Solange Ghernaouti

Sécurité informatique et réseaux

Cours avec plus de 100 exercices corrigés

4e édition

DUNOD

Illustration de couverture :
WavebreakmediaMicro-Fotolia.com

ISBN 978-2-10-059912-7

TABLE DES MATIÈRES

AVANT-PROPOS

Ce livre offre une synthèse des problématiques et des éléments de solution liés à la sécurité informatique, qui inclut la sécurité des systèmes d'information, des réseaux de télécommunication, la sécurité de l'information et la cybersécurité. Par une approche transversale, intégrative et pragmatique, il traite à la fois des aspects de gestion des risques informatiques, de gouvernance, de conformité réglementaire, de gestion stratégique et opérationnelle de la sécurité. Il présente les technologies qui permettent de réaliser des services et des fonctions de sécurité dans une approche d'ingénierie de la sécurité et d'intelligence juridique.

En traitant des différentes expressions de la criminalité informatique, il donne les clés nécessaires à la compréhension des menaces d'origine criminelle et des principales questions soulevées par la lutte contre la cybercriminalité.

- Le **chapitre 1** introduit les **principes fondamentaux** et les domaines d'application de la sécurité informatique qui doivent être appréhendés de manière systémique. Il constitue la base nécessaire à la compréhension globale des différents aspects et dimensions de la sécurité.
- Le **chapitre 2** définit la notion de **crime informatique** et de **cybercrime,** il met en avant les vulnérabilités inhérentes au monde numérique et aux environnements Internet ainsi que leur exploitation à des fins malveillantes. Il identifie les différentes pistes de prévention et de lutte contre la cybercriminalité.
- Le **chapitre 3** traite des aspects de **maîtrise des risques** informatiques, de **gestion stratégique** et de **gouvernance** de la sécurité informatique et des télécommunications. Les **dimensions politiques, juridique et socio-économique** dans lesquelles s'inscrit la sécurité informatique sont identifiées pour insister sur la nécessité de doter les individus, les organisations et les États, de moyens suffisants et nécessaires à leur protection et à la confiance dans un monde en réseau. Les métiers de la sécurité informatique, les acteurs, les compétences comme les notions d'organisation, de responsabilité et de mission de sécurité sont présentés.
- Le **chapitre 4** aborde les **outils méthodologiques**, les **normes**, les **méthodes**, les bonnes pratiques, les démarches à disposition pour analyser les besoins de sécurité, **définir une politique de sécurité**, mettre en place des mesures, **auditer**, **mesurer**, évaluer, **certifier** la sécurité. Ce chapitre traite également de la **gestion de crise**, des **plans de secours et de continuité** des activités.
- Le **chapitre 5** est consacré aux principes fondamentaux et invariants concernant les **mécanismes cryptographiques** (de **chiffrement)** mis en œuvre dans des

environnements distribués pour offrir des services de confidentialité, d'authentification, d'intégrité et de non-répudiation. Une introduction à la cryptographie quantique ainsi que les avantages, inconvénients et limites des systèmes de chiffrement sont proposés. Les concepts et les mécanismes de signature numérique, de certificats numériques, d'infrastructures de gestions de clés (PKI), de tiers de confiance, d'autorité de certification sont analysés.

- Le **chapitre 6** traite des problématiques de **sécurité des infrastructures de télécommunication** réalisant Internet. Il présente notamment la nouvelle version sécurisée du protocole Internet (IPv6, IPSec), les principes de sécurité liés au routage, au contrôle d'accès, à des réseaux privés virtuels (**VPN**), à l'externalisation et au ***cloud computing***.
- Le **chapitre 7** est dédié à la manière dont les **réseaux sans fil** sont sécurisés. Les technologies de la sécurité des réseaux cellulaires **GSM**, **GPRS**, **UMTS** sont étudiées comme celles des **réseaux locaux sans fil 802.11** et des **réseaux personnels**.
- Après avoir présenté dans les chapitres précédents, les protocoles cryptographiques implantés dans des infrastructures réseaux filaires et sans fil, le **chapitre 8** analyse la manière dont les **systèmes pare-feu** et de **détection d'intrusion** contribuent à renforcer la sécurité des environnements informatiques.
- Le **chapitre 9** est dédié à la protection des contenus et des principaux services applicatifs de l'Internet, notamment de la sécurité de la messagerie électronique, de la téléphonie sur Internet, de la navigation web, du commerce électronique, des paiements en ligne, des documents XML. Sont également abordées les notions de protection des données par le tatouage électronique la gestion des droits numériques (DRM) et les problématiques de sécurité liées à l'usage de l'informatique personnelle et des réseaux sociaux en entreprise.
- Le **chapitre 10** traite de la **gestion de réseau** comme outil de cohérence et d'**intégration des mesures** de sécurité et des savoir-faire managérial et technologique.

Chaque chapitre comprend, entre autres, une présentation de ses objectifs, un résumé et des exercices. Un certain relief est introduit dans le texte par des **termes** mis en gras pour souligner leur importance, par la traduction anglaise du vocabulaire de la sécurité (*security vocabulary*) et par des encarts. De nombreuses références, un glossaire des principaux termes, un lexique de sigles ou encore la correction des exercices contribuent à une meilleure assimilation des thèmes abordés.

Une bibliographie succincte ainsi que quelques références en ligne et un index concluent cet ouvrage.

Les chapitres peuvent se lire de manière séquentielle ou indépendamment les uns des autres. Le lecteur pourra s'intéresser uniquement :

- à une introduction générale et à une **approche transversale de la sécurité** (chapitre 1) ;
- à la **criminalité** informatique et la cybercriminalité (chapitre 2) ;
- à la **gouvernance**, à la politique de sécurité, aux normes et méthodologies de **gestion stratégique et opérationnelle** de la sécurité (chapitres 3 et 4) ;
- aux **techniques**, **mécanismes** et **solutions** de sécurité :

- ◇ techniques de chiffrement (chapitre 5),
- ◇ techniques mises en œuvre pour la sécurité des infrastructures de télécommunication (chapitre 6),
- ◇ techniques mises en œuvre pour la sécurité des réseaux sans fil (chapitre 7),
- ◇ techniques de sécurité par des systèmes pare-feu et de détection d'intrusion (chapitre 8),
- ◇ techniques mises en œuvre pour la sécurité des applications, des services et des contenus (chapitre 9),
- ◇ techniques mises en œuvre pour assurer la sécurité au travers de la gestion opérationnelle des réseaux (chapitre 10).

Cette édition revue et augmentée propose **plus d'une centaine d'exercices corrigés** ainsi que des compléments en ligne dont un support de cours **téléchargeable** sur la page associée à l'ouvrage sur le site des éditions Dunod, *www.dunod.com*.

Ce livre est le fruit de mes activités de recherche et d'enseignement. Il est également le descendant de mes premiers ouvrages entièrement consacrés à la sécurité à savoir : *Stratégie et ingénierie de la sécurité des réseaux* (InterÉditions, 1998) et *Sécurité Internet, stratégies et technologies* (Dunod, 2000).

Je le dédie à mes étudiants d'hier, d'aujourd'hui et de demain, mais aussi à tous les autres, qui lui donnent sa raison d'être.

Solange GHERNAOUTI
www.scarg.org

PRINCIPES DE SÉCURITÉ 1

PLAN

OBJECTIFS

- ➤ Identifier les critères et les principales caractéristiques et fonctions de la sécurité informatique.
- ➤ Comprendre les champs d'application, les différents aspects et la dimension interdisciplinaire de la sécurité informatique et de la cybersécurité.
- ➤ Aborder la notion d'architecture de sécurité.

1.1 OBJECTIFS DE SÉCURITÉ ET FONCTIONS ASSOCIÉES

La notion de sécurité fait référence à la propriété d'un système, d'un service ou d'une entité. Elle s'exprime le plus souvent par les objectifs de sécurité suivants :

- la disponibilité (D) ;
- l'intégrité (I) ;
- la confidentialité (C).

Ces objectifs peuvent être compris comme étant des critères de base (dits *critères DIC*) auxquels s'ajoutent des fonctions de sécurité qui contribuent à confirmer d'une part la véracité, l'authenticité d'une action, entité ou ressource (notion d'**authentification**) et, d'autre part, l'existence d'une action (notion de **non-répudiation** d'une transaction, voire d'**imputabilité** (figure 1.1).

La réalisation de fonctions de sécurité, telles que celles de gestion des identités, du contrôle d'accès, de détection d'intrusion par exemple, contribuent, via des mécanismes de sécurité comme le chiffrement par exemple, à satisfaire les exigences de sécurité exprimées en termes de disponibilité, d'intégrité, de confidentialité. Elles concourent à la protection des contenus et des infrastructures numériques et sont supportées par des solutions techniques. Celles-ci sont à intégrer dans le système à sécuriser, en fonction du cycle de vie de ce dernier, par des approches complémentaires d'ingénierie et de gestion de la sécurité informatique.

1.1.1 Disponibilité

La **disponibilité** d'une ressource est relative à la période de temps pendant laquelle le service offert est opérationnel. Le volume potentiel de travail susceptible d'être pris en charge durant la période de disponibilité d'un service, détermine la **capacité** d'une ressource à être utilisée (serveur ou réseau par exemple).

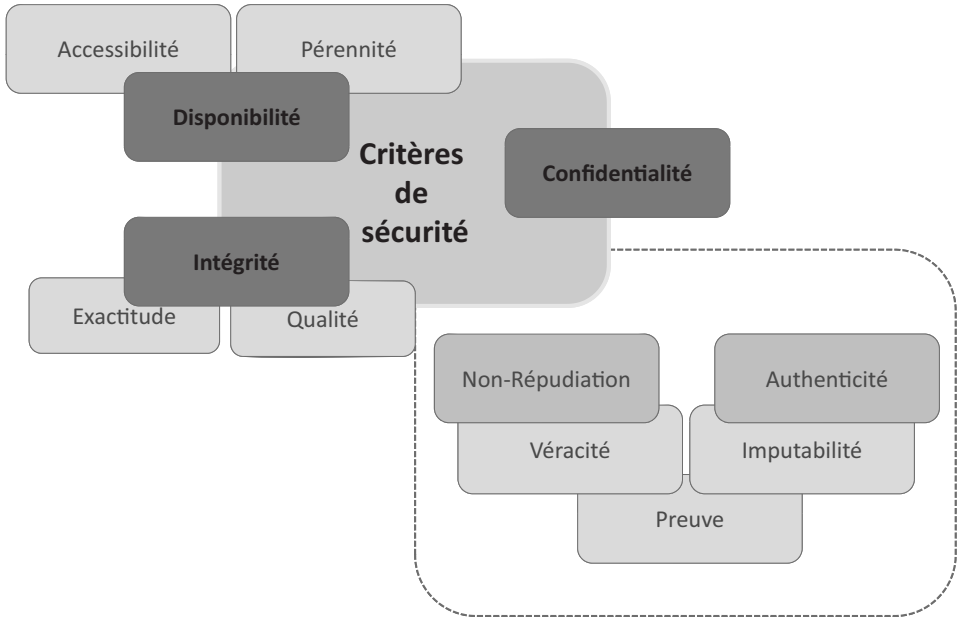

Figure 1.1 – Critères de sécurité.

Il ne suffit pas qu'une ressource soit disponible, elle doit pouvoir être utilisable avec des temps de réponse acceptables. Sa disponibilité est indissociable de sa capacité à être **accessible** par l'ensemble des ayants droit **(notion d'accessibilité)**.

La disponibilité des services, systèmes et données est obtenue par un **dimensionnement approprié** et une certaine redondance des infrastructures ainsi que par une **gestion opérationnelle** et une **maintenance efficaces** des infrastructures, ressources et services.

Un service nominal doit être assuré avec le minimum d'interruption, il doit respecter les clauses de l'engagement de service établies sur des indicateurs dédiés à la mesure de la **continuité de service**[1].

Des pertes de données, donc une indisponibilité de celles-ci, peuvent être possibles si les procédures d'enregistrement et les supports de mémorisation ne sont pas gérés correctement. Ceci constitue un **risque majeur** pour les utilisateurs. Leur

1. La gestion de la continuité des services est traitée au chapitre 4.

sensibilisation à cet aspect de la sécurité est importante mais ne peut constituer un palliatif à une indispensable mise en place de procédures centralisées de sauvegarde effectuées par les services compétents en charge des systèmes d'information de l'entreprise.

De nombreux outils permettent de sauvegarder périodiquement et de façon automatisée les données, cependant, une définition correcte des procédures de restitution des données devra être établie afin que les utilisateurs sachent ce qu'ils ont à faire s'ils rencontrent un problème de perte de données.

Une **politique de sauvegarde** ainsi qu'un arbitrage entre le coût de la sauvegarde et celui du risque d'indisponibilité supportable par l'organisation doivent être préalablement établis pour que la mise en œuvre des mesures techniques soit efficace et pertinente.

1.1.2 Intégrité

Le critère d'**intégrité** des ressources physiques et logiques (équipements, données, traitements, transactions, services) est relatif au fait qu'elles n'ont pas été détruites (altération totale) ou modifiées (altération partielle) à l'insu de leurs propriétaires tant de manière intentionnelle qu'accidentelle. Une fonction de sécurité appliquée à une ressource pour contribuer à préserver son intégrité, permettra de la protéger plus ou moins efficacement contre une menace de corruption ou de destruction.

En effet, il convient de se prémunir contre l'altération des données en ayant la certitude qu'elles n'ont pas été modifiées lors de leur stockage, de leur traitement ou de leur transfert. Les critères de disponibilité et d'intégrité sont à satisfaire par des mesures appropriées afin de pouvoir atteindre un certain niveau de confiance dans les contenus et le fonctionnement des infrastructures informatiques et télécoms.

Si en télécommunication, l'intégrité des données relève essentiellement de problématiques liées au transfert de données, elle dépend également des aspects purement informatiques de traitement de l'information (logiciels d'application, systèmes d'exploitation, environnements d'exécution, procédures de sauvegarde, de reprise et de restauration des données).

En principe, lors de leur transfert, les données ne sont pas altérées par les protocoles de communication qui les véhiculent en les encapsulant.

Des contrôles d'intégrité[1] peuvent être effectués pour s'assurer que les données n'ont pas été modifiées lors de leur transfert par des attaques informatiques qui les interceptent et les transforment (notion d'**écoutes actives**). En revanche ils seront de peu d'utilité pour détecter des écoutes passives qui portent atteintes non à l'intégrité des données mais à leur confidentialité.

1. Voir chapitre 5.

1.1.3 Confidentialité

« La confidentialité est le maintien du secret des informations… » (*Le Petit Robert*). Transposée dans le contexte de l'informatique et des réseaux, la notion de **confidentialité** peut être vue comme la « *protection des données contre une divulgation non autorisée* ».

Il existe deux types d'actions complémentaires permettant d'assurer la confidentialité des données :

- limiter et contrôler leur accès afin que seules les personnes habilitées à les lire ou à les modifier puissent le faire ;
- les rendre inintelligibles en les chiffrant de telle sorte que les personnes qui ne sont pas autorisées à les déchiffrer ne puissent les utiliser.

Le **chiffrement des données** (ou **cryptographie**)[1] contribue à assurer la confidentialité des données et à augmenter la sécurité des données lors de leur transmission ou de leur stockage. Bien qu'utilisées essentiellement lors de transactions financières et commerciales, les techniques de chiffrement sont relativement peu mises en œuvre par les internautes de manière courante.

1.1.4 Identification et authentification

Identifier l'auteur présumé d'un tableau signé est une chose, s'assurer que le tableau est authentique en est une autre. Il en est de même en informatique où des procédures d'**identification** et d'**authentification** peuvent être mises en œuvre pour contribuer à réaliser des procédures de contrôle d'accès et des mesures de sécurité assurant :

- la **confidentialité** et l'**intégrité des données** : seuls les ayants droit identifiés et authentifiés peuvent accéder aux ressources (contrôle d'accès[2]) et les modifier s'ils sont habilités à le faire ;
- la **non-répudiation** et l'**imputabilité** : seules les entités identifiées et authentifiées ont pu réaliser une certaine action (preuve de l'origine d'un message ou d'une transaction, preuve de la destination d'un message…). L'identification et l'authentification des ressources et des utilisateurs permettent d'imputer la responsabilité de la réalisation d'une action à une entité. Celle-ci pourra être tenue responsable de certains faits et éventuellement rendre des comptes, s'ils ont été enregistrés, sauvegardés et analysés. Ainsi la **traçabilité** des événements est une fonction indispensable qui permet de garder la mémoire des actions survenues à des fins d'analyse pour reconstituer et comprendre ce qui s'est passé. Cela permet par exemple d'analyser le comportement du système et des utilisateurs à des fins d'optimisation, de gestion des incidents, de recherche de preuves, d'imputation de responsabilité ou encore d'audit par exemple.

1. Le chiffrement des données est traité au chapitre 5.
2. Le contrôle d'accès est traité au chapitre 6.

L'authentification doit permettre de vérifier l'identité d'une entité afin de s'assurer entre autres, de l'authenticité de celle-ci. Pour cela, l'entité devra prouver son identité, le plus souvent en donnant une information spécifique qu'elle est censée être seule à détenir telle que, par exemple, un mot de passe ou une empreinte biométrique.

Tous les mécanismes de contrôle d'accès logique aux ressources informatiques nécessitent de gérer l'identification, l'authentification des entités et la gestion des droits et permissions associées aux personnes (figure 1.2). Cela exclut l'usage anonyme des ressources. C'est également sur la base de l'identification des personnes et des accès aux ressources que s'établissent des fonctions de facturation et de surveillance.

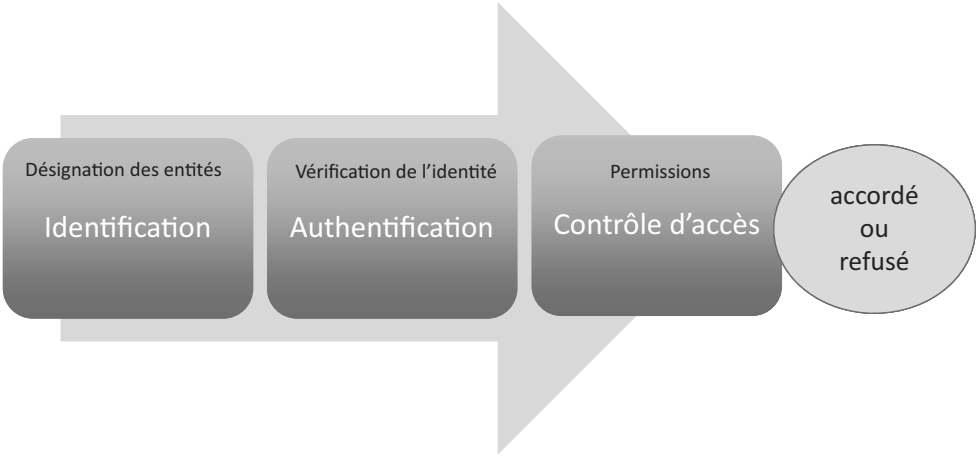

Figure 1.2 – Identification et authentification.

1.1.5 Non-répudiation

La **non-répudiation** est le fait de ne pouvoir nier ou rejeter qu'un événement (action, transaction) a eu lieu. À ce critère de sécurité peuvent être associées les notions d'imputabilité, de traçabilité ou encore parfois d'auditabilité**.**

L'**imputabilité** se définit par l'attribution d'une action (un événement) à une entité déterminée (ressource, personne). Elle peut être réalisée par un ensemble de mesures garantissant l'enregistrement fiable d'informations pertinentes par rapport à une entité et à un événement.

L'établissement de la **responsabilité** d'une personne vis-à-vis d'un acte dans le monde de l'informatique et des télécoms nécessite l'existence de mesures d'authentification des individus et d'imputabilité de leurs actions.

La **traçabilité** permet de suivre la trace numérique laissée par la réalisation d'un événement (message électronique, transaction commerciale, transfert de données…). Cette fonction comprend l'enregistrement des événements, de la date de

leur réalisation et leur imputation. Elle permet, par exemple, de retrouver l'adresse IP d'un système à partir duquel des données ont été envoyées.

L'**auditabilité** se définit par la capacité d'un système à garantir la présence d'informations nécessaires à une analyse ultérieure d'un événement (courant ou exceptionnel) effectuée dans le cadre de procédures de contrôle spécifiques et d'audit. Cet audit peut être mis en œuvre pour diagnostiquer ou vérifier l'état de la sécurité d'un système ou encore pour déterminer s'il y a eu ou non violation de la politique de sécurité[1] et, éventuellement quelles sont les ressources compromises. C'est également la fonction destinée à déceler et à examiner les événements susceptibles de constituer une menace pour la sécurité d'un environnement.

Afin de garder la trace des événements, on recourt à des solutions informatiques qui permettent de les enregistrer (de les journaliser), à la manière d'un journal de bord, dans des fichiers (*log*).

Les coûts liés à la journalisation et la capacité mémoire des journaux n'étant pas infinie, l'administrateur système ou le responsable sécurité ont tout intérêt à identifier les événements pertinents et la durée de rétention des informations contenues dans ces journaux qui pourront faire l'objet d'analyse ultérieure lors de la survenue d'incidents, de procédures d'audit ou d'actions en justice. La durée de rétention des données peut être fixée par des réglementations sectorielles ou par la loi, comme c'est le cas par exemple pour les fournisseurs d'accès et de services Internet, qui doivent garder toutes les données de connexion des internautes. Cela permet lors d'enquêtes policières, d'identifier à partir des adresses IP, les internautes soupçonnés d'avoir enfreint la loi.

1.2 Domaines d'application de la sécurité informatique

Pour une organisation, toutes les sphères d'activité de l'informatique et des réseaux de télécommunication sont concernées par la sécurité d'un système d'information.

En fonction de son domaine d'application la sécurité informatique se décline en (figure 1.3) :

- sécurité physique et environnementale ;
- sécurité de l'exploitation ;
- sécurité logique, sécurité applicative et sécurité de l'information ;
- sécurité des infrastructures informatique et de télécommunication (sécurité des réseaux, sécurité Internet et cybersécurité).

1.2.1 Sécurité physique et environnementale

La **sécurité physique** et **environnementale** concerne tous les aspects liés à la maîtrise des systèmes et de l'environnement dans lesquels ils se situent.

1. La politique de sécurité fait l'objet du chapitre 4.

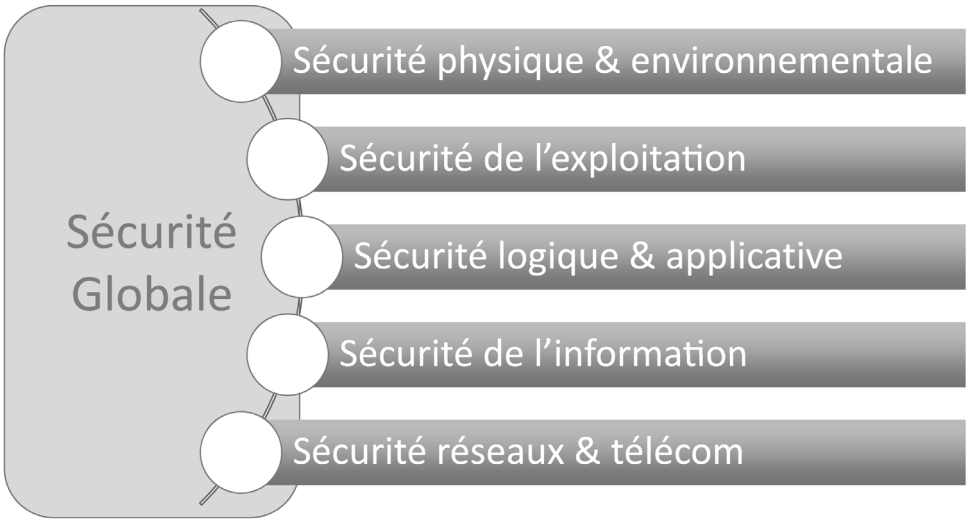

Figure 1.3 – Domaines d'application de la sécurité.

Sans vouloir être exhaustif, nous retiendrons que la sécurité physique repose essentiellement sur :

- la protection des sources énergétiques et de la climatisation (alimentation électrique, refroidissement, etc.) ;
- la protection de l'environnement (mesures *ad hoc* notamment pour faire face aux risques d'incendie, d'inondation ou encore de tremblement de terre… pour respecter les contraintes liées à la température, à l'humidité, etc.) ;
- des mesures de gestion et de contrôle des accès physiques aux locaux, équipements et infrastructures (avec entre autres la traçabilité des entrées et une gestion rigoureuse des clés d'accès aux locaux) ;
- l'usage d'équipements qui possèdent un bon degré de sûreté de fonctionnement et de fiabilité ;
- la redondance physique des infrastructures et sources énergétiques ;
- le marquage des matériels pour notamment contribuer à dissuader le vol de matériel et éventuellement le retrouver ;
- le plan de maintenance préventive (tests, etc.) et corrective (pièces de rechange, etc.) des équipements ce qui relève également de la sécurité de l'exploitation des environnements.

1.2.2 Sécurité de l'exploitation

La **sécurité de l'exploitation** doit permettre un bon fonctionnement opérationnel des systèmes informatiques. Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic, de gestion des performances, de gestion des changements et des mises à jour.

La sécurité de l'exploitation dépend fortement de son **degré d'industrialisation**, qui est qualifié par le niveau de supervision des applications et l'automatisation des tâches. Bien que relevant de la responsabilité de l'exploitation, ces conditions concernent très directement la conception et la réalisation des applications elles-mêmes et leur intégration dans un système d'information.

Les points clés de la sécurité de l'exploitation sont les suivants :

- gestion du parc informatique ;
- gestion des configurations et des mises à jour ;
- gestion des incidents et suivi jusqu'à leur résolution ;
- plan de sauvegarde ;
- plan de secours ;
- plan de continuité ;
- plan de tests ;
- inventaires réguliers et, si possible, dynamiques ;
- automatisation, contrôle et suivi de l'exploitation ;
- analyse des fichiers de journalisation et de comptabilité ;
- gestion des contrats de maintenance ;
- séparation des environnements de développement, d'industrialisation et de production des applicatifs.

La **maintenance** doit être préventive et régulière, et conduire éventuellement à des actions de réparation, voire de remplacement des matériels défectueux.

Au-delà du coût d'une panne entraînant le remplacement des équipements, le **risque d'exploitation** se traduit par une interruption de service ou une perte de données qui peuvent avoir des conséquences préjudiciables pour l'entreprise.

Notons que le domaine de la sécurité de l'exploitation peut, dans une certaine mesure, rejoindre celui des télécommunications, si l'on considère que c'est au niveau des procédures d'exploitation que l'on fixe les paramètres servant à la facturation de l'utilisation des ressources informatiques ou de télécommunication. Toutefois, ceci est plus spécifiquement relatif à la gestion de la comptabilité et à la maîtrise du risque financier. C'est également lors de l'exploitation des ressources que l'on vérifie l'adéquation du niveau de service offert, par rapport à celui spécifié dans un contrat de service et à sa facturation.

1.2.3 Sécurité logique, applicative et sécurité de l'information

La **sécurité logique** fait référence à la réalisation de mécanismes de sécurité par logiciel contribuant au bon fonctionnement des programmes, des services offerts et à la protection des données. Elle s'appuie généralement sur :

- la qualité des développements logiciels et des tests de sécurité ;
- une mise en œuvre adéquate de la **cryptographie** pour assurer intégrité et confidentialité ;
- des **procédures de contrôle d'accès logique, d'authentification** ;

- des procédures de détection de logiciels malveillants, de détection d'intrusions et d'incidents ;
- mais aussi sur un dimensionnement suffisant des ressources, une certaine redondance ainsi que sur des procédures de **sauvegarde** et de restitution des informations sur des supports fiables éventuellement spécialement protégés et conservés dans des lieux sécurisés pour les applications et données critiques.

La sécurité logique fait également référence à la **sécurité applicative** qui doit tenir compte des besoins de sécurité et de robustesse développement des logiciels, des applications et de leur contrôle qualité. Le cycle de vie des logiciels, comme leur intégration dans des environnements de production doit également satisfaire aux exigences de sécurité en termes de disponibilité, de continuité des services, d'intégrité ou de confidentialité.

La **sécurité applicative** comprend le développement pertinent de solutions logicielles (ingénierie du logiciel, qualité du logiciel) ainsi que leur intégration et exécution harmonieuses dans des environnements opérationnels.

Elle repose essentiellement sur l'ensemble des facteurs suivants :

- une méthodologie de développement (en particulier le respect des normes de développement propre à la technologie employée et aux contraintes d'exploitabilité) ;
- la robustesse des applications ;
- des contrôles programmés ;
- des jeux de tests ;
- des procédures de recettes ;
- l'intégration de mécanismes de sécurité, d'outils d'administration et de contrôle de qualité dans les applications ;
- la sécurité des progiciels (choix des fournisseurs, interface sécurité, etc.) ;
- l'élaboration et la gestion des contrats (les relations avec des sous-traitants éventuels comprenant des clauses d'engagement de responsabilité) ;
- un plan de migration des applications critiques ;
- la validation et l'audit des programmes ;
- la qualité et la pertinence des données ;
- un plan d'assurance sécurité.

Bien **protéger l'information**, c'est avant tout comprendre son rôle, son importance stratégique et l'impact des décisions qui la concernent. C'est également assurer son **exactitude** et sa **pérennité** pour le temps nécessaire à son exploitation et à son archivage. Cela nécessite de déterminer le niveau de protection nécessaire aux informations manipulées, par une **classification des données** qui permet de qualifier leur **degré de sensibilité** (normale, confidentielle, etc.) et de les protéger en fonction de ce dernier. Ainsi, à partir d'un tableau mettant en relation le type de données et leur degré de sensibilité, la nature et le nombre de verrous logiques à y affecter peuvent être déterminés et des mesures de sécurité ad hoc développées. Par ailleurs, du point de vue de l'utilisateur, une bonne sécurité doit lui assurer le respect de son intimité numérique (*privacy*) et de ses données personnelles.

1.2.4 Sécurité des infrastructures de télécommunication

La **sécurité des télécommunications** consiste à offrir à l'utilisateur final et aux applications communicantes, une connectivité fiable de « bout en bout ». Cela passe par la réalisation d'une **infrastructure réseau** sécurisée au niveau des accès au réseau et du transport de l'information (sécurité de la gestion des noms et des adresses, sécurité du routage, sécurité des transmissions à proprement parler) et cela s'appuie sur des mesures architecturales adaptées, l'usage de plates-formes matérielles et logicielles sécurisées et une gestion de réseau de qualité.

La sécurité des télécommunications ne peut à elle seule garantir la sécurité des informations. Elle ne constitue qu'un maillon de la chaîne sécuritaire car il est également impératif de sécuriser l'**infrastructure informatique** dans laquelle s'exécutent les programmes. Pris au sens large, cela comprend la sécurité physique et environnementale des systèmes (poste de travail de l'utilisateur, serveur ou système d'information, (figure 1.4)).

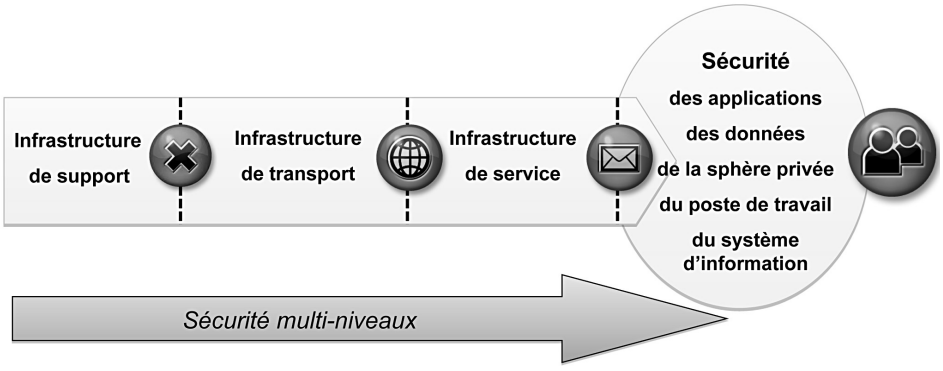

Figure 1.4 – Sécurité des infrastructures de télécommunication.

Pour que les infrastructures informatiques et télécoms soient cohérentes, performantes et sécurisées de manière optimale, l'**infrastructure de sécurité** (outils, procédures, mesures) et la gestion de la sécurité doivent être réalisées de manière sécurisée. Les solutions de sécurité doivent être également sécurisées (notion de **récursivité de la sécurité**).

La sécurité des télécommunications est peu différente de celle que l'on doit mettre en œuvre pour protéger les systèmes. Bien que vulnérables, les réseaux de télécommunication ne le sont pas plus que les systèmes d'extrémité ou que les personnes qui les conçoivent, les gèrent ou les utilisent.

Un environnement informatique et de télécommunication sécurisé implique la sécurisation de tous les éléments qui le compose. La sécurité est toujours celle du maillon le plus faible. Implanter des mécanismes de chiffrement pour rendre les données transférées confidentielles est de peu d'utilité si d'aucun peut y accéder

lorsqu'elles sont manipulées par des plates-formes matérielles et logicielles non correctement sécurisées.

L'implantation de mesures de sécurité doit répondre à des besoins de sécurité clairement identifiés à la suite d'une **analyse des risques** spécifiquement encourus par une organisation. Les besoins s'expriment en termes d'exigences de sécurité à satisfaire au travers d'une **politique de sécurité** (cf. chapitre 4). De plus, un système sécurisé, mobilisant d'importants moyens sécuritaires, aussi pertinents soient-ils, ne pourra être efficace que s'il s'appuie sur des personnes intègres et sur un code d'utilisation adéquat des ressources informatiques pouvant être formalisé par une **charte** de sécurité. Souplesse et confiance réciproque ne peuvent se substituer à la rigueur et au contrôle imposés par le caractère stratégique des enjeux économiques et politiques que doivent satisfaire les systèmes d'information et les réseaux de télécommunications.

Il ne faut jamais oublier que dans le domaine de la sécurité, la confiance n'exclut pas le contrôle ! La sécurité, en tant que propriété d'un système, peut être qualifiable (notion d'assurance de sécurité qui fait référence à la quantification de la qualité de la sécurité). En revanche, la confiance est une relation binaire entre deux entités qui relève du sentiment.

1.2.5 Cas particulier de la cybersécurité

Désormais, un grand nombre d'activités sont réalisées via Internet. L'usage des technologies de l'Internet, les services offerts, les transactions réalisées et les données manipulées sont constitutifs du cyberespace. La racine « **cyber** » provient du mot **cybernétique** qui avait été formé en français en 1834 pour désigner la « science du gouvernement », à partir du grec *Kubernêtiké*, signifiant diriger, gouverner. Terme repris en 1948, par Norman Wiener aux États – Unis et qui a donné naissance à la cybernétique (*cybernetics*), science constituée par l'ensemble des théories relatives au contrôle, à la régulation et à la communication entre l'être vivant et la machine.

Depuis lors, le préfixe cyber contribue à définir des traitements automatiques réalisables par des techniques de l'informatique et des télécommunications. Il est devenu relatif à l'environnement informatique accessible par Internet et la téléphonie mobile et, plus largement, aux activités rendues possibles par les **technologies du numérique**. Dans le cyberespace où tout internaute peut se déplacer (naviguer, surfer), entrer en relation avec des systèmes et des personnes (via toujours des systèmes et des logiciels informatiques) et réaliser (obtenir) des services. Même s'il donne accès à des mondes dits virtuels, le **cyberespace**, est bien réel. Il est rapidement devenu une extension de notre espace naturel et est le reflet de notre société avec ses réalités politique, économique, sociale et culturelle.

La cybersécurité est un sous-ensemble de la sécurité informatique et des réseaux appliqués aux cyberespace et à tout environnement informatique connecté à l'Internet. Elle peut être mise en défaut par des **cyberattaques** informatiques. Du fait de l'usage extensif de l'Internet, de nouvelles menaces sont apparues générant des risques additionnels dont les impacts, de niveaux d'importance variables, peuvent affecter les individus, les organisations ou les États.

1.3 Différentes facettes de la sécurité

1.3.1 Diriger la sécurité

La sécurité informatique d'une organisation doit s'appréhender d'une manière globale et stratégique (notion de stratégie de sécurité) et s'appuie sur :

- la définition d'une **politique de sécurité** ;
- la motivation et la **formation** du personnel ;
- la mise en place de **mesures proactives et réactives** ;
- **l'optimisation** de l'usage des technologies de l'information et des communications (TIC) ainsi que de celui des solutions de sécurité.

L'utilisation seule d'outils de sécurité ne peut pas résoudre les problèmes de sécurité d'une organisation. En aucun cas, ils ne se substituent à une gestion cohérente de l'appréhension des risques et des problématiques de sécurité. Les besoins de sécurité doivent être clairement identifiés et constamment réévalués au regard des risques encourus et de leur évolution.

La prolifération désordonnée d'outils de sécurité non intégrés dans un processus continu de gestion ne peut qu'entraver l'usage, alourdir l'exploitation, générer des coûts ou encore dégrader les performances d'un système d'information.

La sécurité informatique passe également par une gestion rigoureuse des ressources humaines, des systèmes informatiques, des réseaux, des locaux et de l'infrastructure environnementale, des mesures de sécurité. La **maîtrise de la sécurité informatique** est avant tout une question de gestion dont les outils, technologies ou solutions de sécurité constituent une partie liée à la réalisation opérationnelle des environnements sécurisés. Des outils comme ceux de chiffrement ou les pare-feu ne permettent pas de sécuriser correctement un environnement à protéger s'ils ne sont pas inscrits dans une démarche de gestion précise des risques et s'ils ne sont pas accompagnés de procédures qui régissent leur utilisation ou configuration. Ainsi, piloter la sécurité correspond à la volonté de **maîtriser les risques** liés à l'usage des technologies de l'information, les coûts engendrés pour se protéger des menaces et au déploiement des moyens nécessaires pour gérer les incidents ou les situations de crise, pour réagir à une situation non sollicitée mettant en danger la performance du système d'information et celle de l'organisation. Gouverner la sécurité informatique et des télécommunications s'inscrit dans une dimension humaine, organisationnelle, managériale et économique des organisations répondant à une volonté politique de leur direction pour maîtriser les risques et protéger les valeurs.

Ainsi, la sécurité repose sur des axes managériaux, technique et juridique qui doivent être abordés de manière complémentaire. **Elle n'est jamais acquise définitivement**. La constante évolution des besoins, des systèmes, des menaces ou des risques rend instable toute mesure de sécurité. Cela se traduit par un problème de gestion de la qualité constante dans un environnement dynamique et évolutif. Dans ce contexte, la sécurité informatique ne peut s'appréhender que comme un **processus continu de gestion** afin de répondre de manière optimale (en termes de coût et de

niveau de sécurité) aux besoins de production de l'organisation et de protection de ses actifs.

Pour beaucoup d'entreprises, l'outil informatique est un levier essentiel dans leur activité et leur développement. Dans ce cas, l'indisponibilité de l'outil informatique ou son dysfonctionnement constituent un risque majeur. Il peut toutefois être réduit par une gestion rigoureuse des ressources et de leur sécurité.

La démarche de sécurité informatique comme la démarche qualité participent à satisfaire les exigences de rentabilité et de compétitivité des entreprises dont la performance peut être accrue par un système d'information correctement sécurisé. En effet, il ne faut pas perdre de vue la finalité de celui-ci qui est de permettre à l'organisation qui le met en œuvre de réaliser des services ou des produits dont la qualité et les critères de sécurité sont garantis.

1.3.2 Importance du juridique dans la sécurité des systèmes d'information

La **responsabilité** des acteurs (responsable sécurité ou directeur de systèmes d'information par exemple) est de plus en plus invoquée lors de sinistre où les ressources informatiques qu'ils gèrent sont l'objet ou le moyen d'une fraude. Il est nécessaire que les responsables puissent démontrer que des mesures suffisantes de protection du système d'information et des données ont été mises en œuvre afin de se protéger contre un **délit de manquement à la sécurité** (à défaut d'une obligation de résultat, il existe une **obligation de moyens** concernant la sécurité).

Les responsables d'entreprises eux-mêmes doivent être extrêmement attentifs à l'égard du **droit des technologies du numérique** et s'assurer que leur système d'information est en conformité juridique. Désormais, les enjeux juridiques liés à la sécurité informatique sont devenus prépondérants et doivent être pris en compte dans la mise en place de solutions de sécurité, qu'ils soient relatifs à la conservation des données, à la responsabilité des prestataires ou des hébergeurs, à la gestion des données personnelles des clients, à la surveillance des événements informatiques générés par l'activité des employés, à la propriété intellectuelle, aux contrats informatiques ou encore à la signature électronique par exemple. L'**intelligence juridique**[1] devient l'un des facteurs clés du succès de la réalisation de la sécurité informatique des organisations.

Le droit dans le domaine du numérique peut devenir un atout stratégique pour les organisations qui le maîtrisent.

1.3.3 Éthique et formation

Il est nécessaire d'éduquer, d'informer et de former aux technologies de traitement de l'information et des communications, et non uniquement à la sécurité et aux

1. Les aspects juridiques sont abordés au chapitre 3.

mesures de dissuasion. La sensibilisation aux problématiques de sécurité ne doit pas se limiter à la promotion d'une certaine culture de la sécurité et de son éthique. En amont de la culture sécuritaire, il doit exister une véritable culture de l'informatique ; ce qui peut correspondre à la notion de « permis de conduire informatique ».

Une **éthique sécuritaire** doit être développée au sein de l'entreprise pour tous les acteurs du système d'information. Elle doit se traduire par une charte reconnue par chacun et par un engagement personnel à la respecter.

Cette charte déontologique d'utilisation des ressources informatiques et des services Internet doit notamment comprendre des clauses relatives :

- à son domaine d'application ;
- à la définition des moyens et procédures d'accès aux ressources informatiques et services Internet ;
- aux règles d'utilisation professionnelle, rationnelle et loyale des ressources ;
- aux procédures de sécurité ;
- au bon usage des ressources (y compris des données manipulées et transférées) ;
- aux conditions de confidentialité ;
- au respect de la législation concernant les logiciels ;
- au respect de l'intégrité des systèmes informatiques ;
- au rappel des principales lois en vigueur à respecter ;
- aux moyens de contrôle du respect de la charte (surveillance des employés) ;
- aux sanctions encourues en cas de non-respect.

Des **actions de sensibilisation, d'information ou de formation** sur les enjeux, les risques et les mesures préventives et dissuasives de sécurité sont nécessaires pour éduquer l'ensemble du personnel à adopter une démarche sécurité. En fonction du contexte et des besoins, celles-ci peuvent porter, par exemple, sur le développement d'une culture de la sécurité informatique ou encore sur la configuration de pare-feu ou sur les mesures dissuasives ainsi que les conséquences pénales potentielles résultant du non-respect des obligations sécuritaires.

La signature de la **charte de sécurité** doit s'accompagner de moyens aux signataires afin qu'ils puissent la respecter.

1.3.4 Architecture de sécurité

L'**architecture de sécurité** reflète l'ensemble des dimensions organisationnelle, juridique, humaine et technologique de la sécurité informatique à prendre en considération pour une appréhension complète de la sécurité d'une organisation (figure 1.5). Définir une architecture globale de la sécurité permet de visualiser la dimension générale et la nature transversale de la sécurité informatique d'une entreprise et d'identifier ses diverses facettes et composantes afin de pouvoir les développer de façon cohérente, complémentaire et harmonieuse. Cela facilite l'intégration de mesures, de procédures et d'outils de sécurité.

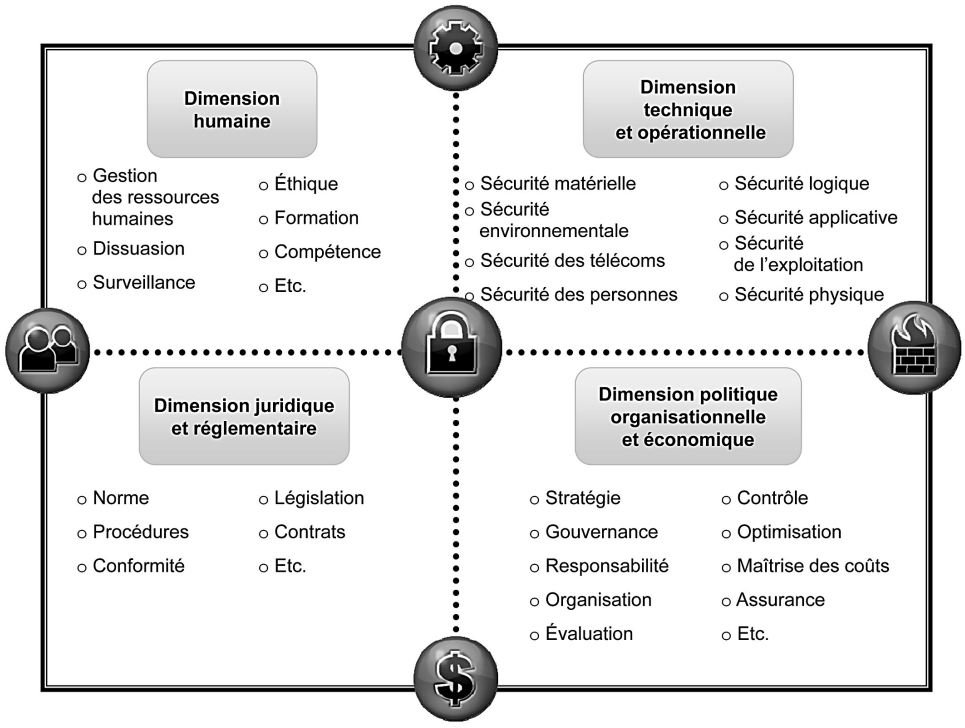

Figure 1.5 – Les différentes dimensions d'une architecture de sécurité.

Une démarche d'assurance des actifs, de gestion des risques, comme le respect des procédures, la formation, le comportement éthique des utilisateurs ou la conformité réglementaire sont autant de points à identifier dans un cadre d'architecture de sécurité. Ainsi, les critères de la sécurité pourront être réalisés judicieusement par le biais de mesures et de procédures complémentaires.

En outre, disposer d'un cadre architectural permet de disposer d'un **référentiel de sécurité** qui facilite la réalisation opérationnelle de la sécurité ainsi que son évaluation lors d'audit. Cette approche permet également de pouvoir identifier les critères minima de sécurité pour chacun des éléments ainsi que leurs interactions et les éventuelles incompatibilités des différents niveaux de sécurité qui pourraient en découler.

La conception d'un système d'information sécurisé passe par la définition d'une structure conceptuelle qu'est l'architecture de sécurité. Celle-ci est fondamentale pour autoriser une approche systémique intégrant une prise en compte complète de l'ensemble des problèmes de sécurité du système d'information et de l'organisation afin de répondre de manière cohérente et globale à sa **stratégie sécuritaire.**

Résumé

Obtenir un niveau de sécurité informatique suffisant pour prévenir les risques technologique et informationnel est primordial tant pour les individus que pour les organisations ou les États qui utilisent ou fournissent des services *via* les technologies du numérique.
Il est important de pouvoir identifier les valeurs à protéger et les risques correctement afin de déterminer les exigences de sécurité et les moyens de les satisfaire. Ceci implique une approche globale, pluridisciplinaire et systémique de la sécurité.
La sécurité informatique doit permettre de répondre aux besoins de disponibilité, d'intégrité et de confidentialité de certaines ressources.
Les télécommunications (infrastructures et services) répondent à une problématique de sécurité peu différente de celle des ressources informatiques dont la résolution répond aux mêmes impératifs techniques, organisationnels, managériaux juridiques et humains. Protéger les informations lors de leur transfert ne suffit pas car ces dernières sont tout aussi vulnérables, sinon plus, lorsqu'elles sont manipulées, traitées et mémorisées.
La sécurité informatique dans le contexte de l'Internet et du cyberespace est le plus souvent dénommée « cybersécurité ».
La sécurité informatique sera effective dans la mesure où l'on sait mettre en place des mesures de protection homogènes et complémentaires des ressources informatiques et de télécommunication, mais aussi de l'environnement qui les héberge. Toutefois, outre des mesures de sécurité proactives de protection des valeurs, il est nécessaire de prévoir des mesures réactives pour pallier la survenue d'incidents non sollicités qu'ils soient d'origine criminelle ou qu'ils relèvent d'erreurs ou de catastrophes naturelles.
Aux aspects purement techniques de la sécurité, il faut associer la mise en œuvre efficace de procédures d'exploitation et de gestion. Par ailleurs, le personnel de l'organisation doit être formé aux mesures de sécurité et doit s'engager à les respecter. Ainsi, la sécurité informatique fait également appel à l'intégrité des personnes qui conçoivent, gèrent, utilisent les infrastructures informatiques et à une gestion appropriée des ressources humaines.

Exercices

1.1 Faites un tableau récapitulatif identifiant les capacités des systèmes, les critères de sécurité et les types de mesures de sécurité permettant de les satisfaire.

1.2 Quels sont les objectifs de la sécurité informatique ?

1.3 Expliquez la notion d'architecture de sécurité. À à quels besoins correspond-elle ? Expliquez de quelle manière les différentes dimensions qui la composent sont complémentaires.

1.4 Dans un réseau de télécommunication, à quels besoins correspondent les notions d'identification et d'authentification, quels services permettent-ils de réaliser ?

1.5 En matière de sécurité informatique, faut-il privilégier une démarche proactive ou réactive ?

1.6 Justifiez que la sécurité informatique et réseau relève d'une problématique de gestion.

1.7 Pourquoi doit-on appréhender la sécurité de manière globale ?

1.8 Expliquez de quelle manière le critère de non-répudiation contribue à la sécurité informatique.

1.9 Quelles peuvent être les origines d'un problème de sécurité informatique ?

1.10 Pourquoi en matière de sécurité informatique, la sécurité physique est importante ?

1.11 Qu'est-ce que la cybersécurité ?

Solutions

1.1 Du point de vue de la sécurité informatique, les systèmes doivent offrir les caractéristiques suivantes (tableau 1.1) :

- **Capacité d'un système à pouvoir être utilisé** — cela correspond à la disponibilité des ressources et des services, fonction de leur dimensionnement correct et d'une certaine redondance des ressources, mais également des procédures de sauvegarde, de reprise et d'exploitation adaptées aux besoins de fonctionnement.
- **Capacité d'un système à exécuter les actions et à rendre les services que l'on attend de lui dans des conditions de performance et d'utilisation adaptées** — cela traduit un besoin de continuité, de durabilité, de fiabilité, de convivialité et de sûreté de fonctionnement.
- **Capacité d'un système à ne permettre l'accès aux données qu'aux personnes et processus autorisés** — pour offrir confidentialité et intégrité des données. Elles sont assurées par des processus de contrôle d'accès, d'erreur, de cohérence et par des mécanismes de chiffrement.
- **Capacité d'un système à prouver que des actions, transactions ont bien eu lieu** à des fins de traçabilité, de preuve, d'imputabilté, de contrôle, d'audit ou de non-répudiation d'actions ou d'événements.

Ces diverses capacités permettent des services de qualité dans des conditions déterminées et peuvent être appréhendées comme des critères de sécurité ou des compétences de sécurité. Leur réalisation passe par la mise en œuvre de mesures spécifiques de sécurité contribuant à bâtir la confiance que peut avoir un utilisateur envers son environnement informatique.