification comme les approches biométriques ou celles basées sur la possession d'un objet ou sur des mécanismes physiques de contrôle d'accès.

[29] En principe, les codes de vérification envoyés par SMS constituent également une telle protection. Cependant, la sécurité des procédures d'authentification par SMS est remise en question, de sorte que ces procédures ne devraient être utilisées que s'il n'y a pas de meilleure solution.

utilisateur (p. ex. la session)[30] d'une manière qui reflète l'état de la technique. On peut citer comme exemples les tickets Kerberos, les jetons SAML et OIDC[31] ainsi que les jetons web JSON (JWT).

- **Élevé :** les informations sur la base desquelles une authentification directe ou indirecte peut être effectuée sont non seulement dynamiques et générées à nouveau pour chaque processus d'authentification, mais dépendent aussi d'une clé cryptographique stockée dans un module matériel dédié et qui ne peut pas, en déployant un effort raisonnable, être déchiffrée à l'aide de ce module. De plus, le module matériel doit être personnel et avoir été délivré lors d'un processus d'enregistrement défini et traçable, puis remis à une personne de manière contrôlable et vérifiable. Les exemples typiques sont les jetons OTP (p. ex. ceux de RSA, de Vasco ou d'un autre fabricant), les solutions OTP fondées sur un TPM, les authentifications sur la base de certificats matériels TLS, les implémentations de FIDO2 sans possibilité de synchronisation et d'exportation de clés, ainsi que les authentifications basées sur un *Swisscom Mobile ID*. Les mêmes exigences que pour le niveau de sécurité moyen s'appliquent à l'authentification indirecte. Il est en outre exigé que l'authentification par rapport aux tickets Kerberos ou aux autres tiers émettant des jetons ait été effectuée sur la base d'une procédure d'authentification de niveau élevé.

Les exemples mentionnés ne sont pas exhaustifs et sont résumés dans le tableau B.1.

Niveau de sécurité	Exemples
Faible	• Nom d'utilisateur et mot de passe • Jetons au porteur (p. ex. cookies)
Moyen	• Nom d'utilisateur et mot de passe avec code de vérification envoyé par SMS • Nom d'utilisateur et mot de passe avec restriction à un appareil* • Solution logicielle OTP (p. ex. *Google Authenticator* ou *Microsoft Authenticator*) • Authentification sur la base d'un certificat logiciel TLS* • Implémentations de FIDO2 avec possibilités de synchronisation et d'exportation de clés (p. ex. *Passkeys**) • Tickets Kerberos • SAML et jetons d'identification et d'accès dans le cadre de l'OIDC et de l'OAuth 2.0

[30] Cette exigence implique entre autres que la durée de validité d'un tel jeton ne doit pas être excessive au regard de son utilisation prévue.

[31] Alors que les jetons SAML reposent sur un format de jeton XML plus ancien, employé depuis environ 2005, dont les conditions, utilisées par les fournisseurs de services, sont appelées *assertions*, les jetons OIDC font référence à un format de jeton plus récent basé sur OAuth 2.0 et JSON. Utilisées par les *relying parties*, les conditions sont appelées *claims*. Les jetons SAML sont généralement employés pour les solutions SSO à l'échelon de l'entreprise, tandis que les jetons OIDC sont plutôt utilisés pour les API spécifiques à l'authentification et à l'autorisation.

	• JWT
Élevé	• Jetons OTP (p. ex. RSA, Vasco) • Solution OTP basée sur un TPM* • Authentification sur la base d'un certificat matériel TLS* • Implémentations de FIDO2 sans possibilité de synchronisation et d'exportation de clés* • *Swisscom Mobile ID* • Tickets Kerberos et autres jetons émis sur la base d'une authentification de niveau élevé

Tableau B.1 Niveaux de sécurité des procédures, moyens et services d'authentification

En principe, le cumul de plusieurs procédures et moyens d'authentification appartenant à même niveau de sécurité ne permet pas d'augmenter ce niveau. Les *Passkeys* restent par exemple à un niveau de sécurité moyen même s'ils sont combinés avec un nom d'utilisateur et un mot de passe avec code de vérification envoyé par SMS.

Des procédures, moyens et/ou services d'authentification plus poussés sont nécessaires pour les applications critiques en matière de sécurité pour lesquelles on peut s'attendre à des tentatives d'intrusion visant à prendre le contrôle de sessions authentifiées (*session hijacking*) ou à s'immiscer dans les communications par une attaque d'hameçonnage en temps réel (*real-time phishing*) ou de type homme du milieu (*man in the middle*, MITM). Une restriction à un appareil (autrement dit une connexion des terminaux à la session), par exemple, permet de se prémunir contre des attaques par détournement de session, tandis qu'une liaison des informations d'authentification à la session protège contre les attaques MITM. Les procédures, moyens et services d'authentification plus poussés sont signalés par un astérisque (*) dans le tableau B.1. Il convient de noter que les procédures, moyens et services doivent en général être configurés de façon à offrir une protection contre les attaques par détournement de session et MITM. En l'absence de précautions particulières, une telle protection n'est souvent pas assurée par défaut.

Annexe C Exigences fondamentales

Les exigences fondamentales compilées et détaillées dans la présente annexe sont structurées selon les fonctions du NIST CSF. Alors que les exigences de la fonction 1 (*govern*) concernent l'organisation ou l'entreprise responsable d'un objet informatique à protéger, toutes les autres fonctions du CSF (*identify*, *protect*, *detect*, *respond* et *recover*) se rapportent aux objets informatiques à protéger proprement dits. Contrairement au CSF, les fonctions *respond* et *recover* sont regroupées ici à des fins de simplification (et alignées sur la fonction *respond* en termes de couleur).

Toutes les exigences s'appliquent également le long des chaînes logistiques. Il revient à la direction de définir les obligations ainsi que les modalités de contrôle correspondantes, la responsabilité globale de la sécurité lui incombant dans tous les cas.

Les exigences fondamentales 1.2 et 2.1 ne s'appliquent pas lors de l'utilisation de la MCSR. Elles sont signalées par un astérisque (*).

Des possibilités de mise en œuvre concrètes sont parfois mentionnées. Elles ne doivent être considérées que comme des recommandations et n'excluent pas d'autres options de concrétisation dont la qualité doit toujours être adaptée aux besoins de protection de l'organisation ou de l'entreprise, ou de l'objet informatique à protéger.

1	**GOVERN (GV)**
1.1	**Organisation de la sécurité** L'organisation de la sécurité doit être définie, communiquée au personnel et mise en œuvre sous cette forme. Il convient en particulier d'identifier clairement les personnes de contact, avec leurs compétences et leurs responsabilités en matière de cybersécurité stratégique et opérationnelle[32]. Ces personnes doivent également disposer des aptitudes techniques nécessaires à l'exercice de leurs responsabilités.
1.2 *	**Gestion des cyberrisques** La gestion des cyberrisques doit être définie et fixée. Il y a lieu de clarifier si les cyberrisques doivent être traités et comment, et de quelle manière la direction est impliquée, que ce soit directement ou indirectement par le biais d'une gestion des risques globale. Des critères d'évaluation et de classification des cyberrisques doivent être établis. Pour les cyberrisques critiques[33], des MTO appropriées[34] doivent être déterminées et mises en œuvre.

[32] La cybersécurité stratégique comprend le pilotage et l'orientation de la cybersécurité. La cybersécurité opérationnelle, quant à elle, englobe la gestion des vulnérabilités, des incidents, des fournisseurs, de la formation, de la sensibilisation et des autorisations.

[33] Un cyberrisque est critique lorsque ses conséquences potentielles sont graves et qu'elles ont un impact significatif sur l'activité.

[34] Les MTO à effet préventif, détectif et réactif servent à mettre en œuvre les fonctions *protect*, *detect* et *respond*. Ces trois fonctions sont importantes et se complètent mutuellement. Des MTO appropriés doivent être définis et mises en œuvre pour chaque risque pertinent, les MTO à effet détectif et réactif étant absolument indispensables.

1.3	**Contrôle du personnel** La fiabilité des collaborateurs[35] doit être contrôlée en fonction de leur niveau hiérarchique et de leurs activités.
1.4	**Formation et sensibilisation** Les collaborateurs doivent être sensibilisés et formés aux questions de cybersécurité en fonction de leur niveau hiérarchique et de leurs activités. Dans la mesure du possible, il faut également aborder, lors des formations, des exemples d'incidents réels ainsi que les conclusions qui en ont été tirées pour l'organisation ou l'entreprise.

2	**IDENTIFY (ID)**
2.1 *	**Objets informatiques à protéger** Tous les composants matériels et logiciels essentiels doivent être documentés avec leurs données d'entrée et de sortie, leurs configurations et leurs flux de données. Ils doivent par ailleurs être analysés en fonction de leurs besoins de protection[36]. Plusieurs composants (périphériques inclus) logiquement apparentés peuvent être regroupés et agrégés en un seul objet informatique à protéger. Les analyses des besoins de protection et les documentations correspondantes doivent inclure toutes les MTO déjà réalisées et celles qui doivent encore être mises en œuvre. Elles doivent être régulièrement mises à jour.
2.2	**Chaînes logistiques** Toutes les dépendances au sein des chaînes logistiques doivent être identifiées, évaluées en fonction de leur importance pour l'activité (c'est-à-dire les processus d'affaires et de production) et surveillées[37]. Il convient en particulier de veiller à ce que les fournisseurs de services (p. ex. SaaS) ou de composants matériels ou logiciels essentiels aux processus d'affaires et de production, ainsi que les fournisseurs disposant d'un accès privilégié ou d'accès à des données sensibles (p. ex. lors de travaux de surveillance et de maintenance nécessaires) soient eux-mêmes protégés au mieux et donc résilients, grâce à la mise en œuvre de MTO appropriées.

[35] À cet égard, les collaborateurs externes doivent être pris en compte au même titre que les collaborateurs internes.

[36] Cette exigence s'applique à tous les composants matériels et logiciels essentiels de l'infrastructure informatique, qu'ils soient exploités sur place ou fournis en tant que service par un prestataire de services cloud. Le besoin de protection dépend de l'importance des composants matériels et logiciels ou des objets informatiques à protéger pour les processus d'affaires et de production qu'ils soutiennent, ainsi que de l'acceptabilité des répercussions en cas de violation des objectifs de protection.

[37] Cela s'applique aussi bien aux technologies de l'information (TI) qu'aux technologies opérationnelles (TO), conformément à l'annexe A.

3	PROTECT (PR)
3.1	**Protection physique, configuration et exploitation** Les objets informatiques agrégés à protéger et les composants matériels et logiciels doivent être configurés et exploités de façon à réduire au maximum leur surface d'attaque[38]. Il convient en particulier (a) d'assurer une protection physique[39] adéquate, (b) de cloisonner logiquement et d'isoler l'objet le mieux possible (p. ex. à l'aide de technologies de virtualisation) et (c) de procéder à un renforcement technique, celui-ci impliquant entre autres • la suppression des comptes prédéfinis[40], • la désactivation des services non nécessaires, • l'exigence d'une confirmation interactive (p. ex. en appuyant sur une touche) pour les modifications des paramètres de sécurité des appareils physiques, (d) de prévenir au mieux les possibilités de perturbations et d'incidents avec des composants interdépendants et indépendants les uns des autres.
3.2	**Gestion des faiblesses et des vulnérabilités** Les objets informatiques agrégés à protéger et les composants matériels et logiciels doivent faire l'objet d'une surveillance, de préférence automatisée[41], dans le cadre de leur cycle de vie et au regard des faiblesses et vulnérabilités connues. Ils doivent par ailleurs être entretenus et maintenus à jour conformément aux bonnes pratiques ou aux instructions des fabricants (p. ex. par l'installation rapide de correctifs ou le remplacement de composants). Pour les appareils en réseau, un mécanisme de mise à jour automatisé du micrologiciel doit être disponible et activé par défaut, pour autant que cela soit techniquement possible.

[38] Cette exigence suit le principe qu'il ne faut pas exposer à internet des objets qui ne doivent pas être accessibles à tout le monde.

[39] D'une part, la protection physique doit protéger contre les dangers météorologiques naturels tels que la grêle, les tempêtes, la pluie, la neige ou la foudre, les dangers naturels gravitationnels tels que les inondations, les coulées de boue, les avalanches ou les chutes de pierres, ainsi que les dangers tectoniques et géologiques tels que les tremblements de terre ou les émissions de radon. D'autre part, la protection physique doit également contrôler et garantir l'accès et la possibilité d'accès physique aux seules personnes autorisées, par exemple à l'aide de caméras de télévision en circuit fermé (CCTV).

[40] Il n'existe donc pas de données d'accès prédéfinies. Si celles-ci sont nécessaires à l'activation, elles doivent être générées une nouvelle fois après la mise en service et fournies à l'utilisateur.

[41] Il est possible d'utiliser des services de surveillance tels que *Shadowserver* (www.shadowserver.org) afin de détecter d'éventuelles vulnérabilités. La surveillance continue des vulnérabilités doit se référer à la *Software Bill of Material* (SBOM), mise à disposition par le fabricant, et suivre les instructions supplémentaires.

3.3	**Gestion des identités et des contrôles d'accès** Les objets informatiques agrégés à protéger et les composants matériels et logiciels doivent être intégrés dans un système complet de contrôle des identités et des accès garantissant que seuls les accès authentifiés et autorisés sont possibles. (a) Un accès est authentifié lorsque l'identité de l'entité accédant au système a été déterminée et vérifiée à l'aide d'une procédure, d'un moyen ou d'un service d'authentification conforme au besoin de protection[42]. (b) Un accès est autorisé lorsque les droits d'accès et les privilèges de l'entité qui accède au système permet aussi l'accès sous cette forme. L'attribution des droits d'accès et des privilèges doit être aussi limitée que possible (principe du moindre privilège).
3.4	**Sécurité du réseau** Les objets informatiques agrégés à protéger et les composants matériels et logiciels doivent être protégés adéquatement contre les attaques réseau[43]. Cette protection peut en principe être obtenue de deux manières. • Le composant ou l'objet informatique à protéger est exploité dans un réseau (segment) séparé[44] disposant d'une protection périmétrique appropriée qui elle-même comporte une restriction des services, des protocoles et des ports réseau (au sens d'un pare-feu). • Le composant ou l'objet informatique à protéger dispose lui-même de mécanismes et de mesures de sécurité adéquates (au sens de *confiance zéro* ou *minimale*)[45].

[42] L'accès peut s'effectuer de manière interactive par un utilisateur ou de façon non interactive par un service ou un processus. Il est également possible d'accéder au système via une procédure de réinitialisation des clés d'authentification. Dans tous les cas, les exigences en matière d'authentification sont les mêmes. Une classification possible en trois niveaux de sécurité est proposée à l'annexe B pour les approches d'authentification basées sur la connaissance, c'est-à-dire reposant sur un élément que l'utilisateur connaît ou possède (p. ex. un mot de passe ou une clé cryptographique). Dans tous les cas, l'authentification doit être conçue de façon à ne pas pouvoir être simplement réinitialisée et donc contournée. À défaut des approches d'authentification basées sur les connaissances, l'exigence peut aussi être mise en œuvre à l'aide d'autres approches d'authentification ou de mesures physiques.

[43] Cette exigence vise principalement à empêcher les attaques visant à passer le hachage (*pass-the-hash*) et ce qu'on nomme les mouvements latéraux (*lateral movements*). Ces derniers font également l'objet de l'extension de *STRIDE* à *STRIDE-LM*.

[44] Dans le cadre de la segmentation du réseau, il convient de s'assurer que, au minimum, les systèmes TI et TO sont séparés les uns des autres (en d'autres termes qu'ils fonctionnent dans des segments différents).

[45] Le terme habituellement utilisé est *confiance zéro*. Toutefois, on lui préfère dans ce contexte la notion de *confiance minimale*, étant donné qu'il faut toujours émettre des hypothèses sur les relations de confiance et que celles-ci doivent être réduites au minimum.

3.5	**Protection contre les logiciels malveillants** Les objets informatiques agrégés à protéger et les composants matériels et logiciels doivent bénéficier d'une protection efficace[46] contre les programmes malveillants (*malware*) et les attaques basées sur les données[47], au moyen de mesures appropriées.
3.6	**Cryptage et suppression des données** Pendant leur stockage, leur traitement et leur transfert, les données doivent être adéquatement protégées en ce qui concerne leur confidentialité et leur intégrité (p. ex. au moyen de procédés cryptographiques adéquats). Les données qui ne sont plus nécessaires doivent être supprimées conformément à leur niveau de protection et aux prescriptions réglementaires[48]. Cette exigence s'applique aussi bien à l'exploitation qu'au développement de systèmes et d'applications.
3.7	**Sauvegarde des données** Toutes les données liées aux processus d'affaires et de production importants doivent être sauvegardées régulièrement. Idéalement, il y a lieu de mettre en œuvre un concept de sauvegarde prévoyant un stockage des données multigénérationnel en ligne et hors ligne sur plusieurs sites. Par ailleurs, les données doivent pouvoir être restaurées à tout moment, dans les meilleurs délais et dans leur intégralité. Leur restauration doit faire l'objet d'exercices périodiques.
3.8	**Développement** La cybersécurité doit être prise en compte dès le début lors du développement de composants matériels et logiciels. Cela comprend notamment la modélisation des menaces lors de la planification architecturale, le respect des directives[49] et des bonnes pratiques lors de la mise en œuvre (ou la

[46] Cette exigence ne doit pas nécessairement être satisfaite à l'aide d'un logiciel supplémentaire. Dans de nombreux cas, il suffit d'utiliser les fonctionnalités des systèmes d'exploitation en place et de les configurer en conséquence. La protection peut également être assurée en vérifiant les données et/ou en bloquant des données inutiles lors de leur transmission (en d'autres termes avant qu'elles n'atteignent les systèmes finaux).

[47] Lors d'une attaque basée sur les données, des données sont introduites dans un système TI ou une application, ce qui provoque un dysfonctionnement.

[48] Dès qu'un certain niveau de protection est requis, une suppression logique au niveau du système d'exploitation n'est pas suffisante. Les données à supprimer doivent être écrasées plusieurs fois avec des données aléatoires.

[49] Pour le développement de logiciels, la directive du *minimum viable secure product* (produit minimal viable et sécurisé, MVSP ; https://mvsp.dev) est tout indiquée. Les principes de *security by design* (sécurité dès la conception) et de *security by default* (sécurité par défaut) doivent être pris en compte dans le développement. Le principe de *security by default* signifie que les moyens informatiques sont développés, configurés et exploités de manière à activer par défaut toutes les mesures de sécurité pertinentes dans un environnement spécifique afin qu'elles puissent déployer leurs effets sans que les utilisateurs doivent s'en soucier. Le principe de *security by design* exige que la sécurité soit prise en compte dès le début du développement comme partie intégrante du processus.

	prévention des pratiques non sécurisées), l'utilisation d'une plateforme CI/CD incluant des contrôles de sécurité continus, la conception d'interfaces (en particulier les interfaces utilisateur graphiques) qui ne prêtent pas à confusion ainsi que l'utilisation sécurisée, par les développeurs, d'environnements de développement intégrés et de *plugins* correspondants. Les environnements de développement et de production doivent toujours être séparés.
3.9	**Disponibilité** Les objets informatiques agrégés à protéger et les composants matériels et logiciels doivent être sécurisés en ce qui concerne leur disponibilité. Ils doivent disposer en particulier de capacités suffisantes en termes de calcul, de stockage et de transmission, et les composants importants doivent être redondants lorsque cela est judicieux.

4	**DETECT (DE)**
4.1	**Enregistrement et surveillance** Pour chacun des objets informatiques agrégés à protéger (en particulier les réseaux) et des composants matériels et logiciels, les activités, incidents et événements liés à la sécurité doivent être enregistrés[50] et évalués de manière automatisée et aussi rapide que possible (p. ex. dans le cadre d'un SOC) afin de détecter d'éventuelles attaques.
4.2	**Annonce** Pour chacun des objets informatiques agrégés à protéger et des composants matériels et logiciels, il doit être clairement indiqué comment les personnes externes peuvent signaler des vulnérabilités et des incidents liés à la sécurité[51].

5	**RESPOND (RS) et RECOVER (RC)**
5.1	**Gestion des incidents** Les incidents et les dysfonctionnements détectés qui sont susceptibles d'affecter les processus d'affaires et de production pertinents doivent être triés et résolus dans les meilleurs délais.

[50] Les enregistrements doivent être conservés sous une forme adéquate pendant une durée raisonnable, dans un format non modifiable. Ils doivent pouvoir être remis à disposition afin de garantir la traçabilité des activités liées à la sécurité. Des *canaries* devraient également être utilisés pour détecter une éventuelle compromission.

[51] Cela peut être effectué par l'intermédiaire d'un fichier *security.txt* disponible sur le web, conformément à la norme RFC 9116.

5.2	**Planification d'urgence** La restauration de la capacité opérationnelle doit être garantie pour chacun des objets informatiques agrégés à protéger et des composants matériels et logiciels[52]. À cette fin, des plans d'urgence et de restauration[53] doivent être définis, hiérarchisés, régulièrement exercés et, le cas échéant, améliorés. Ces plans doivent être intégrés dans un plan d'urgence global pour l'ensemble de l'organisation ou de l'entreprise.
5.3	**Communication** Les responsabilités et les objectifs de la communication doivent être connus pour tous les plans d'urgence à établir, conformément à l'exigence 5.2.

[52] Il convient également de tenir compte des dépendances dans les chaînes logistiques TI/TO, conformément à l'exigence fondamental 2.2, et de la réutilisation des données sécurisées, conformément à l'exigence fondamentale 3.7.

[53] Les conclusions et les enseignements tirés d'incidents de sécurité antérieurs et d'éventuelles simulations doivent être pris en compte dans ces plans.