PRESIDENCE DE LA REPUBLIQUE

REPUBLIQUE DE COTE D'IVOIRE
Union – Discipline – Travail

ANNEXE I AU DECRET N° 2021-916 DU 22 DECEMBRE 2021 PORTANT ADOPTION DU REFERENTIEL GENERAL DE SECURITE DES SYSTEMES D'INFORMATION ET DU PLAN DE PROTECTION DES INFRASTRUCTURES CRITIQUES

UNION – DISCIPLINE – TRAVAIL

REPUBLIQUE DE CÔTE D'IVOIRE

REFERENTIEL GENERAL DE SECURITE DES SYSTEMES D'INFORMATION (RGSSI)

Référentiel de sécurité pour l'audit des systèmes d'informations

SOMMAIRE

1. Introduction

Parallèlement au développement des technologies du numérique, on assiste aujourd'hui à la montée en puissance des vulnérabilités des systèmes d'information à cause de la multiplication et de la diversification des activités illicites dans le cyberespace et des attaques informatiques qui perturbent à maintes reprises, le fonctionnement des systèmes d'information et de communication de nombre de pays.

Il s'agit pour la Côte d'Ivoire de mettre en œuvre des politiques et/ou stratégies en vue de protéger son espace numérique, de doter les systèmes d'information des organisations établies sur le territoire, d'une capacité de défense et de résilience à même de créer les conditions d'un environnement de confiance et de sécurité propice au développement de la société de l'information.

L'une des principales actions prises consiste à auditer annuellement les systèmes d'informations des personnes morales afin d'élever et d'homogénéiser le niveau de protection et le niveau de maturité de la sécurité de l'ensemble des systèmes d'information des administrations et organismes privés ainsi que des infrastructures d'importance vitale.

Pour se protéger des vulnérabilités, les organismes doivent, à l'issue d'une démarche de gestion des risques, sécuriser leur système d'information de façon adaptée et proportionnée. Les mesures de sécurité mises en place dans ce but, peuvent être de différentes natures : organisationnelles, physiques et techniques. Sur ce dernier volet, la mise en œuvre de produits de sécurité est certes fondamentale, mais paraît, à elle seule insuffisante : l'absence d'application des mises à jour et des correctifs de sécurité, le maintien de mots de passe faibles ou constructeurs, la mauvaise configuration de logiciels ou le non-respect de règles élémentaires de sécurité lors du développement d'un logiciel ou d'une application sont autant de vulnérabilités exploitables par un attaquant.

L'audit est l'un des moyens à disposition de tout organisme pour éprouver et s'assurer du niveau de sécurité de son système d'information. Il permet, en pratique, de mettre en évidence les forces mais surtout les faiblesses et les vulnérabilités du système d'information. Ses conclusions permettent d'identifier les axes d'amélioration, de proposer des recommandations et de contribuer ainsi, à l'élévation de son niveau de sécurité, en vue notamment, de son homologation de sécurité.

Le Référentiel Général de Sécurité fixe les règles auxquelles sont soumises les fonctions des systèmes d'information contribuant à la sécurité des données échangées par voie électronique telles que les fonctions d'identification, de signature électronique, de confidentialité et d'intégrité.

2. Contexte

Dans le cyberespace, monde immatériel, les conséquences des attaques informatiques contre les systèmes d'information des États, des entreprises ou contre les ordinateurs des citoyens ne sont le plus souvent visibles que des spécialistes et restent ignorées du grand public.

Le cyberespace offre un potentiel exceptionnel pour la réalisation de toutes sortes d'infractions même économiques, par la mise en péril d'infrastructures critiques, commises de façon isolée ou organisée. Il s'agit notamment de l'appropriation de données personnelles, de l'espionnage du patrimoine scientifique, économique et commercial d'entreprises victimes de leurs concurrents ou de puissances étrangères, de l'arrêt de services nécessaires au bon fonctionnement de l'économie ou de la vie quotidienne, de la compromission d'informations de souveraineté et

même, dans certaines circonstances, de la perte de vies humaines qui sont aujourd'hui, les conséquences potentielles ou réelles de l'imbrication entre le numérique et l'activité humaine.

Devant l'irruption du cyberespace dans le champ de la sécurité nationale et à la mesure des enjeux, la loi n°2017-803 du 07 décembre 2017 d'orientation de la société de l'information en Côte d'Ivoire, vient définir les droits, rôles et responsabilités des acteurs publics et privés dans la société de l'information.

Ainsi, aux termes de son article 13, « ... *l'Etat met en œuvre, une législation appropriée permettant la sanction aux droits et aux libertés d'autrui, à l'ordre public et aux bonnes mœurs, commisses par voie électronique. L'Etat, seul ou en collaboration avec les collectivités territoriales, les structures et établissements publics, les entreprises privées et les organisations de la société civile, œuvre pour la vulgarisation de l'utilisation des TIC et pour une lutte efficace contre la cybercriminalité. L'Etat adopte et met en œuvre, une stratégie de cybersécurité et une politique de coopération judiciaire et sécuritaire en matière de lutte contre la cybercriminalité* ».

A cet égard, le législateur a confié à l'ARTCI, la mission d'assurer la sécurité des réseaux et systèmes d'information, au plan national.

En effet, en application des dispositions de l'article 50 de la loi N° 2013-456 du 30 juillet 2013 relative aux transactions électroniques, l'ARTCI procède à « *l'audit et à la certification des systèmes d'information des personnes morales établies en Côte d'Ivoire et exerçant des activités de transactions électroniques* ».

Par ailleurs, l'ordonnance n°2017-500 du 02 août 2017 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, fait obligation à l'ARTCI de définir un ensemble de règles et d'exigences de sécurité et auxquelles les systèmes d'information doivent être conformes à travers le RGSSI.

Le présent Référentiel Général de Sécurité des Systèmes d'Information (RGSSI) s'est fortement inspiré des normes ISO 27001 : 2013 et ISO 27002 : 2013 afin de le hisser aux normes internationales.

Le RGSSI décrit les mesures de sécurité organisationnelles et techniques qui doivent être appliquées par les administrations et ses démembrements et les organismes privés ainsi que les infrastructures d'importance vitale.

3. Objectif du référentiel

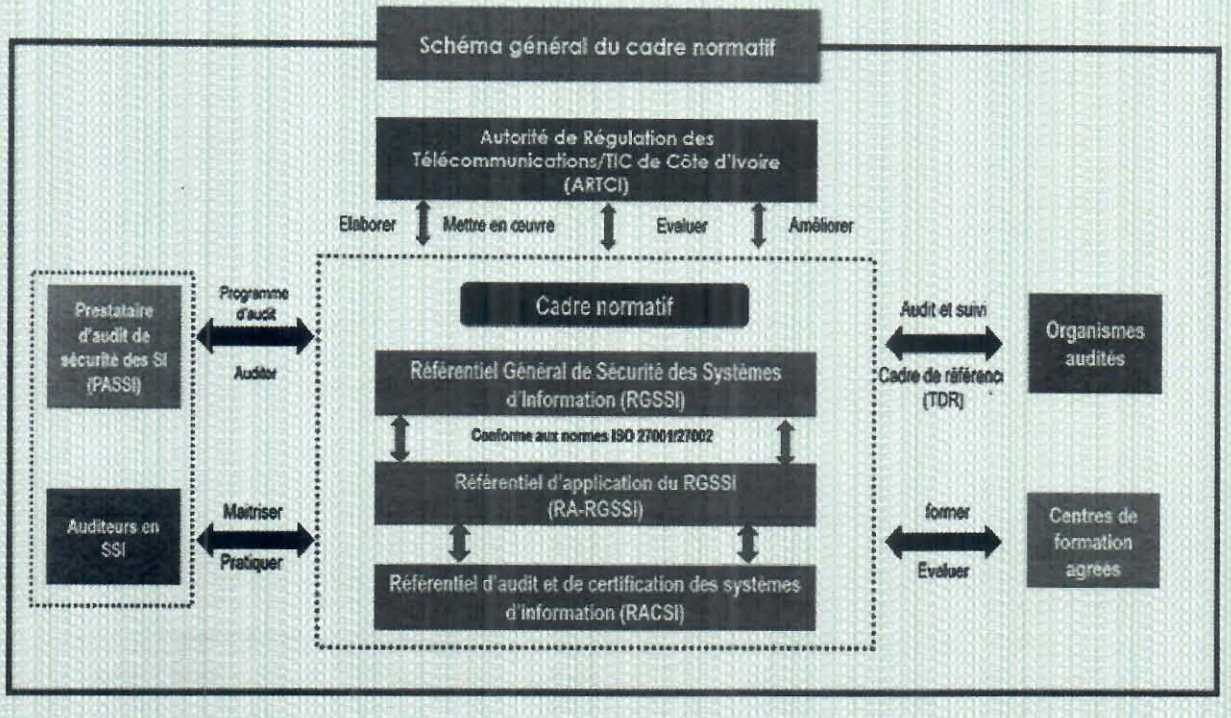
L'objectif de ce document est de représenter la norme ivoirienne en matière de sécurité des systèmes d'information pour faciliter les échanges électroniques sécurisés. Il inclut les règles et exigences de sécurité spécifiques aux infrastructures critiques.

Le présent référentiel vise notamment à :

- favoriser l'adoption par les administrations et les organismes privés de bonnes pratiques en matière de sécurité des systèmes d'information ;
- adapter les solutions techniques aux justes besoins de sécurité identifiés pour chaque système d'information ;
- offrir aux autorités administratives et privées les labels de sécurité permettant de s'assurer de la qualité des produits et des services de sécurité proposés par le marché ;

Le référentiel général de sécurité des systèmes d'information (RGSSI) constitue ainsi l'un des composants du cadre normatif pour la sécurité des systèmes d'information en Côte d'Ivoire.

Le schéma général du cadre normatif, ci-dessous, présente la structure dudit cadre et ses implications sur les différents intervenants que sont: l'ARTCI, les Organismes audités aussi bien du secteur public que privé, les centres de formations, les prestataires d'audit en sécurité des systèmes d'information et les auditeurs en sécurité des systèmes d'information.



Contenu du référentiel

L'audit de la sécurité des systèmes d'information est un jalon de l'amélioration de la maturité de la sécurité du système d'information en vue d'établir un équilibre entre les risques et les bénéfices de l'utilisation des moyens de traitement de l'information et d'assurer une amélioration quantifiable, efficace et efficiente des processus qui s'y rapporte.

Le référentiel d'audit repose sur cent trente-huit (138) critères regroupés en seize (16) Domaines numérotés de D1 à D16 ainsi qu'il suit :

D1. Leadership et gouvernance de la sécurité de l'information
D2. Politiques de sécurité de l'information
D3. Organisation de la sécurité de l'information
D4. Gestion des risques liés à la sécurité de l'information
D5. Sécurité des ressources humaines
D6. Gestion des actifs informationnels
D7. Contrôle d'accès
D8. Cryptographie
D9. Sécurité physique et environnementale
D10. Sécurité liée à l'exploitation
D11. Sécurité des communications
D12. Acquisition, développement et maintenance des systèmes d'information
D13. Relations avec les fournisseurs

D14. Gestion des incidents liés à la sécurité de l'information
D15. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
D16. Conformité

4. Les Termes et Définitions

Pour les besoins du présent référentiel, les termes et définitions employés sont définis suivant les dispositions de la norme internationale ISO 27000.

5. Leadership & gouvernance de la sécurité de l'information (D1)

5.1 Leadership et engagement

Le responsable de l'organisation doit faire preuve de leadership et affirmer son engagement en faveur de la sécurité de son système d'information.

A ce titre, l'organisation doit :

a) s'assurer qu'une politique et des objectifs soient établis en matière de sécurité de l'information et qu'ils sont compatibles avec l'orientation stratégique de l'organisation ;

b) s'assurer que les exigences liées à la sécurité de l'information soient intégrées aux processus métiers de l'organisation ;

c) s'assurer que les ressources nécessaires pour la gestion de la sécurité de l'information soient disponibles ;

d) communiquer sur l'importance de disposer d'un management de la sécurité de l'information efficace et de se conformer aux exigences légales et réglementaires et aux normes internationales et les bonnes pratiques ;

e) S'assurer que le système de management de la sécurité de l'information produit le ou les résultats escomptés;

f) orienter et soutenir les personnes pour qu'elles contribuent à l'efficacité de la gestion de la sécurité de l'information ;

g) promouvoir l'amélioration continue de la gestion de la sécurité de l'information et aider les personnes qui en sont responsables à faire également preuve de leadership dès lors que cela s'applique à leurs domaines de responsabilités ;

h) Aider les autres managers concernés à faire également preuve de leadership dès lors que cela s'applique à leurs domaines de responsabilités.

5.2 Rôles, responsabilités et autorités au sein de l'organisation

Le responsable de l'organisation doit s'assurer que les responsabilités et autorités des rôles concernés par la sécurité de l'information sont attribuées et communiquées au sein de l'organisation.

6. Politiques de sécurité de l'information (D2)

L'organisation doit apporter à la sécurité de l'information, une orientation et un soutien de la part de sa direction, conformément aux exigences métier et aux lois et règlements en vigueur.

6.1 Politiques de sécurité de l'information

L'organisation est tenue de définir un ensemble de politiques en matière de sécurité de l'information approuvés par la direction, diffusés et communiqués aux salariés ainsi qu'aux tiers concernés.

Elle doit définir à son plus haut niveau, une « Politique générale de sécurité de l'information », approuvée par la direction et décrivant l'approche adoptée pour gérer les objectifs de sécurité de l'information.

A cet effet, les politiques générales de sécurité de l'information traitent des exigences créées par :

a) la stratégie d'entreprise;

b) les réglementations, la législation et les contrats;

c) l'environnement réel et anticipé des menaces liées à la sécurité de l'information ;

Cette politique générale de sécurité de l'information comporte des précisions concernant:

a) la définition de la sécurité de l'information, ses objectifs et ses principes pour orienter toutes les activités relatives à la sécurité de l'information;

b) l'attribution des responsabilités générales et spécifiques en matière de management de la sécurité de l'information à des fonctions définies;

c) les processus de traitement des dérogations et des exceptions.

A un niveau inférieur, la politique spécifique de sécurité de l'information doit être étayée par des politiques portant sur des thèmes spécifiques qui imposent notamment, la mise en œuvre de mesures de sécurité de l'information, structurées pour répondre aux besoins de certains groupes cibles d'une organisation ou pour englober certains thèmes, dont :

a) le contrôle d'accès;

b) la classification (et le traitement) de l'information ;

c) la sécurité physique et environnementale;

d) ceux axés sur l'utilisateur final, notamment:

   1) l'utilisation correcte des actifs ;

   2) le bureau propre et écran vide;

   3) le transfert de l'information ;

   4) les appareils mobiles et le télétravail;

5) les restrictions en matière d'installation et d'utilisation de logiciels;

e) la stratégie de sauvegarde et de rétention des données;

f) le transfert de l'information ;

g) la protection contre les logiciels malveillants ;

h) la gestion des vulnérabilités techniques;

i) les mesures de sécurité cryptographiques;

j) la sécurité des communications;

k) la protection de la vie privée et des informations personnelles identifiables;

l) les relations avec les fournisseurs.

Le besoin en politiques internes liées à la sécurité de l'information varie en fonction des organisations.

Les politiques doivent être communiquées aux salariés et aux tiers concernés sous une forme pertinente, accessible et compréhensible par leurs destinataires, par exemple, «programme d'apprentissage, de formation et de sensibilisation à la sécurité de l'information à l'endroit des salariés».

Les politiques de sécurité de l'information peuvent être diffusées dans un document unique dénommé « politique de sécurité de l'information » ou dans un ensemble de documents séparés, mais interdépendants. Si l'une quelconque des politiques de sécurité de l'information est diffusée hors de l'organisation, il importe de veiller à ne pas divulguer d'informations confidentielles.

6.2 Revue des politiques de sécurité de l'information

Pour garantir la constance de la pertinence, de l'adéquation et de l'efficacité des politiques liées à la sécurité de l'information, l'organisation doit revoir ses politiques à intervalles réguliers ou en cas de changements majeurs. Chaque politique doit avoir un propriétaire ayant accepté la responsabilité de la développer, de la revoir et de l'évaluer.

La revue comporte une appréciation des possibilités d'amélioration de la politique de l'organisation et une approche de management de la sécurité de l'information pour répondre aux changements intervenant dans l'environnement organisationnel, aux circonstances liées à l'activité, au contexte juridique ou à l'environnement technique. Elle tient également compte des revues de direction. Une fois révisée, la politique de sécurité est approuvée par la direction.

7. Organisation de la sécurité de l'information (D3)

L'organisation doit établir un cadre de gestion pour engager, puis vérifier la mise en œuvre ainsi que le fonctionnement de la sécurité de l'information en son sein.

7.1 Fonctions et responsabilités liées à la sécurité de l'information

Les responsabilités en matière de sécurité de l'information doivent être attribuées conformément à la politique générale de sécurité de l'information.

Il convient de déterminer d'une part, les responsabilités liées à la protection des actifs individuels et la mise en œuvre de processus de sécurité spécifiques et d'autre part, celles liées aux activités de gestion des risques en matière de sécurité de l'information et, en particulier, les responsabilités liées à l'acceptation des risques résiduels.

Si nécessaire, des directives détaillées appropriées à certains sites et moyens de traitement de l'information pourront compléter ces responsabilités.

Il convient de déterminer les responsabilités locales en ce qui concerne la protection des actifs et la mise en œuvre des processus de sécurité spécifiques.

Il convient de préciser les domaines de responsabilité de chacun et notamment de prendre les mesures suivantes :

a) identifier et déterminer les actifs et les processus de sécurité;

b) affecter une entité responsable à chaque actif ou processus et de documenter ses responsabilités dans le détail;

c) définir et documenter les différents niveaux d'autorisation;

d) Pour être à même d'assurer les responsabilités relevant de leur domaine en matière de sécurité, il convient que les personnes désignées soient compétentes dans ce domaine et qu'elles bénéficient de possibilités leur permettant de se tenir au courant des évolutions;

e) I identifier et documenter les activités de coordination et de supervision relatives aux questions de sécurité liées aux relations avec les fournisseurs.

7.2 Séparation des tâches

L'organisation doit séparer les tâches et les domaines de responsabilité incompatibles pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation.

Il convient de veiller à ce que personne ne puisse accéder à, modifier ou utiliser des actifs sans en avoir reçu l'autorisation ou sans avoir été détecté. Il convient de séparer le déclenchement d'un événement de son autorisation. Il convient d'envisager la possibilité de collusion lors de la conception des mesures.

Lorsqu'il est difficile de procéder à la séparation des tâches, il convient d'envisager d'autres mesures comme la surveillance des activités, des systèmes de traçabilité et la supervision de la direction.

7.3 Relations avec les autorités compétentes

L'organisation doit entretenir des relations appropriées avec les autorités compétentes notamment l'autorité en charge de la sécurité des systèmes d'information.

Il convient que les organisations mettent en place des procédures spécifiant quand et comment il convient de contacter les autorités compétentes (par exemple, les autorités chargées de l'application des lois, les organismes de réglementation, les autorités de surveillance).

Ces procédures définissent également comment il convient de signaler dans les meilleurs délais les incidents liés à la sécurité de l'information (par exemple, en cas de suspicion de violation de la loi).

Les organisations subissant une cyberattaque peuvent recourir aux autorités compétentes pour engager des actions requises.

Les relations avec les autres autorités concernent les services collectifs, les services d'urgence, les fournisseurs d'électricité, la santé et la sécurité, comme la caserne de pompiers (pour la continuité de l'activité), les opérateurs en télécommunication (pour le routage et la disponibilité), les fournisseurs de services Internet, etc.

7.4 Relations avec des groupes de travail spécialisés

L'organisation doit entretenir des relations appropriées avec des groupes d'intérêt, des forums spécialisés dans la sécurité et des associations professionnelles.

Il convient d'envisager une inscription à des groupes d'intérêt ou à des foras spécialisés aux fins suivantes :

a) mieux connaître les bonnes pratiques et se tenir informé de l'évolution des savoirs relatifs à la sécurité ;

b) s'assurer que la connaissance de l'environnement de la sécurité de l'information est à jour et exhaustive ;

c) recevoir rapidement des alertes, des conseils et des correctifs logiciels portant sur les attaques et les vulnérabilités ;

d) avoir accès à des conseils de spécialistes sur la sécurité de l'information ;

e) partager et échanger des informations sur les nouvelles technologies, les produits, les menaces ou les vulnérabilités ;

f) mettre en place des relais d'information appropriés lors du traitement d'incidents liés à la sécurité de l'information.

Des accords de partage de l'information peuvent être établis en vue d'améliorer la coopération et la coordination dans le domaine de la sécurité. De tels accords identifient les exigences en matière de protection des informations confidentielles.

7.5 La sécurité de l'information dans la gestion de projet

L'organisation doit traiter la sécurité de l'information dans la gestion de projet, quel que soit le type de projet concerné.

Il convient d'intégrer la sécurité de l'information dans la ou les méthodes de gestion de projet de l'organisation pour veiller à ce que les risques de sécurité de l'information soient identifiés et traités dans le cadre dudit projet.

Cette préconisation s'applique de manière générale à tout projet quel qu'il soit, indépendamment de sa nature ; c'est le cas d'un projet lié à un processus clé de l'activité, aux technologies de l'information, à la gestion des installations et autres processus.

Les méthodes de gestion de projet en vigueur imposent que :

a) les objectifs en matière de sécurité de l'information soient intégrés aux objectifs du projet;

b) une appréciation du risque de sécurité de l'information soit effectuée au commencement du projet pour identifier les mesures nécessaires;

c) la sécurité de l'information soit intégrée à toutes les phases de la méthodologie de projet appliquée.

Pour tous les projets, il convient de traiter et de revoir régulièrement les incidences sur la sécurité de l'information. Il convient de déterminer et d'attribuer les responsabilités en matière de sécurité de l'information à des fonctions spécifiques définies dans les méthodes de gestion de projet.

7.6 Politique en matière d'appareils mobiles

L'organisation doit adopter une politique et des mesures de sécurité complémentaires pour gérer les risques découlant de l'utilisation des appareils et terminaux mobiles.

Lors de l'utilisation d'appareils mobiles, il convient de veiller particulièrement à ce que les informations liées à l'activité de l'organisation ne soient pas compromises. Il convient que la politique en matière d'appareils mobiles tienne compte des risques liés au fait de travailler avec des appareils mobiles dans des environnements non protégés.

Il convient que la politique en matière d'appareils mobiles envisage :

a) l'enregistrement des appareils mobiles;

b) les exigences liées à la protection physique;

c) les restrictions liées à l'installation de logiciels;

d) les exigences liées aux versions logicielles des appareils mobiles et à l'application de correctifs;

e) les restrictions liées aux connexions à des services d'information;

f) les contrôles d'accès;

g) les techniques cryptographiques;

h) la protection contre les logiciels malveillants;

i) la désactivation, l'effacement des données ou le verrouillage à distance;

j) les sauvegardes;

k) l'utilisation des services web et des applications web.

Il convient d'être vigilant lors de l'utilisation d'appareils mobiles dans des lieux publics, des salles de réunions et autres zones non protégées.

Il convient de mettre en place des mesures de protection visant à empêcher les accès non autorisés ou la divulgation d'informations stockées et traitées par ces appareils, par exemple en utilisant des techniques cryptographiques et en imposant l'utilisation d'informations d'authentification secrètes.

Il convient également que les appareils mobiles soient physiquement protégés contre le vol, en particulier lorsqu'ils sont laissés, par exemple, dans un véhicule privé ou tout autre moyen de transport, une chambre d'hôtel, un centre de congrès ou une salle de réunion.

Il convient d'établir une procédure spécifique tenant compte des exigences juridiques, des exigences liées aux assurances et des exigences de sécurité de l'organisation, en cas de vol ou de perte d'appareils mobiles.

Il convient de ne pas laisser sans surveillance les appareils dans lesquels sont stockées des informations importantes, sensibles ou critiques liées à l'activité de l'organisation et, si possible, de les mettre sous clé ou de les doter de systèmes de verrouillage spéciaux.

Il convient d'organiser, à destination des personnes utilisant des appareils mobiles, des formations de sensibilisation aux risques supplémentaires liés à ce mode de travail et aux mesures de sécurité qu'il convient de mettre en œuvre.

Lorsque la politique en matière d'appareils mobiles autorise l'utilisation d'appareils mobiles personnels, il convient que la politique et les mesures de sécurité complémentaires envisagent également :

a) une séparation entre l'utilisation privée et l'utilisation professionnelle des appareils, impliquant la mise en œuvre d'un logiciel pour faciliter cette séparation et protéger les données liées à l'activité de l'organisation figurant sur un appareil privé;

b) de ne permettre l'accès aux informations de l'organisation que lorsque l'utilisateur a signé un contrat d'utilisateur final par lequel il prend acte de ses missions (protection physique, mise à jour des logiciels, etc.), renonce à la propriété des données de l'organisation et autorise l'entreprise à effacer ses données à distance en cas de perte ou de vol de l'appareil, ou lorsque son utilisation n'est plus autorisée. Cette politique doit tenir compte de la législation en vigueur sur la protection de la vie privée.

Les connexions sans fil des appareils mobiles reposent sur le même principe que les autres types de connexion réseau. Cependant, elles présentent des différences importantes qu'il convient de prendre en compte lors de la définition des mesures de sécurité. Différences typiques :

c) certains protocoles de sécurité sans fil sont en phase de rodage et leurs failles sont connues;

d) la sauvegarde des informations stockées sur les appareils mobiles n'est pas toujours possible en raison d'une bande passante limitée ou parce que les appareils mobiles ne sont pas connectés au moment où les sauvegardes automatiques sont programmées.

7.7 Télétravail

L'organisation doit mettre en œuvre une politique et des mesures de sécurité complémentaires pour protéger les informations consultées, traitées ou stockées sur des sites de télétravail.

Le télétravail renvoie à toutes les formes de travail effectué en dehors des locaux de l'organisation, et comprend les environnements de travail non traditionnels, tels que les environnements connus sous le nom de « travail à distance », « tiers-lieu », « espaces flexibles » et « travail virtuel ». La direction doit s'assurer que les responsabilités et autorités des rôles concernés par la sécurité de l'information sont attribuées et communiquées au sein de l'organisation.

Il convient que les organisations autorisant les activités de télétravail émettent une politique définissant les conditions et les restrictions d'utilisation liées au télétravail. Il convient d'envisager les aspects suivants lorsqu'ils sont pertinents :

a) le niveau de sécurité physique en place sur le site de télétravail, y compris le niveau de sécurité physique du bâtiment et de l'environnement immédiat ;

b) l'environnement physique de télétravail proposé ;

c) les exigences en matière de sécurité des communications, en tenant compte de la nécessité d'accéder à distance aux systèmes internes de l'organisation, de la sensibilité des informations consultées ou transmises via le réseau de communication et de la sensibilité du système interne ;

d) la fourniture de l'accès à un bureau virtuel, évitant le traitement et le stockage des informations sur un équipement détenu à titre privé ;

e) la menace que représente l'accès non autorisé aux informations ou ressources par d'autres personnes présentes dans l'espace, par exemple des membres de la famille, des amis ;

Il convient d'inclure aux lignes directrices et aux dispositions à prendre en compte :

a) la fourniture des matériels et des meubles de rangement adaptés aux activités de télétravail, en cas d'interdiction d'utilisation d'un matériel détenu à titre privé et non soumis au contrôle de l'organisation;

b) la définition des tâches autorisées, les heures de travail, la classification des informations susceptibles d'être détenues, ainsi que les systèmes et services internes auxquels le télétravailleur est autorisé à accéder;

c) la fourniture d'un appareil de communication approprié, ainsi que des méthodes de sécurisation de l'accès à distance;

d) la sécurité physique;

e) les règles et préconisations concernant l'accès de la famille et des visiteurs au matériel et aux informations;

f) la fourniture de services d'assistance et de maintenance matérielles et logicielles;

g) la souscription d'une assurance;

h) les procédures relatives à la sauvegarde et à la continuité de l'activité;

i) l'audit et la surveillance liée à la sécurité;

j) la révocation des droits d'utilisation et des droits d'accès, ainsi que la restitution du matériel au terme des activités de télétravail.

8. Gestion des risques liés à la sécurité du système d'information (D4)

8.1 Actions liées aux risques et opportunités

Chaque organisation doit tenir compte des enjeux et des exigences, et déterminer les risques et opportunités qui nécessitent d'être abordés pour sécuriser son système d'information :

a) s'assurer que la stratégie de la sécurité de l'information peut atteindre le ou les résultats escomptés ;

b) empêcher ou limiter les effets indésirables ;

c) appliquer une démarche d'amélioration continue.

A ce titre, elle pourrait se référer aux normes internationales reconnues relatives à la gestion des risques en sécurité de l'information, dans leurs versions à jour.

L'organisation doit planifier :

a) les actions menées pour traiter ces risques et opportunités ;

b) la manière d'intégrer et de mettre en œuvre les actions au sein des processus pour garantir la sécurité de l'information ;

c) la manière d'évaluer l'efficacité de ces actions.

8.2 Appréciation des risques de sécurité de l'information

L'organisation doit définir et appliquer un processus d'appréciation des risques de sécurité de l'information qui :

a) établit et tient à jour les critères de risque de sécurité de l'information incluant :

   1) les critères d'acceptation des risques ;

   2) les critères de réalisation des appréciations des risques de sécurité de l'information ;

b) s'assure que la répétition de ces appréciations des risques produit des résultats cohérents, valides et comparables ;

c) identifie les risques de sécurité de l'information en :

   1) appliquant le processus d'appréciation des risques de sécurité de l'information pour identifier les risques liés à la perte de confidentialité, d'intégrité et de disponibilité des informations du système de l'information de l'organisation ;et

   2) identifiant les propriétaires des risques ;

d) analyse les risques de sécurité de l'information en :

   1) appréciant les conséquences potentielles dans le cas où les risques identifiés se concrétisaient ;

   2) procédant à une évaluation réaliste de la vraisemblance d'apparition des risques identifiés ; et

   3) déterminant les niveaux des risques ;

e) évalue les risques de sécurité de l'information en:

   1) comparant les résultats d'analyse des risques avec les critères de risque déterminés ; et

2) priorisant les risques analysés pour le traitement des risques.

Chaque organisation doit conserver des informations documentées sur le processus d'appréciation des risques de sécurité de l'information.

8.3 Traitement des risques de sécurité de l'information

Chaque organisation doit définir et appliquer un processus de traitement des risques de sécurité de l'information pour :

a) choisir les options de traitement des risques appropriées, en tenant compte des résultats de l'appréciation des risques ;

b) déterminer toutes les mesures nécessaires à la mise en œuvre des options de traitement des risques de sécurité de l'information choisie ;

c) élaborer un plan de traitement des risques de sécurité de l'information ; et

d) obtenir des propriétaires des risques l'approbation du plan de traitement des risques et l'acceptation des risques résiduels de sécurité de l'information.

Chaque organisation doit conserver des informations documentées sur le processus de traitement des risques de sécurité de l'information.

8.4 Objectifs de sécurité de l'information et plans pour les atteindre

L'organisation doit établir, aux fonctions et niveaux concernés, des objectifs de sécurité de l'information. Les objectifs de sécurité de l'information doivent :

a) être cohérents avec la politique de sécurité de l'information ;

b) être mesurables (si possible) ;

c) tenir compte des exigences applicables à la sécurité de l'information, et des résultats de l'appréciation et du traitement des risques ;

d) être communiqués et être mis à jour quand cela est approprié.

Chaque organisation doit conserver des informations documentées sur les objectifs liés à la sécurité de l'information.

9. Sécurité des ressources humaines (D5)

L'organisation doit s'assurer que les salariés et les contractants comprennent leurs responsabilités et qu'ils sont compétents pour remplir les fonctions que l'organisation envisage de leur confier.

Il convient que les accords contractuels conclus avec les salariés et les contractants déterminent leurs responsabilités et celles de l'organisation en matière de sécurité de l'information.

9.1 Avant l'embauche

L'organisation doit s'assurer que les salariés et les contractants comprennent leurs responsabilités et qu'ils sont compétents pour remplir les fonctions que l'organisation envisage de leur confier.

9.1.1 Sélection des candidats

Il convient que des vérifications des informations concernant tous les candidats à l'embauche soient réalisées conformément aux lois, aux règlements et à l'éthique, et il convient qu'elles soient proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés.

9.1.2 Termes et conditions d'embauche

Il convient que les accords contractuels conclus avec les salariés et les contractants déterminent leurs responsabilités et celles de l'organisation en matière de sécurité de l'information.
Il convient que les obligations contractuelles des salariés ou des contractants stipulent et précisent clairement les aspects suivants, en mettant en évidence les politiques de sécurité de l'information de l'organisation :

a) il convient que tous les salariés et contractants ayant accès à des informations confidentielles signent un engagement de confidentialité ou de non-divulgation avant d'obtenir l'accès aux moyens de traitement de l'information ;

b) les responsabilités juridiques et les droits des salariés ou des contractants concernant par exemple les droits de reproduction et la législation sur la protection des données ;

c) les responsabilités relatives à la classification des informations et à la gestion des actifs de l'organisation liés aux informations, aux systèmes de traitement des informations et aux services d'information que le salarié ou le contractant utilise ;

d) les responsabilités du salarié ou du contractant quant à la manipulation de l'information reçue de la part d'autres organisations ou tiers ;

e) les actions à engager si le salarié ou le contractant ne tient pas compte des exigences en matière de sécurité de l'organisation.

Lors du processus de pré embauche, il convient d'informer clairement les candidats à l'embauche des rôles et des responsabilités en matière de sécurité. Il convient que l'organisation s'assure que les salariés et les contractants approuvent les dispositions relatives à la sécurité de l'information concernant la nature et l'étendue de leur futur accès aux actifs de l'organisation liés aux services et aux systèmes d'information.
Si nécessaire, il convient que les responsabilités stipulées dans le contrat de travail continuent à s'appliquer pendant une durée définie après la fin du contrat.

9.2 Pendant la durée du contract

L'organisation doit s'assurer que les salariés et les contractants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités.

9.2.1 Responsabilités de la direction

L'organisation doit s'assurer que les salariés et les contractants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités.

Il convient que la direction demande à tous les salariés et contractants d'appliquer les règles de sécurité conformément aux politiques et aux procédures en vigueur dans l'organisation.

Il convient qu'il relève des responsabilités de la direction de s'assurer que les salariés et les contractants :

a) sont correctement informés sur leurs fonctions et leurs responsabilités en matière de sécurité de l'information avant de se voir accorder l'accès à l'information confidentielle ou aux systèmes d'information ;

b) prennent connaissance des lignes directrices spécifiant les attentes en matière de sécurité de l'information qu'impliquent leurs fonctions au sein de l'organisation ;

c) sont incités à appliquer les politiques de sécurité de l'information de l'organisation ;

d) acquièrent un niveau de sensibilisation à la sécurité en adéquation avec leurs fonctions et leurs responsabilités au sein de l'organisation ;

e) respectent les conditions de leur embauche, ce qui intègre notamment la politique de sécurité de l'information de l'organisation et les méthodes de travail appropriées ;

Il convient que la direction manifeste son soutien aux politiques, aux procédures et aux mesures relatives à la sécurité de l'information et serve de modèle.

9.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information

L'ensemble des salariés de l'organisation et, le cas échéant, les contractants doivent suivre un apprentissage et des formations de sensibilisation adaptés et qu'ils doivent recevoir régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions.

Il convient que le programme de sensibilisation à la sécurité de l'information vise à sensibiliser le personnel et, le cas échéant, les contractants aux responsabilités qui leur incombent en matière de sécurité de l'information et aux moyens dont ils disposent pour s'acquitter de ces responsabilités.

Il convient d'établir un programme de sensibilisation à la sécurité de l'information qui soit cohérent avec les politiques de l'organisation relatives à la sécurité de l'information et avec les procédures associées, et qui tient compte des informations à protéger et des mesures mises en œuvre pour assurer cette protection.

Il convient que le programme de sensibilisation comporte un certain nombre d'activités de sensibilisation telles que des campagnes et la diffusion de livrets ou de bulletins d'information.

Il convient que le programme de sensibilisation soit planifié en tenant compte des fonctions des salariés au sein de l'organisation et, le cas échéant, de ce que l'organisation attend des contractants.

Il convient que les activités prévues dans le programme de sensibilisation soient programmées dans le temps, de préférence à échéances régulières, de manière à se répéter afin d'inclure les nouveaux salariés et contractants.

Il convient également que le programme de sensibilisation soit mis à jour régulièrement pour rester cohérent avec les politiques et les procédures de l'organisation, et qu'il s'appuie sur les enseignements tirés des incidents de sécurité.

Il convient que la formation de sensibilisation soit assurée comme spécifié par le programme de sensibilisation à la sécurité de l'information de l'organisation. La formation de sensibilisation peut être délivrée de différentes manières, par exemple en salle de cours, par apprentissage à distance, apprentissage en ligne, auto-apprentissage, etc.

9.2.3 Processus disciplinaire

Chaque organisation doit mettre en place un processus disciplinaire formel et connu de tous pour prendre des mesures à l'encontre des salariés ayant enfreint les règles liées à la sécurité de l'information.

Il convient de ne pas déclencher le processus disciplinaire avant d'avoir d'abord vérifié l'existence de l'infraction.

Il convient que le processus disciplinaire formel garantisse un traitement correct et juste des salariés suspectés d'avoir enfreint les règles de sécurité.

Il convient que le processus disciplinaire formel fournisse une réponse graduée prenant en considération des facteurs tels que la nature et la gravité de la violation, ainsi que son impact sur l'activité de l'organisation.

Il convient également de préciser s'il s'agit d'une première infraction ou d'une récidive, si le contre venant a reçu la formation adéquate, et de tenir compte des dispositions légales applicables, des contrats commerciaux et de tout autre facteur nécessaire.

Il convient également que le processus disciplinaire constitue un élément dissuasif empêchant les salariés d'enfreindre les politiques et procédures relatives à la sécurité de l'organisation, ainsi que toute autre règle de sécurité. Les violations délibérées des règles peuvent nécessiter des actions immédiates.

9.3 Rupture, terme ou modification du contrat de travail

L'organisation doit protéger ses intérêts dans le cadre du processus de modification, de rupture ou de terme d'un contrat de travail.

9.3.1 Achèvement ou modification des responsabilités associées au contrat de travail

L'organisation doit définir les responsabilités et les missions liées à la sécurité de l'information qui restent valables à l'issue de la rupture, du terme ou de la modification du contrat de travail, d'en informer le salarié ou le contractant et de veiller à leur application.

Il convient que les responsabilités liées aux fins de contrats incluent les exigences permanentes liées à la sécurité et les responsabilités légales ainsi que, le cas échéant, les responsabilités figurant dans tout engagement de confidentialité et dans les conditions d'embauche se poursuivant pendant une période de temps définie après le départ du salarié ou du contractant de l'organisation.

Il convient que les responsabilités et les missions encore valables au-delà de la rupture ou du terme du contrat de travail figurent dans les conditions du contrat du salarié ou du contractant.

Il convient de gérer les changements de poste ou de responsabilités comme un terme mis au poste ou aux responsabilités en question, et de déterminer les nouvelles responsabilités ou les nouvelles fonctions.

10. Gestion des actifs informationnels (D6)

10.1 Responsabilités relatives aux actifs

L'organisation doit identifier ses actifs informationnels et définir les responsabilités appropriées en matière de protection.

10.1.1 Inventaire des actifs

L'organisation doit identifier les actifs associés à l'information et aux moyens de traitement de l'information et de dresser et tenir à jour un inventaire de ces actifs.

A ce titre, elle identifie les actifs informationnels impliqués dans le cycle de vie de l'information et documente leur importance. Le cycle de vie de l'information doit englober sa création, son traitement, son stockage, sa transmission, sa suppression et sa destruction. La documentation doit être tenue à jour dans des inventaires dédiés ou déjà en place, selon le cas. L'inventaire des actifs doit être précis, à jour, cohérent et en adéquation avec les autres inventaires. Il convient d'attribuer à chaque actif identifié un propriétaire et d'identifier la classification.

10.1.2 Propriété des actifs

Il convient que les actifs figurant à l'inventaire aient un propriétaire.
Le propriétaire des actifs doit être désigné dès leur création, leur acquisition ou lorsqu'ils sont transférés à l'organisation. Il convient que le propriétaire de l'actif soit responsable de la bonne gestion de cet actif tout au long de son cycle de vie. Il convient que le propriétaire de l'actif :

a) s'assure que les actifs sont inventoriés;

b) s'assure que les actifs sont correctement classés et protégés;

c) définisse et revoit périodiquement les classifications et les restrictions d'accès aux actifs importants, en tenant compte des politiques de contrôle d'accès applicables;

d) s'assure que les manipulations de suppression ou de destruction des actifs sont réalisées correctement.

10.1.3 Utilisation correcte des actifs

Chaque organisation doit identifier, documenter et mettre en œuvre des règles d'utilisation correcte de l'information, des actifs associés à l'information et des moyens de traitement de l'information.

Il convient que les salariés et les utilisateurs tiers utilisant ou ayant accès aux actifs de l'organisation soient conscients des exigences de sécurité de l'information liées aux actifs de l'organisation associés à l'information, aux moyens de traitement de l'information et aux ressources. Il convient qu'ils soient responsables de l'utilisation qu'ils font de toute ressource de traitement de l'information et de toute utilisation effectuée sous leur responsabilité.

10.1.4 Restitution des actifs

Tous les salariés et utilisateurs tiers doivent restituer la totalité des actifs de l'organisation qu'ils ont en leur possession au terme de la période d'emploi, du contrat ou de l'accord.

Il convient de formaliser le processus de fin de mission ou d'emploi pour qu'il inclue la restitution de tous les actifs physiques et électroniques créés, appartenant à l'organisation ou lui ayant été confiés. Si un salarié ou un utilisateur tiers achète du matériel à l'organisation ou utilise son propre matériel.

Il convient de suivre des procédures pour garantir que toutes les informations pertinentes sont transférées à l'organisation et correctement effacées du matériel. Si un salarié ou un utilisateur tiers détient des connaissances importantes pour les activités en cours, il convient que cette information soit documentée et transférée à l'organisation.

Lors de la période de préavis, il convient que l'organisation vérifie que les salariés et les contractants quittant l'organisation ne procèdent pas à des copies non autorisées d'information utile (par exemple en matière de propriété intellectuelle).

10.2 Classification de l'information

L'organisation doit s'assurer que l'information bénéficie d'un niveau de protection approprié conforme à son importance.

10.2.1 Classification des informations

Chaque organisation doit classer les informations en termes de valeur, d'exigences légales, de sensibilité ou de leur caractère critique pour l'entreprise.

Il convient que la classification de l'information et les mesures de protection associées tiennent compte des besoins de l'organisation en matière de partage ou de limitation de l'information, ainsi que des exigences légales.

Il convient que les propriétaires des actifs liés à l'information soient responsables de leur classification.

Il convient que le plan de classification comporte des conventions de classification et des critères de revue de cette classification dans le temps. Il convient que le niveau de protection du plan de classification soit apprécié en analysant la confidentialité, l'intégrité, la disponibilité et toute autre exigence relative à l'information à évaluer.

Il convient que le plan de classification soit cohérent avec la politique de contrôle d'accès.

Il convient d'attribuer à chaque niveau un nom significatif et logique dans le contexte de l'application du plan de classification.

Il convient que le plan soit identique pour toute l'organisation, de sorte que tout le monde puisse classer l'information et les actifs associés de la même façon, comprenne les exigences de protection de la même manière et applique la protection appropriée.

Il convient que la classification soit intégrée aux processus de l'organisation et qu'elle soit cohérente et identique pour toute l'organisation.

Il convient que les résultats de la classification traduisent la valeur des actifs en fonction de leur sensibilité et de leur caractère critique pour l'organisation, par exemple en termes de confidentialité, d'intégrité et de disponibilité.

Il convient que les résultats de la classification soient mis à jour en fonction des évolutions de leur valeur, de leur sensibilité et de leur caractère critique tout au long de leur cycle de vie.

10.2.2 Marquage des informations

L'organisation doit élaborer et mettre en œuvre un ensemble approprié de procédures pour le marquage de l'information, conformément au plan de classification de l'information adopté par l'organisation.

Les procédures de marquage de l'information doivent s'appliquer à l'information et aux actifs associés présentés sous un format physique ou électronique.

Il convient que le marquage respecte le plan de classification. Il convient que les marques soient facilement reconnaissables. Il convient que les procédures donnent des indications sur l'endroit et la façon dont les marques sont fixées, compte tenu de la manière dont on accède à l'information ou de la façon de manipuler les actifs, en fonction des types de support. Les procédures peuvent définir des cas pour lesquels le marquage n'est pas indispensable, par exemple dans le cas d'information non confidentielle en vue d'alléger la charge de travail.

Il convient que les salariés et les contractants soient sensibilisés aux procédures de marquage.

Il convient que les données délivrées par des systèmes contenant de l'information classée comme sensible ou critique portent des marques appropriées.

10.2.3 Manipulation des actifs

L'organisation doit élaborer et mettre en œuvre des procédures de traitement des actifs, conformément au plan de classification de l'information adopté par l'organisation.

Il convient de rédiger des procédures spécifiant comment manipuler, traiter, stocker et communiquer l'information en fonction de sa classification.

10.3 Manipulation des supports

L'organisation doit empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de l'information de l'organisation stockée sur des supports.

10.3.1 Gestion des supports amovibles

L'organisation doit mettre en œuvre des procédures de gestion des supports amovibles conformément au plan de classification adopté par l'organisation.

10.3.2 Mise au rebut des supports

L'organisation doit procéder à une mise au rebut sécurisée des supports qui ne servent plus, en suivant des procédures formelles.

Il convient que les procédures formelles de mise au rebut sécurisée des supports réduisent au minimum le risque de fuites d'information confidentielle vers des personnes non autorisées. Il convient que les procédures de mise au rebut sécurisée des supports contenant de l'information confidentielle soient proportionnelles à la sensibilité de cette information. Il convient d'envisager les éléments suivants :

a) il convient de stocker les supports contenant de l'information confidentielle et de les mettre au rebut de façon sûre et sécurisée, par exemple par incinération ou déchiquetage, ou d'en effacer les données utilisées dans d'autres applications de l'organisation;

b) il convient de mettre en place des procédures d'identification des éléments pouvant nécessiter une mise au rebut sécurisé;

c) il peut s'avérer plus facile d'organiser la collecte et la mise au rebut sécurisées de l'ensemble des supports, plutôt que de tenter d'isoler les supports sensibles;

d) de nombreuses organisations proposent des services de collecte et d'enlèvement des supports; il convient de sélectionner avec soin le prestataire approprié disposant de mesures de sécurité et d'une expérience suffisantes;

e) il convient de journaliser la mise au rebut des éléments sensibles pour en assurer la traçabilité.

En cas d'accumulation de supports en vue de leur mise au rebut, il convient de prendre en compte l'effet d'agrégation qui peut rendre sensible une grande quantité d'information à l'origine non confidentielle.

10.3.3 Transfert physique des supports

L'organisation doit protéger les supports contenant de l'information contre les accès non autorisés, l'utilisation frauduleuse ou l'altération lors du transport.

L'information peut être vulnérable à un accès non autorisé, à une utilisation frauduleuse ou à une altération pendant le transport physique, par exemple lors de l'envoi de supports par courrier ou par coursier. Cette mesure concerne également les documents papier.

Lorsque les supports contiennent une information confidentielle non cryptée, il convient d'envisager une protection physique supplémentaire.

11. Contrôle d'accès (D7)

11.1 Exigences métier en matière de contrôle d'accès

L'organisation doit limiter l'accès à l'information et aux moyens de traitement de l'information.

11.1.1 Politique de contrôle d'accès

L'organisation doit établir, documenter et revoir une politique du contrôle d'accès sur la base des exigences métier et de sécurité de l'information.

Il convient que les propriétaires des actifs déterminent des règles de contrôle d'accès, des droits d'accès et des restrictions d'accès appropriés aux fonctions spécifiques de l'utilisateur des actifs, avec la quantité de détails et la rigueur des mesures correspondant aux risques associés en matière de sécurité de l'information.

Les contrôles d'accès sont à la fois logiques et physiques et il convient de les envisager conjointement. Il convient que les utilisateurs et les prestataires de services soient clairement informés des exigences de l'organisation auxquelles doivent répondre les contrôles d'accès.

Il convient que la politique tienne compte des exigences suivantes :

a) exigences en matière de sécurité des applications métier;

b) politiques relatives à la diffusion de l'information et aux autorisations, par exemple nécessité de connaître le principe, les niveaux de sécurité de l'information et la classification de l'information;

c) cohérence entre la politique des droits d'accès et la politique de classification de l'information des différents systèmes et réseaux;

d) législation et obligations contractuelles applicables relatives à la limitation de l'accès aux données ou aux services;

e) gestion des droits d'accès dans un environnement décentralisé mis en réseau qui reconnaît tous les types de connexions disponibles;

f) cloisonnement des rôles pour le contrôle d'accès, par exemple la demande d'accès, l'autorisation d'accès et l'administration des accès;

g) exigences en matière d'autorisation formelle des requêtes d'accès;

h) exigences en matière de revue régulière des droits d'accès;

i) annulation de droits d'accès;

j) archivage des enregistrements de tous les événements significatifs relatifs à l'utilisation et à la gestion des identités des utilisateurs et des informations d'authentification secrètes;

k) fonctions avec accès privilégié.

Il convient de faire preuve de prudence lors de la spécification des règles de contrôle d'accès :

a) établir des règles fondées sur le principe suivant: «Tout est généralement interdit sauf autorisation expresse» plutôt que sur la règle, moins fiable, selon laquelle «Tout est généralement autorisé sauf interdiction expresse»;

b) tenir compte des modifications apportées automatiquement aux étiquettes par les moyens de traitement de l'information, et les modifications qui sont à l'appréciation de l'utilisateur;

c) examiner les modifications apportées automatiquement aux droits d'accès de l'utilisateur par le système d'information, et les modifications qui sont décidées par un administrateur;

d) examiner les règles qui nécessitent une approbation spécifique avant toute mise en œuvre, et les règles pour lesquelles aucune autorisation préalable n'est nécessaire.

Il convient que les règles de contrôle d'accès s'appuient sur des procédures formelles et des responsabilités définies.

11.1.2 Accès aux réseaux et aux services en réseau

Les utilisateurs doivent avoir uniquement accès aux réseaux et aux services en réseau pour lesquels ils ont spécifiquement reçu une autorisation.

Il convient de définir une politique relative à l'utilisation des réseaux et des services en réseau. Il convient que cette politique couvre :

a) les réseaux et les services en réseau pour lesquels l'accès a été accordé;

b) les procédures d'autorisation désignant les personnes autorisées à accéder à tels ou tels réseau et service en réseau;

c) les procédures et mesures de gestion destinées à protéger l'accès aux connexions réseau et aux services en réseau;

d) les moyens utilisés pour accéder aux réseaux et aux services en réseau (par exemple réseau privé virtuel ou réseau sans fil);

e) les exigences d'authentification de l'utilisateur pour l'accès à différents services en réseau;

f) la surveillance de l'utilisation faite de ces services en réseau.

Il convient que la politique d'utilisation des services en réseau soit cohérente avec la politique de contrôle d'accès de l'organisation.

11.2 Gestion de l'accès utilisateur

L'organisation doit maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes et services d'information.

11.2.1 Enregistrement et désinscription des utilisateurs

L'organisation doit mettre en œuvre une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à permettre l'attribution de droits d'accès.

Il convient que la procédure de gestion des identifiants utilisateurs inclue :

a) la création d'identifiants utilisateurs uniques permettant de relier les utilisateurs à leurs actions et de les leur imputer; il convient de n'autoriser l'utilisation d'identifiants communs que lorsque les aspects opérationnels et liés à l'activité de l'organisation l'exigent; il convient que ces identifiants communs soient approuvés et documentés;

b) la suppression ou le blocage immédiat des identifiants des utilisateurs qui ont quitté l'organisation;

c) la détection périodique des identifiants utilisateurs redondants, suivie de leur suppression ou de leur blocage;

d) l'assurance que des identifiants utilisateurs redondants ne sont pas attribués à d'autres utilisateurs.

11.2.2 Maîtrise de la gestion des accès utilisateur

L'organisation doit mettre en œuvre un processus formel de maîtrise de la gestion des accès utilisateur pour attribuer ou révoquer des droits d'accès à tous les types d'utilisateurs de tous les systèmes et de tous les services d'information.

Il convient que le processus de maîtrise de la gestion des attributions ou des révocations des droits d'accès accordés à des identifiants utilisateurs inclue :

a) l'obtention de l'autorisation d'utilisation du système ou du service d'information de la part du propriétaire de ce système ou de ce service d'information; il peut également s'avérer approprié de séparer l'approbation des droits d'accès de leur gestion;

b) la vérification que le niveau d'accès accordé est adapté aux politiques d'accès et qu'il est cohérent avec les autres exigences telles que la séparation des tâches;

c) l'assurance que les droits d'accès ne sont pas activés (par exemple, par les prestataires de services) tant que le processus d'autorisation n'est pas terminé;

d) la tenue à jour d'un enregistrement centralisé de tous les droits d'accès accordés aux identifiants utilisateurs pour leur permettre d'utiliser des systèmes et des services;

e) l'adaptation des droits d'accès des utilisateurs qui ont changé de fonction ou de poste et la suppression ou le blocage immédiat des droits d'accès des utilisateurs qui ont quitté l'organisation;

f) une revue régulière des droits d'accès avec les propriétaires des systèmes ou des services d'information.

Il convient d'envisager d'établir des rôles d'accès utilisateurs en fonction des exigences métier, qui regroupent des droits d'accès dans des profils d'utilisateurs types.

Il convient d'envisager d'inclure des clauses dans les contrats de travail et les contrats de service stipulant les sanctions encourues en cas de tentative d'accès non autorisé par un salarié ou un contractant.

11.2.3 Gestion des privilèges d'accès

L'organisation doit restreindre et contrôler l'attribution et l'utilisation des privilèges d'accès.

Il convient de contrôler l'attribution des privilèges d'accès par le biais d'une procédure formelle d'autorisation, conformément à la politique de contrôle des accès applicable. Il convient d'envisager les étapes suivantes :

a) il convient d'identifier les privilèges d'accès associés à chaque système ou chaque processus, par exemple le système d'exploitation, le système de gestion de la base de données et chaque application, ainsi que les utilisateurs auxquels il est nécessaire d'attribuer ces privilèges;

b) il convient d'attribuer des privilèges d'accès aux utilisateurs en suivant les impératifs liés à leur activité et au cas par cas, conformément à la politique de contrôle d'accès, c'est-à-dire en fonction de l'exigence minimale requise par leur rôle fonctionnel;

c) il convient de tenir à jour une procédure d'autorisation et un enregistrement de tous les privilèges qui ont été attribués. Il convient de ne pas attribuer de privilèges d'accès tant que le processus d'autorisation n'est pas terminé ;

d) il convient de définir les exigences en matière d'expiration des privilèges d'accès;

e) il convient d'associer les privilèges d'accès à un identifiant utilisateur différent de l'identifiant utilisateur employé pour les tâches ordinaires. Il convient que les tâches ordinaires des utilisateurs ne soient pas réalisées à l'aide d'un identifiant doté de privilèges ;

f) il convient de procéder à une revue régulière des compétences des utilisateurs bénéficiant de privilèges d'accès afin de vérifier qu'elles sont conformes à leurs tâches;

g) il convient d'établir et de tenir à jour des procédures spécifiques afin d'éviter l'utilisation non autorisée d'identifiants génériques d'administration, selon les capacités de configuration du système;

h) en ce qui concerne les identifiants génériques d'administration, il convient de préserver la confidentialité des informations secrètes d'authentification lorsque ces identifiants sont partagés (par exemple, changer fréquemment de mots de passe et dès que possible lorsqu'un utilisateur privilégié quitte l'organisation ou change de fonction, les communiquer à l'aide de mécanismes appropriés aux utilisateurs privilégiés).

11.2.4 Gestion des informations secrètes d'authentification des utilisateurs

Il convient que l'attribution des informations secrètes d'authentification soit réalisée dans le cadre d'un processus de gestion formel.

Il convient que ce processus prévoie les exigences suivantes :

a) il convient d'exiger des utilisateurs qu'ils signent une déclaration par laquelle ils s'engagent à ne pas divulguer leurs informations secrètes d'authentification personnelle et à

communiquer leurs informations secrètes d'authentification de groupe (à savoir les informations partagées) aux seuls utilisateurs du groupe; il est possible d'inclure cette déclaration signée dans le contrat de travail;

b) lorsqu'il est demandé aux utilisateurs de définir eux-mêmes leurs informations secrètes d'authentification, ilconvientdeleurfournirauprealabledesinformationssecretesd'authentification sécurisées et temporaires qu'ils doivent changer dès la première utilisation;

c) il convient d'établir des procédures permettant de vérifier l'identité d'un utilisateur avant d'attribuer des nouvelles informations secrètes d'authentification ou des informations secrètes d'authentification temporaires;

d) il convient que la communication des informations secrètes d'authentification temporaires soit sécurisée; il convient d'éviter de les envoyer par courrier électronique non protégé (texte en clair) ou de la transmettre par l'intermédiaire de tiers;

e) il convient que les informations secrètes d'authentification temporaires soient uniques pour chaque personne et qu'il ne soit pas possible, par déduction, de les deviner;

f) il convient que les utilisateurs accusent réception des informations secrètes d'authentification;

g) il convient que les informations secrètes d'authentification par défaut définies par les constructeurs et éditeurs soient modifiées après installation des systèmes ou logiciels.

11.2.5 Revue des droits d'accès utilisateur

Il convient que les propriétaires d'actifs revoient les droits d'accès des utilisateurs à intervalles réguliers.

Il convient que la revue des droits d'accès utilisateurs tienne compte de ce qui suit:

a) il convient de revoir les droits d'accès utilisateurs à intervalles réguliers et après tout changement tel qu'une promotion, une rétrogradation ou le départ d'un salarié ;

b) il convient de revoir et de réattribuer les droits d'accès utilisateurs en cas de changement de fonction au sein de l'organisation;

c) il convient de revoir, à des intervalles de temps plus fréquents, les autorisations liées à des droits d'accès privilégiés;

d) il convient de vérifier l'attribution de privilèges à intervalles réguliers pour s'assurer qu'aucun privilège non autorisé n'a été accordé;

e) il convient de journaliser les modifications apportées aux comptes dotés de privilèges aux fins de revue périodique.

11.2.6 Suppression ou adaptation des droits d'accès

Les droits d'accès de l'ensemble des salariés et utilisateurs tiers à l'information et aux moyens de traitement de l'information doivent être supprimés à la fin de leur période d'emploi, ou adapter en cas de modification du contrat ou de l'accord.

Il convient qu'à l'achèvement de la période d'emploi, les droits d'accès d'une personne à l'information et aux actifs associés aux services et aux moyens de traitement de l'information soient supprimés ou suspendus. Cela permettra de déterminer s'il est nécessaire de supprimer les droits d'accès.

Il convient que les modifications apportées à un contrat entraînent le retrait de tous les droits d'accès n'ayant pas été approuvés dans le cadre du nouveau contrat.

Il convient que les droits d'accès à supprimer ou à adapter concernent les accès physiques et logiques. La suppression ou l'adaptation peuvent être réalisées par suppression, révocation ou remplacement des clés, des cartes d'identification, des moyens de traitement de l'information ou des abonnements.

Il convient que toute documentation recensant les droits d'accès des salariés et des contractants rende compte de leur suppression ou de leur adaptation. Si un salarié ou un utilisateur tiers quittant l'organisation connaît les mots de passe d'identifiants utilisateurs toujours actifs, il convient de changer ces mots de passe à l'achèvement de la période d'emploi ou dès la modification du contrat ou de l'accord.

Il convient que les droits d'accès à l'information et aux actifs associés aux moyens de traitement de l'information soient restreints ou supprimés avant la fin de la période d'emploi ou la modification du contrat en fonction de l'évaluation des facteurs de risque suivants:

a) s'agit-il d'une résiliation ou d'une modification du contrat intervenue à l'initiative du salarié, de l'utilisateur tiers ou de la direction, et pour quel motif?

b) quelles sont les responsabilités du salarié, de l'utilisateur tiers ou autre utilisateur?

c) quelle est la valeur des actifs accessibles?

11.3 Responsabilités des utilisateurs

L'organisation doit rendre les utilisateurs responsables de la protection de leurs informations d'authentification.

11.3.1 Utilisation d'informations secrètes d'authentification

L'organisation doit exiger des utilisateurs des informations secrètes d'authentification qu'ils appliquent les pratiques de l'organisation en la matière.

Il convient de recommander aux utilisateurs de prendre les précautions suivantes:

a) préserver la confidentialité de l'authentification secrète, en s'assurant de ne pas la divulguer à des tiers, ni même à leurs supérieurs;

b) ne pas conserver d'enregistrement des informations secrètes d'authentification (par exemple sur support papier, fichier électronique ou équipement portable), sauf si le support de stockage est sûr et si la méthode de stockage a été approuvée (par exemple, un coffre-fort pour mots de passe);

c) changer les informations secrètes d'authentification à chaque fois que quelque chose indique qu'elles pourraient être compromises;

d) en cas d'utilisation de mots de passe comme information secrète d'authentification, choisir des mots de passe de qualité, d'une longueur minimale suffisante, qui:
   1) sont faciles à retenir;
   2) ne peuvent pas être rattachés à une information personnelle facile à deviner ou à obtenir, par exemple: noms, numéros de téléphone, dates d'anniversaire, etc.;
   3) sont invulnérables à une attaque par dictionnaire (c'est-à-dire un mot de passe uniquement composé de mots figurant dans des dictionnaires); et
   4) ne sont pas composés de caractères consécutifs identiques, totalement numériques ou totalement alphabétiques;
   5) doivent être changés à la première connexion s'ils sont temporaires;

e) ne pas partager les informations secrètes d'authentification d'une personne;

f) assurer une protection correcte des mots de passe lorsqu'ils sont utilisés comme information secrète d'authentification dans des procédures de connexion automatique et qu'ils sont stockés;

g) ne pas utiliser les mêmes informations secrètes d'authentification pour les activités professionnelles et extra-professionnelles.

11.4 Contrôle de l'accès au système et aux applications

L'organisation doit veiller à empêcher les accès non autorisés aux systèmes et aux applications.

11.4.1 Restriction d'accès à l'information

L'organisation doit restreindre l'accès à l'information et aux fonctions d'application système conformément à la politique de contrôle d'accès.

Il convient que les restrictions d'accès soient fonction des exigences de chaque application métier et conformes à la politique de contrôle d'accès définie.

Pour soutenir les exigences relatives aux restrictions d'accès, il convient d'envisager de :

a) créer des menus permettant de contrôler l'accès aux fonctions d'application système;

b) contrôler les données auxquelles peut accéder un utilisateur donné;

c) contrôler les droits d'accès des utilisateurs, par exemple: lecture, écriture, suppression et exécution;

d) contrôler les droits d'accès aux autres applications;

e) limiter les informations contenues dans les éléments de sortie: fournir des contrôles d'accès physiques ou logiques permettant d'isoler les applications, les données des applications ou les systèmes sensibles.

f) fournir des contrôles d'accès physiques ou logiques permettant d'isoler les applications, les données des applications ou les systèmes sensibles.

11.4.2 Sécuriser les procédures de connexion

Lorsque la politique de contrôle d'accès l'exige, il convient que l'accès aux systèmes et aux applications soit contrôlé par une procédure de connexion sécurisée.

Il convient de choisir une technique d'authentification permettant de vérifier l'identité déclarée par l'utilisateur.

Lorsqu'un niveau élevé d'authentification et d'identification est requis, il convient d'utiliser des méthodes d'authentification autres que l'utilisation de mots de passe : par exemple un procédé cryptographique, une carte à puce, des jetons d'authentification ou des techniques de biométrie.

Il convient que la procédure de connexion à un système ou à une application soit conçue de manière à réduire au minimum les possibilités d'accès non autorisé. Par conséquent, il convient que cette procédure de connexion ne dévoile qu'un minimum d'information sur le système ou l'application, afin d'éviter de faciliter la tâche d'un éventuel utilisateur non autorisé.

Il convient qu'une bonne procédure de connexion :

a) n'affiche pas les identifiants du système ou de l'application tant que le processus de connexion n'est pas terminé;

b) affiche un avertissement précisant que l'accès de l'ordinateur est limité aux seuls utilisateurs autorisés;

c) ne propose pas, pendant la procédure de connexion, de messages d'aide qui pourraient faciliter un accès non autorisé;

d) valide l'information de connexion seulement lorsque toutes les données d'entrée ont été saisies. Si une condition d'erreur survient, il convient que le système n'indique pas quelle partie des données est correcte ou incorrecte ;

e) assure une protection contre les tentatives de connexion par force brute;

f) enregistre les tentatives réussies et avortées;

g) lance une alerte de sécurité en cas de détection d'une brèche possible, réussie ou avortée, dans les contrôles de connexion;

h) affiche les informations suivantes après une connexion réussie:
   1) la date et l'heure de la dernière connexion réussie;
   2) les détails relatifs à toute tentative de connexion avortée depuis la dernière tentative réussie;

i) n'affiche pas le mot de passe qui est entré;

j) ne transmette pas les mots de passe au sein d'un réseau sous la forme d'un texte en clair;

k) mette fin aux sessions inactives au bout d'une période définie d'inactivité, notamment dans les endroits présentant des risques élevés, comme les lieux publics ou à l'extérieur des locaux soumis au management de la sécurité de l'organisation, ou à l'occasion de l'utilisation d'appareils mobiles;

l) restreigne les temps de connexion pour apporter une sécurité supplémentaire aux applications à haut risque et réduire les risques de tentatives d'accès non autorisé.

Il convient d'adapter le niveau d'authentification de l'utilisateur en fonction de la classification de l'information à laquelle il souhaite accéder.

11.4.3 Système de gestion des mots de passe

Il convient que les systèmes qui gèrent les mots de passe soient interactifs et fournissent des mots de passe de qualité.

Il convient qu'un système de gestion des mots de passe :

a) impose l'utilisation d'identifiants et de mots de passe utilisateurs individuels afin de garantir l'imputabilité;

b) autorise l'utilisateur à choisir et à modifier ses mots de passe, et prévoie une procédure de confirmation afin de tenir compte des erreurs de saisie;

c) impose le choix de mots de passe de qualité;

d) impose aux utilisateurs de changer leur mot de passe à la première connexion;

e) impose des changements réguliers de mot de passe au besoin ;

f) tienne à jour un enregistrement des anciens mots de passe et empêche leur réutilisation;

g) n'affiche pas les mots de passe à l'écran lors de leur saisie;

h) stocke les fichiers de mots de passe à d'autres emplacements que les données d'application système;

i) stocke et transmette les mots de passe sous une forme protégée.

11.4.4 Utilisation de programmes utilitaires à privilèges

Il convient de limiter et de contrôler étroitement l'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application.

Il convient de prendre en compte les directives suivantes en matière d'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application :

a) utiliser des procédures d'identification, d'authentification et d'autorisation spécifiques aux programmes utilitaires;

b) séparer les programmes utilitaires des logiciels d'application;

c) limiter l'emploi des programmes utilitaires à un nombre minimal acceptable d'utilisateurs de confiance bénéficiant d'une autorisation;

d) autoriser une utilisation ad hoc des programmes utilitaires;

e) poser des limites à la disponibilité des programmes utilitaires, par exemple limiter la durée d'une autorisation de modification;

f) journaliser toutes les utilisations de programmes utilitaires;

g) définir et documenter les niveaux d'autorisation relatifs aux programmes utilitaires;

h) désinstaller ou désactiver tous les programmes utilitaires inutiles;

i) ne pas mettre de programmes utilitaires à la disposition des utilisateurs ayant accès à des applications relatives à des systèmes pour lesquels la séparation des tâches est requise.

11.4.5 Contrôle d'accès au code source des programmes

Il convient de restreindre l'accès au code source des programmes.

Il convient d'exercer un contrôle strict de l'accès au code source des programmes et aux éléments associés (tels que les exigences de conception, les spécifications, les programmes de vérification et de validation), afin d'empêcher l'introduction d'une fonctionnalité non autorisée et d'éviter toute modification involontaire, ainsi que préserver la confidentialité en matière de propriété intellectuelle de valeur.

En ce qui concerne le code source des programmes, ce contrôle peut prendre la forme d'un stockage centralisé du code, de préférence dans les bibliothèques de programmes sources.

Il convient de prendre en compte les lignes directrices suivantes pour contrôler l'accès aux bibliothèques de programmes sources en vue de réduire les risques d'altération des programmes informatiques :

a) lorsque cela est possible, il convient que les bibliothèques de programmes sources ne soient pas stockées sur les systèmes en exploitation;

b) il convient que le code source du programme et les bibliothèques de programmes sources soient gérés conformément aux procédures établies;

c) il convient que le personnel chargé de l'assistance technique ne dispose pas d'un accès illimité aux bibliothèques de programmes sources;

d) il convient que la mise à jour des bibliothèques de programmes sources et des éléments associés, ainsi que la délivrance des programmes sources aux programmeurs ne soient réalisées qu'après attribution d'une autorisation appropriée;

e) il convient de stocker les listings de programmes dans un environnement sécurisé;

f) il convient de tenir à jour un journal d'audit de tous les accès aux bibliothèques de programmes sources;

g) il convient de soumettre les processus de maintenance et de copie des bibliothèques de programmes sources à des procédures strictes de contrôle des modifications.

Si le code source du programme est destiné à être publié, il convient d'envisager des mesures supplémentaires pour garantir son intégrité (par exemple, une signature électronique).

12. Cryptographie (D8)

L'organisation doit garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.

12.1.1 Politique d'utilisation des mesures cryptographiques

L'organisation doit élaborer et de mettre en œuvre une politique d'utilisation de mesures cryptographiques en vue de protéger l'information.

Lors de l'élaboration d'une politique cryptographique, il convient de prendre en compte les points suivants :

a) l'approche de la direction en ce qui concerne l'utilisation de mesures cryptographiques au sein de l'organisation, y compris les principes généraux de protection en fonction desquels il convient que l'information liée à l'activité de l'organisation soit protégée ;

b) sur la base d'une appréciation du risque, il convient d'identifier le niveau de protection requis en tenant compte du type, de la puissance et de la qualité de l'algorithme de chiffrement requis;

c) l'utilisation d'une technique de chiffrement, en vue de protéger les informations transportées au moyen d'un support sur des appareils amovibles ou mobiles, ou acheminées par des voies d'intercommunication;

d) l'approche de gestion des clés, notamment les méthodes à utiliser pour protéger les clés de chiffrement et récupérer des informations chiffrées en cas de perte, de compromission ou d'endommagement des clés ;

e) les rôles et les responsabilités, par exemple qui est responsable:

   1) de la mise en œuvre de la politique;

   2) de la gestion des clés, notamment la génération des clés;

f) les normes à adopter pour une mise en œuvre efficace dans l'ensemble de l'organisation (quelle solution pour quel processus métier?);

g) l'incidence du chiffrement de l'information dans le cas des mesures reposant sur l'analyse de contenu (par exemple, la détection de logiciels malveillants).

Lors de la mise en œuvre de la politique cryptographique, l'organisation doit tenir compte de la réglementation et des restrictions en Côte d'Ivoire et des recommandations de l'ARTCI pouvant s'appliquer aux techniques cryptographiques.

Il convient que la décision d'utiliser une solution cryptographique s'inscrive dans le cadre d'un processus plus large d'appréciation du risque et de sélection des mesures. Cette appréciation peut donc être utilisée pour déterminer la pertinence d'une mesure cryptographique, le type de mesure qu'il convient d'appliquer, dans quel but et pour quel processus métier.

Il convient de consulter un spécialiste pour sélectionner les mesures cryptographiques appropriées permettant de répondre aux objectifs de la politique de sécurité de l'information.

12.1.2 Gestion des clés et des certificats électroniques

L'organisation doit élaborer et de mettre en œuvre tout au long de leur cycle de vie une politique sur l'utilisation, la protection et la durée de vie des clés et des certificats cryptographiques.

Il convient que la politique comporte des exigences de gestion des clés cryptographiques couvrant l'ensemble de leur cycle de vie: génération, stockage, archivage, extraction, attribution, retrait et destruction des clés.

Il convient de sélectionner les algorithmes de chiffrement, la longueur des clés et les pratiques d'utilisation conformément aux bonnes pratiques. Une gestion appropriée des clés exige des processus sécurisés de génération, de stockage, d'archivage, d'extraction, d'attribution, de retrait et de destruction des clés cryptographiques.

Il convient de protéger toutes les clés cryptographiques contre tout risque de modification ou de perte. En outre, il est nécessaire de protéger les clés secrètes et privées contre toute utilisation, ainsi que contre toute divulgation non autorisée. Il convient de prévoir une protection physique du matériel utilisé pour générer, stocker et archiver les clés.

Il convient que le système de gestion des clés repose sur une série convenue de normes, de procédures et de méthodes sécurisées en vue de:

a) générer des clés pour divers systèmes cryptographiques et diverses applications;

b) générer et obtenir des certificats de clés publiques;

c) attribuer les clés aux utilisateurs prévus et leur indiquer le mode d'activation à la réception des clés;

d) stocker les clés, et notamment définir comment les utilisateurs autorisés peuvent accéder aux clés;

e) mettre à jour ou remplacer les clés, en prévoyant des règles portant sur les moments auxquels il convient de changer les clés et la façon de procéder;

f) traiter les clés compromises;

g) révoquer les clés, définir notamment le mode de retrait ou de désactivation des clés, par exemple lorsque les clés sont compromises ou lorsqu'un utilisateur quitte l'organisation (dans ce cas, il convient également d'archiver les clés);

h) récupérer les clés perdues ou altérées;

i) sauvegarder ou archiver les clés;

j) détruire les clés;

k) journaliser et auditer les activités liées à la gestion des clés.

Afin de réduire la probabilité d'utilisation abusive des clefs, il convient de fixer des dates d'activation et de désactivation, de sorte que les clés ne puissent être utilisées que pendant la période de temps définie dans la politique de gestion des clés correspondante.

Outre la gestion sécurisée des clés secrètes et privées, il convient de tenir compte de l'authenticité des clés publiques. Ce processus d'authentification peut être mis en œuvre à l'aide de certificats de clés publiques généralement délivrés par une autorité de certification. Il convient que cette dernière soit une organisation reconnue disposant de mesures et de procédures appropriées garantissant le degré de fiabilité requis.

13. Sécurité physique et environnementale (D9)

12.1 Zones sécurisées

L'organisation doit veiller à empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information, les Datacenters et les moyens de traitement de l'information.

12.1.1 Périmètre de sécurité physique

L'organisation doit définir des périmètres de sécurité servant à protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information.

Le cas échéant, il convient d'envisager et de mettre en œuvre les directives suivantes concernant les périmètres de sécurité physique :

a) il convient de définir des périmètres de sécurité et il convient que l'emplacement et le niveau de résistance de chacun des périmètres soient fonction des exigences relatives à la sécurité des actifs situés à l'intérieur et des conclusions de l'appréciation du risque;

b) il convient que le périmètre d'un bâtiment ou d'un site abritant des moyens de traitement de l'information soit physiquement solide (il convient que le périmètre ou les zones ne présentent aucune faille susceptible de faciliter une intrusion). Il convient que le toit, les murs extérieurs et le sol du site soient construits de manière solide et que les portes extérieures soient toutes convenablement protégées contre les accès non autorisés par des mécanismes de contrôle, par exemple des barres, des alarmes, des verrous. Il convient également de verrouiller les portes et les fenêtres non gardées, et d'envisager une protection extérieure pour les fenêtres, particulièrement celles du rez-de-chaussée ;

c) il convient de placer du personnel à l'accueil ou des moyens de contrôle d'accès physique au site ou au bâtiment. Il convient de limiter l'accès aux sites et aux bâtiments aux seules personnes autorisées ;

d) s'il y a lieu, il convient d'ériger des barrières physiques pour empêcher l'accès physique non autorisé et la contamination de l'environnement;

e) il convient d'équiper d'une alarme l'ensemble des portes-coupe-feu du périmètre de sécurité, de surveiller ces portes et de les tester en même temps que les murs, pour atteindre le niveau de résistance requis conformément aux normes régionales, nationales et internationales appropriées. Il convient qu'elles fonctionnent conformément au code local de prévention des incendies et de manière infaillible ;

f) il convient d'installer des systèmes de détection d'intrus adaptés, conformes aux normes nationales, régionales et internationales, et de les tester régulièrement pour s'assurer qu'ils englobent l'ensemble des portes extérieures et des fenêtres accessibles. Il convient que les alarmes des zones inoccupées soient activées en permanence. Il convient également de couvrir les autres zones, comme la salle informatique ou la salle des télécommunications ;

g) il convient de séparer physiquement les moyens de traitement de l'information gérés par l'organisation de ceux gérés par des tiers.

12.1.2 Contrôle physique des accès

L'organisation doit protéger les zones sécurisées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis.

Il convient de tenir compte des directives suivantes :

a) il convient de consigner la date et l'heure d'arrivée et de départ des visiteurs et il convient que tous les visiteurs soient encadrés, sauf si leur accès a déjà été autorisé. Il convient de leur accorder l'accès uniquement à des fins précises ayant fait l'objet d'une autorisation et de leur remettre les instructions relatives aux exigences de sécurité de la zone et aux procédures d'urgence associées ;

b) il convient de restreindre l'accès aux zones de traitement ou de stockage de l'information confidentielle uniquement aux personnes autorisées en mettant en œuvre des contrôles d'accès appropriés, par exemple un système d'authentification à deux facteurs, tels qu'une carte d'accès et un code PIN secret ;

c) il convient de conserver de manière sécurisée et de contrôler régulièrement un journal physique ou

un système de traçabilité électronique de tous les accès ;

d) il convient d'exiger de l'ensemble des salariés, des contractants et des tiers le port d'un moyen d'identification visible. Il convient qu'ils informent immédiatement le personnel de sécurité s'ils rencontrent des visiteurs non accompagnés ou quiconque ne portant pas d'identification visible ;

e) il convient d'accorder au personnel d'une organisation tiers chargé de l'assistance technique un accès limité aux zones sécurisées ou aux moyens de traitement de l'information confidentielle et uniquement en fonction des nécessités. Il convient que cet accès fasse l'objet d'une autorisation et d'une surveillance ;

f) f) il convient de revoir et de mettre à jour régulièrement les droits d'accès aux zones sécurisées et de les révoquer au besoin.

12.1.3 Sécurisation des bureaux, des salles et des équipements

Il convient de concevoir et d'appliquer des mesures de sécurité physique aux bureaux, aux salles et aux équipements.

Il convient de prendre en compte les directives suivantes sur la sécurisation des bureaux, des salles et des équipements :

a) pour les équipements-clés, il convient de choisir un emplacement non accessible au public ;

b) dans la mesure du possible, il convient que les bâtiments soient discrets et donnent le minimum d'indications sur leur finalité, sans signe manifeste, extérieur ou intérieur, qui permette d'identifier la présence d'activités de traitement de l'information ;

c) il convient que les équipements soient configurés de manière à empêcher que l'information confidentielle ou les activités soient visibles et audibles de l'extérieur. Si nécessaire, il convient d'envisager la mise en place d'un bouclier électromagnétique ;

d) il convient que les répertoires et annuaires téléphoniques internes identifiant l'emplacement des moyens de traitement de l'information confidentielle ne soient pas accessibles sans autorisation.

12.1.4 Protection contre les menaces extérieures et environnementales

Chaque organisation doit concevoir et appliquer des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents.

Il convient de solliciter les conseils de spécialistes sur la façon d'éviter les dommages causés par les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et autres formes de catastrophes naturelles ou d'origine humaine.

12.1.5 Travail dans les zones sécurisées

Il convient de concevoir et d'appliquer des procédures pour le travail en zone sécurisée.

Il convient de tenir compte des directives suivantes :

a) il convient que le personnel soit informé de l'existence de zones sécurisées ou des activités qui s'y pratiquent, sur la seule base du besoin d'en connaître ;

b) il convient d'éviter le travail non supervisé/encadré en zone sécurisée, tant pour des raisons de sécurité personnelle que pour prévenir toute possibilité d'acte malveillant ;

c) il convient de verrouiller physiquement et de contrôler périodiquement les zones sécurisées inoccupées ;

d) il convient d'interdire tout équipement photographique, vidéo, audio ou autres dispositifs d'enregistrement, tels que les appareils photos intégrés à des appareils mobiles, sauf autorisation.

12.1.6 Zones de livraison et de chargement

Il convient de contrôler les points d'accès tels que les zones de livraison et de chargement et les autres points par lesquels des personnes non autorisées peuvent pénétrer dans les locaux et, si possible, de les isoler des moyens de traitement de l'information, de façon à éviter les accès non autorisés.

12.2 Matériels

L'organisation doit empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisation.

12.2.1 Emplacement et protection du matériel

L'organisation doit déterminer l'emplacement du matériel et de le protéger de manière à réduire les risques liés à des menaces et dangers environnementaux et les possibilités d'accès non autorisé.

Il convient de prendre en compte les directives suivantes pour protéger le matériel :

a) il convient de déterminer un emplacement pour le matériel permettant de réduire au minimum les accès inutiles aux zones de travail;

b) il convient de positionner avec soin les moyens de traitement de l'information manipulant des données sensibles, en vue de réduire le risque que cette information puisse être vue par des personnes non autorisées;

c) il convient de sécuriser les moyens de stockage contre tout accès non autorisé;

d) il convient de protéger les éléments nécessitant une protection particulière pour abaisser le niveau général de protection requis;

e) il convient d'adopter des mesures visant à réduire au minimum les risques de menaces physiques et environnementales potentielles, comme le vol, l'incendie, les explosions, la fumée, les fuites d'eau (ou une rupture de l'alimentation en eau), la poussière, les vibrations, les effets engendrés par les produits chimiques, les interférences sur le secteur électrique, les interférences sur les lignes de télécommunication, les rayonnements électromagnétiques et le vandalisme;

f) il convient de fixer des directives sur le fait de manger, boire et fumer à proximité des moyens de traitement de l'information;

g) il convient de surveiller les conditions ambiantes, telles que la température et l'humidité, qui pourraient nuire au fonctionnement des moyens de traitement de l'information;

h) il convient d'équiper l'ensemble des bâtiments d'un paratonnerre et il convient d'équiper toutes les lignes électriques et de télécommunication entrantes de parafoudres;

i) il convient d'envisager l'utilisation de méthodes spéciales de protection, telles que les claviers à membrane, pour le matériel utilisé en environnement industriel;

j) il convient de protéger les moyens de traitement de l'information confidentielle pour réduire au minimum les risques de fuites d'information dues aux émissions électromagnétiques.

12.2.2 Services généraux

L'organisation doit protéger le matériel des coupures de courant et autres perturbations dues à une défaillance des services généraux.

Il convient que les services généraux (tels que l'électricité, les télécommunications, l'alimentation en eau, le gaz, l'évacuation des eaux usées, la ventilation et la climatisation):

a) soient conformes aux spécifications du fabricant du matériel et aux exigences légales locales;

b) fassent l'objet d'une évaluation régulière pour vérifier leur capacité à répondre à la croissance de l'organisation et aux interactions avec les autres services généraux:

c) soient examinés et testés de manière régulière pour s'assurer de leur fonctionnement correct:

d) soient équipés, si nécessaire, d'alarmes de détection des dysfonctionnements;

e) disposent, si nécessaire, d'alimentations multiples sur les réseaux physiques d'acheminement.

Il convient que soient prévus des systèmes d'éclairage et de communication d'urgence. Il convient de placer les interrupteurs et les robinets de secours destinés à couper le courant, l'eau, le gaz ou autres services près des sorties de secours et/ou des salles contenant le matériel.

12.2.3 Sécurité du câblage

L'organisation doit protéger les câbles électriques ou de télécommunication transportant des données ou supportant les services d'information contre toute interception, interférence ou dommage.

Il convient de prendre en compte les directives suivantes sur la sécurité du câblage :

a) il convient d'enterrer, dans la mesure du possible, les lignes électriques et les lignes de télécommunication branchées aux moyens de traitement de l'information ou de les soumettre à toute autre forme de protection adéquate;

b) il convient de séparer les câbles électriques des câbles de télécommunication pour éviter toute interférence ;

c) pour les systèmes sensibles ou critiques, les mesures supplémentaires à envisager comprennent:
   1) l'installation d'un conduit de câbles blindé et de chambres ou de boîtes verrouillées aux points d'inspection et aux extrémités;
   2) l'utilisation d'un blindage électromagnétique pour assurer la protection des câbles;
   3) le déclenchement de balayages techniques et d'inspections physiques pour détecter le branchement d'appareils non autorisés sur les câbles;
   4) un accès contrôlé aux panneaux de répartition et aux chambres de câblage.

12.2.4 Maintenance du matériel

L'organisation doit entretenir le matériel correctement pour garantir sa disponibilité permanente et son intégrité.

Il convient de prendre en compte les directives suivantes sur la maintenance du matériel :

a) il convient d'entretenir le matériel selon les spécifications et la périodicité recommandées par le fournisseur;

b) il convient que seul un personnel de maintenance autorisé assure les réparations et l'entretien du matériel;

c) il convient de conserver un dossier de toutes les pannes suspectées ou avérées et de toutes les tâches de maintenance préventives ou correctives;

d) il convient de mettre en œuvre des mesures appropriées lorsque la maintenance d'un matériel est planifiée en prenant en compte le fait qu'elle soit effectuée par du personnel sur site ou extérieur à l'organisation; lorsque cela est nécessaire, il convient que l'information confidentielle contenue dans le matériel soit effacée ou que le personnel de maintenance ait reçu les autorisations suffisantes;

e) il convient de respecter toutes les exigences de maintenance qu'imposent les polices d'assurance;

f) avant de remettre le matériel en service à l'issue de sa maintenance, il convient de l'inspecter pour s'assurer qu'il n'a pas subi d'altérations et qu'il fonctionne correctement.

12.2.5 Sortie des actifs

Il convient de ne pas sortir un matériel, des informations ou des logiciels des locaux de l'organisation sans autorisation préalable.

Il convient de tenir compte des directives suivantes :

a) il convient d'identifier clairement les salariés et les tiers qui ont autorité pour permettre le retrait des actifs du site;

b) il convient de fixer des limites dans le temps pour la sortie des actifs et de vérifier que la date de retour est respectée;

c) le cas échéant, si nécessaire, il convient d'enregistrer la sortie des actifs et leur retour dans les locaux de l'organisation;

d) il convient de documenter l'identité, la fonction et l'affiliation de toute personne qui manipule ou utilise les actifs. Il convient que ces documents accompagnent le retour du matériel, de l'information ou des logiciels.

Des contrôles ponctuels, destinés à détecter une sortie d'actifs non autorisée, peuvent aussi servir à détecter des appareils d'enregistrement non autorisés, des armes, etc., et empêcher qu'ils pénètrent sur le site et en sortent. Il convient d'effectuer ces contrôles ponctuels conformément à la législation et aux règlements applicables. Il convient que les personnes soient informées de la réalisation de contrôles ponctuels et il convient de n'effectuer les vérifications qu'avec une autorisation répondant aux exigences légales et réglementaires.

12.2.6 Sécurité du matériel et des actifs hors des locaux

L'organisation doit appliquer des mesures de sécurité au matériel utilisé hors des locaux de l'organisation en tenant compte des différents risques associés au travail hors site.

Il convient que ce soit la direction qui autorise l'utilisation de matériels de traitement et de stockage de l'information hors des locaux de l'organisation. Cela s'applique aux matériels détenus par l'organisation et aux matériels détenus à titre privé, mais utilisés pour le compte de l'organisation.

Il convient de prendre en compte les directives suivantes concernant la protection du matériel hors site :

a) il convient de ne pas laisser le matériel et les supports de données sortis des locaux sans surveillance dans des lieux publics;

b) il convient d'observer à tout instant les instructions du fabricant visant à protéger le matériel, par exemple celles sur la protection contre les champs électromagnétiques forts;

c) il convient de déterminer des mesures pour les emplacements de travail hors site, comme le travail à domicile, le télétravail et les sites temporaires, en réalisant une appréciation du risque et d'appliquer les mesures nécessaires le cas échéant, par exemple armoires de classement fermant à clé, politique du bureau propre, contrôles d'accès aux ordinateurs et communication sécurisée avec les bureaux de l'organisation;

d) lorsque du matériel circule hors des locaux de l'organisation entre différentes personnes ou entre des tiers, il convient de tenir à jour un journal détaillant la chaîne de traçabilité du matériel, mentionnant au minimum les noms des personnes responsables du matériel, ainsi que les organisations dont elles relèvent.

Il convient de tenir compte des risques, comme l'endommagement, le vol ou la mise sur écoute, qui peuvent varier considérablement en fonction des lieux, pour déterminer les mesures les plus appropriées.

Les matériels de stockage et de traitement de l'information comprennent tous types d'ordinateurs individuels, d'agendas électroniques, de téléphones mobiles, de cartes à puce, le papier ou tout autre moyen détenu dans le cadre du travail à domicile ou destiné à être transporté hors du lieu de travail habituel.

12.2.7 Mise au rebut ou recyclage sécurisé(e) du matériel

L'organisation doit vérifier chacun des éléments du matériel contenant des supports de stockage pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut ou sa réutilisation.

Avant la mise au rebut ou la réutilisation du matériel, il convient de vérifier s'il contient ou non un support de stockage.

Il convient de détruire physiquement les supports de stockage contenant de l'information confidentielle ou protégée par le droit d'auteur, ou bien de détruire, supprimer ou écraser cette information en privilégiant les techniques rendant l'information d'origine irrécupérable plutôt qu'en utilisant la fonction standard de suppression ou de formatage.

12.2.8 Matériel utilisateur laissé sans surveillance

Il convient que les utilisateurs s'assurent que le matériel non surveillé est doté d'une protection appropriée.

Il convient que tous les utilisateurs soient sensibilisés aux exigences et aux procédures de sécurité destinées à protéger les matériels laissés sans surveillance, ainsi qu'aux responsabilités qui leur incombent pour assurer la mise en œuvre de cette protection. Il convient de recommander aux utilisateurs:

a) de fermer les sessions actives lorsqu'ils ont terminé, sauf si les sessions peuvent être sécurisées par un mécanisme de verrouillage approprié, par exemple un économiseur d'écran protégé par un mot de passe;

b) de se déconnecter des applications ou des services en réseau lorsqu'ils n'en ont plus besoin;

c) lorsqu'ils ne s'en servent pas, de protéger les ordinateurs ou les appareils mobiles contre toute utilisation non autorisée par une clé ou un dispositif équivalent tel qu'un mot de passe.

12.2.9 Politique du bureau propre et de l'écran vide

L'organisation doit adopter une politique du bureau propre pour les documents papier et les supports de stockage amovibles, et une politique de l'écran vide pour les moyens de traitement de l'information.

Il convient que la politique du bureau propre et de l'écran vide tienne compte des classes d'information, des exigences légales et contractuelles, des risques associés et de la culture de l'organisation. Il convient de tenir compte des directives suivantes :

a) lorsque l'information sensible ou critique liée à l'activité de l'organisation n'est pas utilisée, qu'elle soit sous format papier ou sur un support de stockage électronique, il convient de la mettre sous clé (de préférence dans un coffre-fort, une armoire ou tout autre meuble de sécurité), notamment lorsque les locaux sont vides;

b) lorsque les ordinateurs et les terminaux sont laissés sans surveillance, il convient de les

déconnecter ou de les protéger par un verrouillage de l'écran ou du clavier contrôlé par un mot de passe, un jeton ou un autre mécanisme d'authentification de l'utilisateur. Il convient également qu'ils soient protégés par des clés, des mots de passe ou d'autres mesures de sécurité lorsqu'ils ne servent pas ;

c) il convient d'empêcher l'utilisation non autorisée des photocopieurs et autres appareils de reproduction (par exemple les scanneurs ou les appareils photo numériques);

d) il convient de retirer immédiatement des imprimantes les documents contenant de l'information sensible ou classée.

14. Sécurité liée à l'exploitation (D10)

14.1 Procédures et responsabilités liées à l'exploitation

Chaque organisation doit s'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information.

14.1.1 Procédures d'exploitation documentées

L'organisation doit documenter les procédures d'exploitation et de les mettre à disposition de tous les utilisateurs concernés.

Il convient d'établir des procédures documentées pour les activités d'exploitation liées aux moyens de traitement de l'information et de la communication, telles que les procédures de démarrage et d'arrêt des ordinateurs, la sauvegarde, la maintenance du matériel, la manipulation des supports, la gestion du courrier et de la salle informatique, et la sécurité.

Il convient que les procédures d'exploitation précisent les instructions relatives aux activités d'exploitation, notamment :

a) l'installation et la configuration des systèmes ;

b) le traitement et la manipulation de l'information, qu'ils soient automatisés ou manuels ;

c) la sauvegarde des données ;

d) les exigences de planification, y compris les interdépendances avec d'autres systèmes, et les heures de démarrage de la première tâche et d'achèvement de la dernière tâche ;

e) la procédure de redémarrage et de récupération du système à appliquer en cas de défaillance du système ;

f) la gestion du système de traçabilité et de l'information des journaux système ;

g) la surveillance des procédures.

Il convient que les procédures d'exploitation et les procédures documentées s'appliquant aux activités du système soient traitées comme des documents formels et que les modifications qui y sont apportées soient autorisées par la direction.

Lorsque cela est techniquement réalisable, il convient de gérer les systèmes d'information de façon homogène en utilisant des procédures, des outils et des utilitaires identiques.

14.1.2 Gestion des changements

L'organisation doit contrôler les changements apportés à elle aux processus métier, aux systèmes et moyens de traitement de l'information qui influent sur la sécurité de l'information.

Il convient de prendre en compte notamment les éléments suivants :

a) l'identification et la consignation des changements significatifs ;

b) la planification des changements et de la phase de test ;

c) l'appréciation des incidences potentielles de ces changements, y compris les incidences sur la

Sécurité de l'information ;

d) la procédure d'autorisation formelle des changements proposés ;

e) la vérification que les exigences de sécurité de l'information sont respectées ;

f) la transmission des informations détaillées sur les changements apportés à toutes les personnes concernées;

g) les procédures de repli, incluant les procédures et les responsabilités en cas d'abandon et de récupération suite à l'échec des changements ou à des événements imprévus ;

h) la mise en place maîtrisée d'un processus de modification d'urgence permettant une mise en œuvre rapide et contrôlée des modifications nécessitées par la résolution d'un incident.

Il convient de mettre en place des procédures et des responsabilités de gestion formelles pour assurer un contrôle satisfaisant de tous les changements apportés. Lorsque des changements sont effectués, il convient de conserver un journal d'audit contenant toute l'information pertinente.

Un contrôle insuffisant des changements apportés aux systèmes et moyens de traitement de l'information constitue une cause répandue de défaillance du système ou de la sécurité. Des changements apportés à l'environnement d'exploitation, particulièrement s'il s'agit de faire passer un système du stade de développement au stade d'exploitation, peuvent avoir des conséquences sur la fiabilité des applications.

14.1.3 Dimensionnement

L'organisation doit surveiller et ajuster au plus près l'utilisation des ressources et elle doit faire des projections sur les dimensionnements futurs pour garantir les performances exigées du système ;

Il convient d'identifier les exigences de dimensionnement en tenant compte du caractère critique du système concerné pour l'organisation. Il convient d'appliquer un ajustement au plus près et une surveillance des systèmes pour assurer, et s'il y a lieu améliorer, leur disponibilité et leur efficacité ;

Il convient de mettre en place des mesures de détection pour identifier les problèmes en temps voulu. Il convient que les projections en matière de dimensionnement futur tiennent compte des nouvelles exigences métier et système, et des orientations présentes et projetées de l'organisation en matière de capacité de traitement de l'information ;

Il est nécessaire de porter une attention particulière aux ressources pour lesquelles les délais d'approvisionnement sont longs ou les coûts élevés : il convient donc que les responsables surveillent l'utilisation des ressources-clés du système.

Il convient que les responsables identifient les évolutions d'utilisation, en particulier en ce qui concerne les applications métier ou les outils de gestion des systèmes d'information.

Il convient que les responsables utilisent cette information pour identifier et éviter les goulots d'étranglement potentiels, et pour éviter d'avoir à dépendre de personnel-clé, ce qui peut représenter une menace pour la sécurité du système ou pour les services, et qu'ils planifient l'action appropriée.

Il est possible d'atteindre un dimensionnement suffisant en augmentant la capacité du système ou en réduisant la demande. Voici des exemples de gestion de la demande en dimensionnement :

a) suppression des données obsolètes (espace disque) ;

b) mise hors service d'applications, de systèmes, de bases de données ou d'environnements ;

c) optimisation des traitements par lots et de la planification ;

d) optimisation de la logique des applications ou des requêtes de bases de données ;

Il convient d'étudier un plan documenté de la gestion du dimensionnement pour les systèmes critiques.

14.1.4 Séparation des environnements de développement, de test et d'exploitation

L'organisation doit séparer les environnements de développement, de test et d'exploitation pour réduire les risques d'accès ou de changements non autorisés dans l'environnement en exploitation.

Il convient de déterminer et de mettre en œuvre un niveau de séparation entre les environnements d'exploitation, de test et de développement pour prévenir les problèmes d'exploitation.

Il convient d'envisager les éléments suivants :

a) Il convient de définir et de documenter les règles concernant le passage des logiciels du stade de développement au stade d'exploitation ;

b) il convient d'exécuter les logiciels de développement et les logiciels d'exploitation sur des systèmes ou des microprocesseurs informatiques différents et dans des domaines ou répertoires différents ;

c) il convient de tester les modifications apportées aux systèmes et aux applications en exploitation dans un environnement de test ou de pré production avant de les appliquer aux systèmes en exploitation ; en dehors de circonstances exceptionnelles, il convient de ne pas procéder à des tests sur des systèmes en exploitation.

d) il convient que les compilateurs, éditeurs et autres outils de développement ou utilitaires système ne soient accessibles depuis les systèmes en exploitation que lorsque cela est nécessaire ;

e) il convient que les utilisateurs utilisent des profils utilisateurs différents pour les systèmes en exploitation et les systèmes de test et que les menus affichent les messages d'identification adéquats pour réduire le risque d'erreur ;

f) il convient de ne pas copier de données sensibles dans l'environnement du système de test, à moins que le système de test soit doté de mesures de sécurité équivalentes.

Les activités de développement et de test peuvent causer de graves problèmes, tels qu'une modification indésirable des fichiers ou de l'environnement système, ou une défaillance du système.

Il est nécessaire de maintenir un environnement stable et connu de tous permettant de réaliser des tests significatifs et d'empêcher tout accès inapproprié des développeurs à l'environnement d'exploitation.

La séparation physique des environnements de développement, de test et d'exploitation est souhaitable pour réduire les risques de changements accidentels ou d'accès non autorisé aux logiciels en exploitation et aux données liées à l'activité.

14.2 Protection contre les logiciels malveillants

Chaque organisation doit garantir que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants.

14.2.1 Mesures contre les logiciels malveillants

L'organisation doit mettre en œuvre des mesures de détection, de prévention et de récupération, conjuguées à une sensibilisation des utilisateurs adaptée, pour se protéger contre les logiciels malveillants.

Il convient que la protection contre les logiciels malveillants soit fondée sur les programmes de détection de logiciels malveillants et de réparation, la sensibilisation à la sécurité de l'information, et des mesures adéquates de gestion des changements et de l'accès au système.

Il convient d'envisager les préconisations suivantes :

a) établir une politique formelle prohibant l'utilisation de logiciels non autorisés ;

b) mettre en œuvre des contrôles destinés à empêcher ou à détecter l'utilisation de logiciels non autorisés (par exemple, listes blanches d'applications) ;

c) mettre en œuvre des contrôles destinés à empêcher ou à détecter l'utilisation de sites web connus pour leur malveillance ou suspectés en tant que tels (par exemple, liste noire) ;

d) établir une politique formelle indiquant les mesures de protection qu'il convient de prendre pour se protéger des risques liés aux fichiers et logiciels obtenus aussi bien depuis ou via les réseaux externes que sur tout autre support;

e) réduire les vulnérabilités pouvant être exploitées par des logiciels malveillants, par exemple grâce à une gestion des vulnérabilités techniques.

f) mener des revues régulières des logiciels et du contenu de données des systèmes soutenant les processus métier cruciaux. Il convient de mener une investigation formelle sur la présence de tout fichier non approuvé ou de modifications non autorisées ;

g) procéder à l'installation et à la mise à jour régulière de logiciels de détection et de réparation pour analyser les ordinateurs et les supports à titre de mesure de précaution ou comme tâche de routine.

h) définir des procédures et des responsabilités pour assurer la protection des systèmes contre les logiciels malveillants, la formation à l'utilisation de ces systèmes, le signalement et la récupération après une attaque par des logiciels malveillants ;

i) élaborer des plans appropriés de continuité de l'activité en vue de la récupération après une attaque par logiciel malveillant, comprenant les sauvegardes de tous les logiciels et

données nécessaires, et les dispositions de récupération ;

j) mettre en œuvre des procédures pour recueillir régulièrement de l'information, comme l'inscription à des listes de diffusion ou la consultation de sites web apportant de l'information sur les nouveaux logiciels malveillants ;

k) mettre en œuvre des procédures pour vérifier l'information en rapport avec les logiciels malveillants et s'assurer que les bulletins d'alerte sont exacts et informatifs. Il convient que les responsables veillent à l'utilisation de sources qualifiées, telles que des publications réputées, des sites Internet fiables ou des éditeurs de logiciels de protection contre les logiciels malveillants, afin de distinguer les canulars des menaces réelles. Il convient d'informer tous les utilisateurs de l'existence des canulars et de la marche à suivre s'ils en reçoivent ;

l) isoler les environnements au sein desquels les conséquences peuvent s'avérer désastreuses.

L'utilisation, sur l'ensemble de l'environnement de traitement de l'information, d'au moins deux logiciels de protection contre les logiciels malveillants, provenant d'éditeurs différents et reposant sur des technologies différentes, peut améliorer l'efficacité de la protection contre les logiciels malveillants.

14.3 Stratégie de sauvegarde et de rétention/conservation des données

Chaque organisation est tenue de prendre toutes dispositions appropriées pour éviter la perte de données.

14.3.1 Sauvegarde des informations

L'organisation doit réaliser des copies de sauvegarde de l'information, des logiciels et des images systèmes, et de les tester régulièrement conformément à une politique de sauvegarde convenue.

Il convient d'établir une politique de sauvegarde destinée à définir les exigences de l'organisation en matière de sauvegarde de l'information, des logiciels et des systèmes.

Il convient que la politique de sauvegarde définisse les exigences en matière de conservation et de protection des copies de sauvegarde.

Il convient de prévoir des équipements de sauvegarde adéquats pour s'assurer que toute l'information et tous les logiciels essentiels peuvent être récupérés en cas de sinistre ou de défaillance d'un support.

Lors de la conception d'un plan de sauvegarde, il convient de tenir compte des éléments suivants :

a) il convient de produire des enregistrements exacts et complets des copies de sauvegarde effectuées ainsi que des procédures de restauration documentées ;

b) il convient que l'étendue des sauvegardes (par exemple, sauvegarde totale ou différentielle) et leur fréquence rendent compte des exigences métier de l'organisation, des exigences relatives à la sécurité de l'information concernée, et du caractère critique de l'information pour le maintien de l'activité de l'organisation ;

c) il convient de placer les sauvegardes à un endroit suffisamment distant du site

principal pour échapper à tout dommage résultant d'un sinistre sur le site principal ;

d) il convient de doter l'information sauvegardée d'un niveau de protection physique et environnementale approprié cohérent avec les normes appliquées sur le site principal ;

e) il convient de tester régulièrement les supports de sauvegarde pour s'assurer qu'il est possible de s'en servir, le cas échéant, en situation d'urgence. Il convient de combiner cette opération à un test des procédures de restauration et de vérifier le temps de restauration requis. Il convient de tester la capacité de restauration de données sauvegardées sur des supports de test dédiés et de ne pas écraser les supports d'origine au cas où la sauvegarde ou le processus de restauration échouerait, causant la perte de données ou endommageant celles-ci de manière irréversible ;

f) dans les situations où la confidentialité est importante, il convient de protéger les sauvegardes en les chiffrant.

Il convient que les procédures d'exploitation assurent une surveillance de l'exécution des sauvegardes et remédient aux défaillances rencontrées par les sauvegardes programmées, pour garantir l'intégrité des sauvegardes conformément à la politique de sauvegarde.

Il convient de tester régulièrement les dispositions de sauvegarde concernant les systèmes et les services individuels, pour s'assurer qu'elles répondent aux plans de continuité de l'activité. Pour les systèmes et les services critiques, il convient que les dispositions relatives aux sauvegardes couvrent toute l'information système, les applications et les données nécessaires à la récupération totale du système en cas de sinistre.

Il convient de déterminer la durée de conservation de l'information essentielle à l'activité de l'organisation, en prenant en compte toute éventuelle exigence de conservation à titre permanent de copies d'archivage.

14.4 Journalisation et surveillance

Chaque organisation doit enregistrer les événements et générer des preuves.

14.4.1 Journalisation des événements

Il convient de créer, de tenir à jour et de revoir régulièrement les journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information.

Il convient que les journaux d'événement contiennent, lorsque c'est pertinent, les informations suivantes :

a) les identifiants utilisateurs;

b) les activités du système;

c) la date, l'heure et les détails relatifs aux événements significatifs, par exemple les ouvertures et fermetures de session;

d) l'identité ou l'emplacement du terminal si possible et l'identifiant du système;

e) les enregistrements des tentatives d'accès au système, réussies et avortées;

f) les enregistrements des tentatives d'accès aux données et autres ressources, réussies ou avortées;

g) les modifications apportées à la configuration du système;

h) l'utilisation des privilèges;

i) l'emploi des utilitaires et des applications;

j) les fichiers qui ont fait l'objet d'un accès et la nature de l'accès;

k) les adresses et les protocoles du réseau;

l) les alarmes déclenchées par le système de contrôle d'accès;

m) l'activation et la désactivation des systèmes de protection, tels que les systèmes antivirus et les systèmes de détection des intrusions;

n) les enregistrements des transactions réalisées par les utilisateurs dans les applications.

La journalisation des événements pose les fondations des systèmes de surveillance automatisés, capables de générer des rapports consolidés et des alertes relatives à la sécurité du système.

Les journaux d'événements peuvent contenir des données sensibles et des informations à caractère personnel. Il convient de prendre des mesures appropriées de protection de la confidentialité des informations personnelles. Lorsque cela est possible, il convient que les administrateurs systèmes n'aient pas l'autorisation d'effacer ou de désactiver les journaux concernant leurs propres activités.

14.4.2 Protection de l'information journalisée

L'organisation doit protéger les moyens de journalisation et l'information journalisée contre les risques de falsification ou d'accès non autorisé.

Il convient que des mesures soient conçues pour protéger le moyen de journalisation contre les modifications non autorisées de la journalisation des informations et les dysfonctionnements, à savoir :

a) l'altération des types de message enregistrés ;

b) la modification ou la suppression des fichiers journaux ;

c) le dépassement de la capacité du support de stockage du fichier journal, qui a pour effet d'empêcher l'enregistrement des événements ou d'écraser les événements déjà enregistrés.

Il peut être nécessaire d'archiver certains journaux d'audit dans le cadre de la politique de conservation des enregistrements ou à des fins de collecte et de conservation de preuves.

Les journaux système contiennent souvent un volume d'information important. La plus grande partie de cette information ne concerne pas la surveillance liée à la sécurité de l'information.

En vue de faciliter la détection des événements significatifs pour la surveillance liée à la sécurité de l'information, il convient d'envisager la copie automatique des types de messages dans un second journal ou d'utiliser les utilitaires systèmes ou les outils d'audit appropriés pour interroger et rationaliser les fichiers.

Il est nécessaire de protéger les journaux système, car s'il est possible de modifier ou d'effacer les données qu'ils contiennent, leur existence peut créer une fausse impression de sécurité. Pour sauvegarder les journaux, il est possible de recourir à la copie en temps réel des journaux vers un système hors du contrôle de l'administrateur système ou de l'opérateur.

14.4.3 Journaux administrateur et opérateur

Il convient de journaliser les activités de l'administrateur système et de l'opérateur système, ainsi que de protéger et de revoir régulièrement les journaux.

Les détenteurs de comptes utilisateur dotés de privilèges peuvent être à même de manipuler les journaux sur les moyens de traitement de l'information qu'ils contrôlent directement : il est donc nécessaire de protéger et de revoir les journaux afin de garantir l'imputabilité des utilisateurs dotés de privilèges.

Pour vérifier la conformité des activités d'administration système et réseau, il est possible d'utiliser un système de détection d'intrusion hors du contrôle des administrateurs systèmes et réseaux.

14.4.4 Synchronisation des horloges

Il convient de synchroniser les horloges de l'ensemble des systèmes de traitement de l'information concernés d'une organisation ou d'un domaine de sécurité sur une source de référence temporelle unique.

Il convient de documenter les exigences internes et externes liées à la représentation de l'heure, la synchronisation et la précision. Ces exigences peuvent être des exigences légales, réglementaires, contractuelles, des exigences de conformité à des normes ou des exigences liées à la surveillance interne. Il convient de définir pour l'organisation une heure de référence standard.

Il convient de documenter et de mettre en œuvre la méthode utilisée par l'organisation pour obtenir une heure de référence à partir d'une ou des sources externes et la méthode utilisée pour synchroniser de manière fiable les horloges internes.

Le paramétrage correct des horloges est important pour garantir la précision des journaux d'audit qui peuvent être utilisés lors d'investigations ou servir de preuves dans le cadre d'affaires judiciaires ou de procédures disciplinaires. Des journaux d'audit imprécis peuvent gêner les investigations et nuire à la crédibilité des preuves. Pour les systèmes de journalisation, il est possible d'utiliser une horloge maîtresse reliée à un signal horaire radiodiffusé par une horloge atomique nationale.

14.5 Maîtrise des logiciels en exploitation

Chaque organisation doit garantir l'intégrité des systèmes en exploitation.

14.5.1 Installation de logiciels sur des systèmes en exploitation

L'organisation doit mettre en œuvre des procédures pour contrôler l'installation de logiciels sur des systèmes en exploitation.

Pour contrôler les changements de logiciels sur des systèmes en exploitation, il convient de prendre en compte les directives suivantes :

a) il convient que la mise à jour du logiciel en exploitation, des applications et des bibliothèques de programmes soit réalisée uniquement par des administrateurs qualifiés, après autorisation de la direction ;

b) il convient que les systèmes en exploitation contiennent uniquement des codes exécutables approuvés et non des codes en développement ou des compilateurs ;

c) il convient de mettre en œuvre les applications et le logiciel du système d'exploitation seulement au terme d'une série complète de tests ayant donné des résultats satisfaisants. Il convient que la batterie de tests porte sur l'aptitude à l'emploi, la sécurité, les effets sur les autres systèmes et la convivialité.

d) Il convient que les tests soient réalisés sur des systèmes séparés. Il convient de vérifier que toutes les bibliothèques de programmes sources ont été mises à jour ;

e) il convient d'utiliser un système de contrôle de la configuration afin de conserver le contrôle de tous les logiciels mis en œuvre, ainsi que de la documentation système ;

f) il convient de mettre en place une stratégie de retour en arrière avant d'appliquer des modifications ;

g) il convient de tenir à jour un journal d'audit de toutes les mises à jour réalisées sur les bibliothèques de programmes en exploitation ;

h) il convient de conserver les versions antérieures du logiciel d'application à titre de mesure de secours ;

i) il convient d'archiver les versions antérieures du logiciel, ainsi que toute l'information nécessaire, les paramètres, les procédures, les détails de configuration et les logiciels complémentaires associés pendant toute la durée d'archivage des données.

Pour les logiciels fournis par l'éditeur et installés sur les systèmes en exploitation, il convient d'assurer une maintenance permettant de bénéficier de l'assistance technique de l'éditeur. Au fil du temps, les éditeurs de logiciels cessent de fournir une assistance technique pour les anciennes versions. Il convient que l'organisation tienne compte des risques associés à l'utilisation de logiciels dont la maintenance n'est pas prise en charge par l'éditeur.

Il convient que toute décision d'acquérir une nouvelle version tienne compte des exigences métier à l'origine du changement, ainsi que des questions de sécurité liées à la nouvelle version, à savoir l'introduction d'une nouvelle fonction de sécurité de l'information ou le nombre et la gravité des problèmes de sécurité de l'information liés à cette version. Il convient d'appliquer des correctifs

logiciels chaque fois qu'ils permettent de supprimer ou de réduire les failles de sécurité de l'information.

Il convient d'accorder l'accès physique ou logique aux éditeurs uniquement lorsque c'est nécessaire pour répondre aux besoins de l'assistance technique, après autorisation de la direction. Il convient de surveiller les activités de l'éditeur.

Les logiciels peuvent dépendre de logiciels et modules fournis par un tiers qu'il convient de surveiller et de contrôler, afin d'éviter tout changement non autorisé susceptible d'introduire des failles de sécurité.

14.6 Gestion des vulnérabilités techniques

Chaque organisation doit empêcher toute exploitation des vulnérabilités techniques.

14.6.1 Gestion des vulnérabilités techniques

Il convient d'être informé en temps voulu des vulnérabilités techniques des systèmes d'information en exploitation, d'évaluer l'exposition de l'organisation à ces vulnérabilités et de prendre les mesures appropriées pour traiter le risque associé.

Pour une gestion efficace des vulnérabilités techniques, il est indispensable de disposer d'un inventaire des actifs informationnels, exhaustif et à jour.

L'information spécifique nécessaire à la gestion des vulnérabilités techniques comporte le nom de l'éditeur du logiciel, les numéros de version, l'état de déploiement (par exemple, quel logiciel est installé sur quels systèmes) et le nom de la ou des personne(s) responsable(s) du logiciel au sein de l'organisation.

Dès l'identification de vulnérabilités techniques potentielles, il convient d'engager l'action appropriée dans les meilleurs délais.

Il convient d'appliquer les recommandations suivantes pour établir un processus efficace de gestion des vulnérabilités techniques :

a) il convient que l'organisation définisse et établisse les rôles et les responsabilités associés à la gestion des vulnérabilités techniques, notamment la veille en matière de vulnérabilités, l'appréciation du risque, l'application de correctifs logiciels, le suivi des actifs, ainsi que toute responsabilité de coordination requise ;

b) il convient de déterminer les ressources d'information permettant d'identifier les vulnérabilités techniques pertinentes et de sensibiliser les intervenants sur ces vulnérabilités, pour les logiciels et les autres technologies.

c) Il convient de définir un délai de réaction aux notifications relatives à d'éventuelles vulnérabilités techniques pertinentes ;

d) lorsqu'une vulnérabilité technique potentielle est identifiée, il convient que l'organisation détermine les risques associés et les actions à entreprendre : cela peut consister à installer un correctif logiciel sur les systèmes vulnérables ou à appliquer d'autres mesures ;

e) en fonction du caractère d'urgence présenté par la vulnérabilité technique, il convient que l'action soit entreprise conformément aux mesures de gestion des changements ou

en appliquant les procédures de réponse aux incidents liés à la sécurité de l'information;

f) si un correctif logiciel d'une source autorisée est disponible, il convient d'évaluer les risques associés à l'installation de ce correctif;

g) il convient d'évaluer et de tester les correctifs logiciels avant de les installer afin de vérifier leur efficacité et de s'assurer qu'ils n'entraînent pas d'effets collatéraux inacceptables. Si aucun correctif logiciel n'est disponible, il convient d'envisager d'autres mesures, telles que :

   1) la désactivation des services ou des fonctions liés à la vulnérabilité ;

   2) l'adaptation ou l'ajout de contrôles d'accès, par exemple des pare-feu, aux limites du réseau ;

   3) le renforcement du dispositif de surveillance visant à détecter les attaques réelles ;

   4) le renforcement de la politique de sensibilisation aux vulnérabilités ;

h) il convient de tenir un journal d'audit de toutes les procédures entreprises ;

i) il convient de surveiller et d'évaluer à intervalles réguliers le processus de gestion des vulnérabilités techniques afin de s'assurer de son efficacité ;

j) il convient de traiter en priorité les systèmes à haut risque ;

k) il convient d'harmoniser les activités de gestion des incidents avec un processus efficace de gestion des vulnérabilités techniques, pour communiquer les données relatives aux vulnérabilités à la fonction de réponse aux incidents et fournir des procédures techniques à exécuter en cas d'incident;

l) définir une procédure s'appliquant aux situations dans lesquelles une vulnérabilité a été identifiée et pour laquelle il n'existe pas de contre-mesure appropriée.

14.6.2 Restrictions liées à l'installation de logiciels

Il convient d'établir et de mettre en œuvre des règles régissant l'installation de logiciels par les utilisateurs.

Il convient que l'organisation détermine et impose une politique stricte sur le type de logiciels que les utilisateurs peuvent installer.

Il convient d'appliquer le principe du moindre privilège. Les utilisateurs auxquels ont été accordés certains privilèges peuvent avoir la possibilité d'installer des logiciels.

Il convient que l'organisation détermine les types de logiciels dont l'installation est autorisée (par exemple l'installation des mises à jour ou de correctifs à des logiciels existants) et les types d'installation qui sont interdits (par exemple, l'installation de logiciels destinés uniquement à un usage personnel, ou de logiciels dont on ignore s'ils sont potentiellement malveillants ou pour lesquels on éprouve des doutes).

Il convient d'accorder ces privilèges en tenant compte des fonctions des utilisateurs concernés.

14.7 Considérations sur l'audit du système d'information

Chaque organisation doit réduire au minimum l'incidence des activités d'audit sur les systèmes en exploitation.

14.7.1 Mesures relatives à l'audit des systèmes d'information

Pour réduire au minimum les perturbations subies par les processus métier, il convient de planifier avec soin et d'arrêter avec les personnes intéressées les exigences d'audit et les activités impliquant des contrôles des systèmes en exploitation.

Il convient de respecter les points suivants :

a) il convient d'arrêter avec la direction concernée les exigences d'audit liées à l'accès aux systèmes et aux données;

b) il convient d'arrêter le domaine d'application des tests techniques d'audit et de le contrôler;

c) il convient de limiter les tests d'audit à un accès en lecture seule des logiciels et des données;

d) il convient que les accès autres qu'en lecture seule ne soient autorisés que pour les copies séparées des fichiers système. Une fois l'audit terminé, il convient soit de les effacer, soit de les protéger de manière appropriée si les exigences de documentation de l'audit imposent de les conserver ;

e) il convient d'identifier et d'arrêter les exigences relatives aux traitements particuliers ou supplémentaires.

f) il convient que les tests d'audit pouvant compromettre la disponibilité du système soient réalisés en dehors des heures de travail;

g) il convient de contrôler et de journaliser tous les accès afin de disposer d'une traçabilité faisant référence.

15. Sécurité des communications (D11)

15.1 Management de la sécurité des réseaux

Caque organisation doit garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie.

15.1.1 Contrôle des réseaux

L'organisation doit gérer et contrôler les réseaux pour protéger l'information contenue dans les systèmes et les applications.

Il convient de mettre en œuvre des mesures pour assurer la sécurité de l'information sur les réseaux et la protection des services connectés contre les accès non autorisés. Il convient d'envisager en particulier ce qui suit :

a) il convient de définir les responsabilités et les procédures de gestion de l'équipement réseau;

b) le cas échéant, il convient de séparer la responsabilité d'exploitation des réseaux et celle de l'exploitation des ordinateurs;

c) il convient de définir des mesures spéciales pour préserver la confidentialité et l'intégrité des données transmises sur les réseaux publics ou les réseaux sans fil et de protéger les systèmes et applications connectés. Des mesures spéciales peuvent aussi s'avérer nécessaires pour maintenir la disponibilité des services réseau et des ordinateurs connectés ;

d) il convient de procéder à une journalisation et d'assurer une surveillance appropriées permettant l'enregistrement et la détection d'actions susceptibles d'affecter la sécurité de l'information ou qui s'avèrent pertinentes pour la sécurité de l'information;

e) il convient de coordonner étroitement les activités de gestion à la fois pour optimiser le service fourni à l'organisation et pour s'assurer que les mesures sont appliquées de façon homogène à travers toute l'infrastructure de traitement de l'information;

f) il convient d'authentifier les systèmes sur le réseau;

g) il convient de limiter la connexion des systèmes au réseau.

15.1.2 Sécurité des services de réseau

Pour tous les services de réseau, il convient d'identifier les mécanismes de sécurité, les niveaux de service et les exigences de gestion, et de les intégrer dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés.

Il convient de déterminer et de surveiller régulièrement la capacité du fournisseur de services de réseau à gérer ses services de façon sécurisée et il convient de conclure un accord sur le droit à auditer.

Il convient d'identifier les dispositions de sécurité nécessaires à des services en particulier, telles que les fonctions de sécurité, les niveaux de service et les exigences de gestion. Il convient que l'organisation s'assure que les fournisseurs de services de réseau mettent ces mesures en œuvre.

15.1.3 Cloisonnement des réseaux

Il convient que les groupes de services d'information, d'utilisateurs et de systèmes d'information soient cloisonnés sur les réseaux.

Une méthode de management de la sécurité des grands réseaux consiste à les diviser en domaines séparés. Les domaines peuvent être choisis à partir des niveaux de sécurisation (par exemple domaine d'accès public, domaine poste de travail, domaine serveur), par service administratif (par exemple ressources humaines, financier, marketing) ou par combinaison (par exemple connexion du domaine serveur à de nombreux services administratifs).

Le cloisonnement peut être réalisé en utilisant des réseaux physiques différents ou des réseaux logiques différents (par exemple réseau privé virtuel).

Il convient de bien définir le périmètre de chaque domaine. L'accès entre les différents domaines du réseau est autorisé, mais il convient de le contrôler au niveau du périmètre en utilisant une passerelle (exemple: pare-feu, routeur-filtre).

Il convient de déterminer les critères de cloisonnement des réseaux en domaines et l'accès autorisé au-delà des passerelles en s'appuyant sur une appréciation des exigences de sécurité propres à chaque domaine.

Il convient que cette appréciation soit en conformité avec la politique du contrôle d'accès, les exigences d'accès, la valeur et la classification de l'information traitée et qu'elle prenne également en compte le coût relatif et les répercussions sur les performances de l'incorporation d'une technologie de passerelle appropriée.

À noter que les réseaux sans fil nécessitent un traitement spécial en raison d'une mauvaise définition du périmètre du réseau. Dans le cas des environnements sensibles, il convient de veiller à traiter l'ensemble des accès sans fil comme des connexions externes et de séparer ces accès des réseaux internes jusqu'à franchissement de la passerelle conformément à la politique de contrôle des réseaux avant d'accorder l'accès aux systèmes internes.

Les technologies d'authentification, de chiffrement et de contrôle d'accès réseau au niveau utilisateur propres aux réseaux sans fil modernes normalisés peuvent être suffisantes pour permettre une connexion directe au réseau interne de l'organisation, lorsqu'elles sont correctement mises en œuvre.

15.2 Transfert de l'information

Chaque organisation doit maintenir la sécurité de l'information transférée au sein de l'organisation et vers une entité extérieure.

15.2.1 Politiques et procédures de transfert de l'information

L'organisation doit mettre en place des politiques, des procédures et des mesures de transfert formelles pour protéger les transferts d'information transitant par tous types d'équipements de communication.

Il convient que les procédures et mesures à suivre pour utiliser les équipements de communication servant aux transferts de l'information prennent en compte les points suivants :

a) les procédures conçues pour protéger l'information transférée contre l'interception, la reproduction, la modification, les erreurs d'acheminement et la destruction;

b) les procédures de détection et de protection contre les logiciels malveillants qui peuvent être transmis via l'utilisation des communications électroniques;

c) les procédures de protection de l'information électronique sensible communiquée sous forme de pièce jointe;

d) une politique ou des directives décrivant succinctement l'utilisation acceptable des équipements de communication;

e) les responsabilités incombant aux salariés, aux tiers ou à tout autre utilisateur de ne pas compromette l'organisation, par exemple par diffamation, harcèlement, usurpation

d'identité, renvoi de chaînes de messages, achats non autorisés, etc.;

f) l'utilisation de techniques de cryptographie, par exemple pour protéger la confidentialité, l'intégrité et l'authenticité de l'information;

g) les directives sur la conservation et la mise au rebut de toutes les correspondances commerciales, dont les messages, conformément aux législations et réglementations nationales et locales applicables;

h) les mesures et les restrictions liées à l'utilisation des équipements de communication, comme le renvoi automatique de courriers électroniques vers des adresses électroniques extérieures;

i) rappeler au personnel de prendre les précautions appropriées pour ne pas divulguer l'information confidentielle;

j) ne pas laisser de messages comportant de l'information sensible sur les répondeurs puisque ces derniers peuvent être réécoutés par des personnes non autorisées, stockés sur des systèmes à usage collectif ou incorrectement mémorisés à la suite d'une erreur de numérotation;

k) rappeler au personnel les problèmes qu'entraîne l'utilisation de télécopieurs ou de services de télécopie, à savoir:

   1) l'accès non autorisé aux mémoires de messages intégrées pour récupérer des messages;

   2) la programmation délibérée ou accidentelle de machines pour qu'elles envoient des messages à des numéros précis;

   3) l'envoi de documents et de messages au mauvais numéro soit par erreur de numérotation, soit par utilisation d'un numéro mémorisé erroné.

En outre, il convient de rappeler au personnel qu'il est recommandé de ne pas tenir de conversation confidentielle dans des lieux publics, sur des réseaux de communication non sécurisés, dans des bureaux ouverts ou des lieux de réunion.

Il convient que les équipements de transfert de l'information soient conformes aux exigences légales applicables.

Le transfert d'informations peut se produire par le biais de nombreux types d'équipements de communication différents, dont la messagerie électronique, la voix, la télécopie et la vidéo.

Le transfert de logiciels peut se produire par des moyens nombreux et variés, notamment les téléchargements depuis Internet et l'acquisition auprès d'éditeurs fournissant des logiciels clés en main.

Il convient de prendre en compte les implications commerciales, légales et en termes de sécurité liées à l'échange de données électroniques, au commerce électronique et aux communications électroniques, ainsi que les exigences en matière de contrôles.

15.2.2 Accords en matière de transfert d'information

Il convient que les accords traitent du transfert sécurisé de l'information liée à l'activité entre l'organisation et les tiers.

Il convient que les accords en matière de transfert intègrent les aspects suivants :

a) les responsabilités de gestion pour contrôler et informer de la transmission, de la répartition et de la réception;

b) les procédures pour garantir la traçabilité et la non-répudiation;

c) les normes techniques minimales pour l'encapsulation et la transmission;

d) les accords de séquestre;

e) les normes d'identification coursiers;

f) les obligations et les responsabilités en cas d'incident lié à la sécurité de l'information, comme la perte de données;

g) l'utilisation convenue d'un système de marquage pour l'information sensible ou critique, permettant de garantir une compréhension immédiate des marques et la protection appropriée de l'information;

h) les normes techniques pour l'enregistrement et la lecture de l'information et des logiciels;

i) toutes mesures particulières pouvant s'avérer nécessaires pour la protection des pièces sensibles, comme l'utilisation de la cryptographie;

j) tenir à jour la traçabilité de l'information en transit;

k) les niveaux acceptables de contrôle d'accès.

Il convient d'établir et de tenir à jour des politiques, des procédures et des normes pour protéger l'information et les supports physiques en transit, et il convient de les mentionner dans les accords de transfert.

Il convient que la partie sécurité de l'information de tout accord mette en évidence la sensibilité de l'information concernée.

Les accords peuvent être conclus de façon électronique ou manuelle et peuvent prendre la forme de contrats formels. En ce qui concerne l'information confidentielle, il convient que les mécanismes spécifiques employés pour le transfert de cette information soient homogènes dans toutes les organisations et pour tous les types d'accords.

15.2.3 Messagerie électronique

L'organisation doit protéger de manière appropriée l'information transitant par la messagerie électronique.

Pour la sécurité de l'information dans le cadre de la messagerie électronique, il convient de prendre en compte :

a) une protection des messages contre tout accès non autorisé, toute modification ou déni de service en corrélation avec le plan de classification adopté par l'organisation;

b) la qualité de l'adressage et du transport du message;

c) la disponibilité et la fiabilité du service;

d) les questions juridiques, comme les exigences en matière de signatures numériques;

e) l'obtention d'une autorisation avant d'utiliser des services externes publics comme une messagerie instantanée, un réseau social ou le partage de fichiers;

f) des niveaux plus élevés d'authentification permettant de contrôler l'accès depuis les réseaux accessibles au public.

15.2.4 Engagements de confidentialité ou de non-divulgation

Il convient d'identifier, de revoir régulièrement et de documenter les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins de l'organisation en matière de protection de l'information.

Il convient que les modalités des engagements de confidentialité ou de non-divulgation spécifient des exigences de protection de l'information confidentielle en des termes juridiquement exécutoires. Les engagements de confidentialité ou de non-divulgation sont applicables aux tiers et aux salariés de l'organisation.

Il convient de sélectionner ou d'ajouter des éléments en tenant compte de la catégorie du tiers et des accès ou du traitement de l'information confidentielle acceptables pour sa catégorie. Pour identifier les exigences en matière de confidentialité et de non-divulgation, il convient de tenir compte des éléments suivants:

a) une définition de l'information à protéger (par exemple information confidentielle);

b) la durée prévue de l'engagement, y compris les cas où il peut s'avérer nécessaire de poursuivre cette durée indéfiniment;

c) les actions à entreprendre lorsqu'un engagement arrive à expiration;

d) les responsabilités et les tâches des signataires visant à éviter une divulgation non autorisée de l'information;

e) la propriété de l'information, des secrets de fabrication et la propriété intellectuelle, ainsi que leurs liens avec la protection de l'information confidentielle;

f) l'utilisation autorisée de l'information confidentielle et les droits du signataire relatifs à l'utilisation de cette information;

g) le droit d'auditer et de contrôler des activités impliquant l'utilisation de l'information confidentielle;

h) le processus de notification et de signalement d'une divulgation non autorisée ou d'une fuite de l'information confidentielle;

i) les modalités de retour ou de destruction de l'information à l'expiration de l'engagement;

j) les actions à entreprendre en cas de violation de l'engagement.

En fonction des exigences de sécurité de l'information de l'organisation, il peut s'avérer nécessaire d'inclure d'autres dispositions dans les engagements de confidentialité ou de non-divulgation.

Il convient que les engagements de confidentialité et de non-divulgation soient conformes aux lois et règlements en vigueur dans la juridiction dont ils relèvent.

Il convient de revoir les engagements de confidentialité et de non-divulgation à intervalles réguliers et en cas de changements ayant une incidence sur ces exigences.

16. Acquisition, développement et maintenance des systèmes d'information (D12)

16.1 Exigences de sécurité applicables aux systèmes d'information

Chaque organisation doit veiller à ce que la sécurité de l'information fasse partie intégrante des systèmes d'information tout au long de leur cycle de vie. Cela inclut notamment des exigences spécifiques pour les systèmes d'information fournissant des services sur les réseaux publics.

16.1.1 Analyse et spécification des exigences de sécurité de l'information

Il convient que les exigences liées à la sécurité de l'information figurent dans les exigences des nouveaux systèmes d'information ou des changements apportés aux systèmes existants.

Il convient d'identifier les exigences liées à la sécurité de l'information en utilisant différentes méthodes telles que la prise en compte d'exigences de conformité découlant des règlements et des politiques, les revues, la modélisation des menaces, la revue des incidents et les seuils de vulnérabilité. Il convient de documenter les conclusions de l'identification et de les faire revoir par toutes les parties prenantes.

Il convient que les exigences de sécurité de l'information et les mesures rendent compte de la valeur de l'information concernée, ainsi que des éventuels préjudices pour l'activité de l'organisation pouvant résulter de l'absence d'une sécurité adéquate.

Il convient d'intégrer l'identification et la gestion des exigences de sécurité de l'information, ainsi que les processus associés, aux premières phases des projets de système d'information. Tenir compte des exigences de sécurité de l'information au tout début, par exemple dès la phase de conception, peut permettre d'adopter des solutions plus efficaces et plus rentables.

En ce qui concerne les exigences de sécurité de l'information, il convient également de prendre en compte les éléments suivants :

a) le niveau de confiance requis en ce qui concerne l'identité déclarée des utilisateurs, afin d'en déduire les exigences d'authentification utilisateur;

b) la maîtrise de la gestion des accès et des processus d'autorisation pour les utilisateurs de l'organisation ainsi que pour les utilisateurs techniques ou dotés de privilèges;

c) l'information des utilisateurs et des opérateurs sur les devoirs et les responsabilités qui leur incombent;

d) les exigences de protection que requièrent les actifs impliqués, notamment en ce qui concerne la disponibilité, la confidentialité, l'intégrité;

e) les exigences découlant des processus de l'organisation, tels que la journalisation et la surveillance des transactions, les exigences de non-répudiation;

f) les exigences spécifiées par les autres mesures de sécurité, telles que les interfaces pour la

journalisation et la surveillance ou les systèmes de détection de fuite de données.

En ce qui concerne les applications fournissant des services sur les réseaux publics ou mettant en œuvre des transactions, il convient de tenir compte des mesures spéciales de 15.1.2 et 15.1.3.

Si des produits sont achetés, il convient de suivre un processus formel de test et d'acquisition. Dans les contrats conclus avec le fournisseur, il convient de traiter les exigences de sécurité identifiées. Lorsque le produit proposé dispose d'une fonctionnalité de sécurité insuffisante au regard des exigences spécifiées, alors il convient de réexaminer le risque et les mesures associées avant d'acheter ce produit.

Il convient d'évaluer et de mettre en œuvre les recommandations liées à la configuration de la sécurité fournies avec le produit en harmonie avec le logiciel final et/ou la pile de services du système.

Il convient de définir les critères d'acceptation des produits, par exemple en termes de fonctionnalité, qui garantissent que les exigences de sécurité identifiées sont respectées. Il convient d'évaluer les produits au regard de ces critères avant de procéder à l'achat. Il convient de revoir toute nouvelle fonctionnalité pour s'assurer qu'elle n'entraîne pas de risques supplémentaires inacceptables.

16.1.2 Sécurisation des services d'application sur les réseaux publics

Chaque organisation doit protéger l'information liée aux services d'application transmise sur les réseaux publics contre les activités frauduleuses, les différends contractuels, ainsi que la divulgation et la modification non autorisées.

Pour la sécurité de l'information des services d'application utilisant les réseaux publics, il convient de prendre en compte :

a) le niveau de confiance requis par chaque partie en ce qui concerne l'identité déclarée des autres, par exemple par une authentification;

b) les processus d'autorisation liés aux personnes qui peuvent approuver le contenu, émettre ou signer des documents transactionnels clés;

c) l'assurance que les partenaires engagés dans la communication sont pleinement informés des autorisations qui leur sont accordées pour la fourniture ou l'utilisation du service;

d) la détermination et la satisfaction des exigences en matière de confidentialité, d'intégrité, de preuve de la répartition et de la réception des documents-clés et de non-répudiation des contrats, dans le contexte par exemple d'appels d'offres et de contrats;

e) le niveau de confiance requis concernant l'intégrité des documents clés;

f) les exigences de protection de l'information confidentielle;

g) la confidentialité et l'intégrité de toutes transactions de commandes, de détails de paiement, de coordonnées de livraison et de confirmation de réception;

h) le degré de vérification adéquat pour contrôler les détails de paiement fournis par le client;

i) la sélection du mode de règlement le plus adapté pour se prémunir de la fraude;

j) le niveau de protection requis pour maintenir la confidentialité et l'intégrité des éléments du bon de commande;

k) le fait d'éviter la perte ou la duplication des détails de la transaction;

l) la responsabilité juridique induite par toute transaction frauduleuse;

m) les exigences de l'assureur.

Il convient qu'un accord documenté, engageant les deux parties conformément aux conditions de service convenues et incluant les détails liés aux autorisations vienne conforter les dispositions des services d'application convenues entre les partenaires.

Il convient de tenir compte des exigences de résistance aux attaques, qui peuvent inclure des exigences de protection des serveurs utilisés pour les applications concernées ou de garantie de la disponibilité des interconnexions réseau requises pour délivrer les services.

Les applications accessibles à partir des réseaux publics sont exposées à toute une série de menaces associées aux réseaux, telles que les activités frauduleuses, les différends contractuels ou la divulgation d'information au grand public. Par conséquent, il est indispensable de procéder à des appréciations détaillées des risques et de sélectionner avec soin les mesures de sécurité.

16.1.3 Protection des transactions liées aux services d'application

Chaque organisation doit protéger l'information impliquée dans les transactions liées aux services d'application pour empêcher une transmission incomplète, des erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou sa réémission.

Pour la sécurité de l'information des transactions liées aux services d'application, il convient de prendre en compte :

a) l'utilisation de signatures électroniques par chacune des parties impliquées dans la transaction;

b) l'ensemble des aspects de la transaction, ce qui revient à s'assurer que:

   1) les informations secrètes d'authentification utilisateur de toutes les parties sont valables et ont fait l'objet d'une vérification;

   2) la transaction demeure confidentielle;

   3) la confidentialité des informations personnelles de toutes les parties impliquées est maintenue;

c) le canal de communication entre toutes les parties impliquées est chiffré;

d) les protocoles utilisés pour la communication entre les parties sont sécurisés;

e) la nécessité de veiller à ce que le stockage des détails de la transaction soit situé hors de tout environnement accessible au public, à l'instar d'une plateforme de stockage en place sur l'intranet de l'organisation, et qu'il ne soit pas conservé ou exposé sur un support de stockage directement accessible depuis Internet;

f) que lorsqu'une autorité de confiance est utilisée (par exemple dans le but d'émettre et de tenir à jour des signatures ou des certificats électroniques), la sécurité est intégrée et imbriquée tout au long du processus de gestion de bout en bout des certificats ou des signatures.

16.2 Sécurité des processus de développement et d'assistance technique

Chaque organisation doit s'assurer que les questions de sécurité de l'information sont étudiées et mises en œuvre dans le cadre du cycle de développement des systèmes d'information.

16.2.1 Politique de développement sécurisé

Il convient d'établir des règles de développement des logiciels et des systèmes, et de les appliquer aux développements de l'organisation.

Le développement sécurisé est une nécessité pour bâtir un service, une architecture, un logiciel et un système sécurisés. Dans une politique de développement sécurisé, il convient de prendre en compte :

a) la sécurité de l'environnement de développement;

b) les recommandations liées à la sécurité dans le cycle de vie du développement d'un logiciel:

   1) la sécurité de la méthodologie de développement du logiciel;

   2) les recommandations relatives à la sécurité du codage pour chaque langage de programmation utilisé;

c) les exigences de sécurité dans la phase de conception;

d) les points de contrôle de la sécurité aux différentes étapes clés du projet;

e) les référentiels sécurisés;

f) la sécurité liée au contrôle des versions;

g) les connaissances requises en matière de sécurité de l'application;

h) les capacités des développeurs à éviter, découvrir et corriger les vulnérabilités.

Il convient d'utiliser des techniques de programmation sécurisée pour les nouveaux développements et les scénarios de réutilisation de codes, dans les cas où les normes s'appliquant au développement ne sont pas forcément connues ou lorsqu'elles ne sont pas cohérentes avec les bonnes pratiques en cours.

Il convient d'envisager des normes de codage sécurisé et, le cas échéant, rendre leur utilisation obligatoire.

Il convient que les développeurs soient formés à leur utilisation et il convient de vérifier leur bonne utilisation en procédant à des tests et des revues de code.

Si le développement est externalisé, il convient que l'organisation obtienne l'assurance que les tiers se conforment à ces règles de développement sécurisé.

16.2.2 Procédures de contrôle des changements apportés au système

L'organisation doit contrôler les changements apportés au système dans le cycle de développement en utilisant des procédures formelles de contrôle des changements.

Il convient de documenter des procédures formelles de contrôle des changements et d'imposer leur mise en œuvre, afin de garantir l'intégrité des systèmes, des applications et des produits, à

partir des toutes premières étapes de la conception et tout au long des opérations de maintenance qui s'ensuivent.

Il convient que l'introduction de nouveaux systèmes et les changements de grande ampleur apportés aux systèmes existants suivent une procédure formelle de documentation, de spécification, de phase de tests, de contrôle qualité et de mise en œuvre.

Il convient que ce processus intègre une appréciation du risque, une analyse des incidences du changement et une spécification des mesures de sécurité requises. Il convient que ce processus garantisse également que les procédures de sécurité et de contrôle existantes ne sont pas compromises, que les programmeurs chargés de l'assistance n'ont accès qu'aux parties du système nécessaires pour leur permettre d'effectuer leur travail et que tout changement fait l'objet d'un accord formel.

Le cas échéant, il convient d'intégrer les procédures de contrôle des changements et des applications.

Il convient que les procédures de changement prévoient, sans s'y limiter :

a) la tenue à jour d'un enregistrement des niveaux d'autorisation accordés;

b) de veiller à ce que les propositions de changements émanent d'utilisateurs autorisés;

c) de revoir les commandes et les procédures d'intégrité afin de s'assurer qu'elles ne seront pas compromises par les changements;

d) d'identifier tout logiciel, information, élément de base de données et matériel nécessitant un changement;

e) d'identifier et de vérifier le code de sécurité critique pour réduire au minimum la probabilité des risques liés aux failles de sécurité connues;

f) d'obtenir un accord formel pour les propositions détaillées avant le lancement des travaux;

g) de s'assurer que les utilisateurs autorisés acceptent les changements avant leur mise en œuvre;

h) de veiller à la mise à jour de la documentation système après chaque changement, et à l'archivage ou la mise au rebut de l'ancienne documentation;

i) de tenir à jour un contrôle de version pour toutes les mises à jour logicielles;

j) de tenir à jour un système de traçabilité de toutes les demandes de changement;

k) de veiller à ce que la documentation du système d'exploitation et les procédures utilisateurs soient adaptées en fonction des changements;

l) de veiller à programmer la mise en œuvre des changements en temps voulu, de manière à ne pas perturber les activités de l'organisation.

Un changement apporté aux logiciels peut avoir une incidence sur l'environnement en exploitation et vice-versa.

Les bonnes pratiques prévoient que la phase de test d'un nouveau logiciel soit réalisée dans un environnement isolé des environnements de production et de développement. Ce cloisonnement permet de contrôler le nouveau logiciel et d'ajouter une protection supplémentaire aux

informations d'exploitation utilisées dans le cadre des tests. Il convient que ces dispositions intègrent les correctifs logiciels, les « service packs » (ensembles de modifications provisoires) et autres mises à jour.

Lorsqu'il est envisagé d'appliquer des mises à jour automatiques, il convient d'évaluer les risques pour l'intégrité et la disponibilité du système par rapport aux avantages d'un déploiement rapide de mises à jour.

Il convient de ne pas mettre en œuvre des mises à jour automatisées sur des systèmes critiques, car certaines mises à jour sont susceptibles de faire échouer des applications critiques.

16.2.3 Revue technique des applications après changement apporté à la plateforme d'exploitation

Lorsque des changements sont apportés aux plateformes d'exploitation, l'organisation doit revoir et tester les applications critiques métier afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.

Il convient que ce processus prévoit :

a) la revue des procédures de contrôle et d'intégrité des applications afin de s'assurer qu'elles n'ont pas été compromises par les changements apportés à la plateforme d'exploitation;

b) de veiller à ce que les changements apportés à la plateforme d'exploitation soient notifiés en temps opportun, afin que les tests et revues appropriés soient réalisés avant leur mise en œuvre;

c) de veiller à ce que les plans de continuité de l'activité soient modifiés en conséquence.

Les plateformes d'exploitation incluent les systèmes d'exploitation, les bases de données et les logiciels médiateurs. Il convient que la mesure s'applique également aux changements apportés aux applications.

16.2.4 Restrictions relatives aux changements apportés aux progiciels

Il convient de ne pas encourager la modification des progiciels et de se limiter aux changements nécessaires. Il convient également d'exercer un contrôle strict sur ces changements.

Dans la mesure du possible, il convient de ne pas apporter de changements aux progiciels fournis par l'éditeur.

Lorsqu'une modification du progiciel est nécessaire, il convient de tenir compte des points suivants :

a) le risque de compromettre les commandes intégrées et le processus de vérification de l'intégrité;

b) le fait qu'il convienne ou non d'obtenir le consentement de l'éditeur;

c) la possibilité d'obtenir les changements souhaités auprès de l'éditeur, sous la forme de mises à jour de programme classiques;

d) les conséquences si l'organisation devenait responsable de la maintenance du logiciel suite à des changements;

e) la compatibilité avec les autres logiciels en service.

Lorsque des changements s'avèrent nécessaires, il convient de conserver le logiciel original et d'appliquer ces changements à une copie clairement identifiée.

Il convient d'appliquer une politique de gestion des mises à jour afin que tous les logiciels autorisés bénéficient des versions et des correctifs logiciels les plus récents.

Il convient de tester avec soin et de documenter tous les changements apportés afin de pouvoir les réappliquer aux versions ultérieures, le cas échéant. Si nécessaire, il convient que les changements apportés soient testés et validés par un organisme indépendant.

16.2.5 Principes d'ingénierie de la sécurité des systèmes

L'organisation doit établir, documenter, tenir à jour et appliquer des principes d'ingénierie de la sécurité des systèmes à tous les travaux de mise en œuvre de systèmes d'information.

Il convient d'établir, de documenter et d'appliquer des procédures d'ingénierie de la sécurité des systèmes d'information, reposant sur les principes d'ingénierie de la sécurité, aux activités internes d'ingénierie des systèmes d'information.

Il convient de concevoir la sécurité à tous les niveaux de l'architecture (activité, données, applications et technologie) en préservant l'équilibre entre la nécessité d'une sécurité de l'information et la nécessité de son accessibilité.

Il convient d'analyser les nouvelles technologies au regard des risques de sécurité et il convient de revoir la conception par rapport aux modèles d'attaques connus.

Il convient de revoir régulièrement ces principes et les procédures d'ingénierie établies pour s'assurer qu'ils contribuent de manière efficace à l'amélioration des normes de sécurité liées au processus d'ingénierie.

Il convient également de les revoir régulièrement pour s'assurer qu'ils restent d'actualité pour combattre toute nouvelle menace potentielle et continuent de s'appliquer aux avancées réalisées dans les technologies et les solutions appliquées.

S'il y a lieu, il convient d'appliquer les principes d'ingénierie de la sécurité aux systèmes d'information externalisés par le biais de contrats et autres accords exécutoires passés entre l'organisation et le prestataire auprès duquel l'organisation externalise ses systèmes. Il convient que l'organisation confirme que les principes d'ingénierie de la sécurité du prestataire ont la même rigueur que ses propres principes.

16.2.6 Environnement de développement sécurisé

Il convient que les organisations doivent établir un environnement de développement sécurisé pour les tâches de développement et d'intégration du système, qui englobe l'intégralité du cycle de développement du système, et qu'ils en assurent la protection de manière appropriée.

Un environnement de développement sécurisé englobera les personnes, les processus et la technologie associés au développement et à l'intégration du système.

Il convient que les organisations apprécient les risques liés aux tâches individuelles de développement du système et établissent des environnements de développement sécurisés pour des tâches spécifiques de développement du système en tenant compte :

a) de la sensibilité des données à traiter, stocker et transférer par le système;

b) des exigences internes et externes applicables, découlant par exemple de règlements ou de politiques;

c) des mesures de sécurité déjà mises en œuvre par l'organisation qui appuieront la tâche de développement du système;

d) du niveau de fiabilité du personnel travaillant dans l'environnement;

e) du degré d'externalisation associé à la tâche de développement du système;

f) de la nécessité d'opérer un cloisonnement entre différents environnements de développement: du contrôle de l'accès à l'environnement de développement;

g) du contrôle de l'accès à l'environnement de développement;

h) de la surveillance des changements apportés à l'environnement et au code qu'il renferme;

i) du stockage des sauvegardes à des emplacements sécurisés hors site;

j) du contrôle des déplacements de données à partir de l'environnement et vers l'environnement.

Une fois le niveau de protection déterminé pour un environnement de développement spécifique, il convient que les organisations documentent les processus correspondants dans des procédures de développement sécurisé et les fournissent à toutes les personnes en ayant besoin.

16.2.7 Développement externalisé

Il convient que l'organisation devra superviser et contrôler l'activité de développement du système externalisé.

Lorsqu'un développement de système est externalisé, il convient de considérer les aspects suivants au sein de la chaîne d'approvisionnement de l'organisation :

a) accords de licence, propriété du code et droits de propriété intellectuelle relatifs au contenu externalisé;

b) exigences contractuelles relatives à la conception sécurisée, au codage et aux pratiques de tests;

c) fourniture au développeur prestataire du modèle des menaces approuvé;

d) test de conformité de la qualité et de la précision des livrables;

e) communication des preuves montrant que les seuils de sécurité ont été utilisés pour établir les niveaux minimums acceptables en matière de qualité de la sécurité et de la confidentialité des données personnelles;

f) communication des preuves montrant qu'il a été procédé à suffisamment de tests pour garantir l'absence de contenus volontairement ou involontairement malveillants à la livraison;

g) communication des preuves montrant qu'il a été procédé à suffisamment de tests pour garantir l'absence de vulnérabilités connues;

h) accords de séquestre, par exemple si le code source n'est plus disponible;

i) droit contractuel de procéder à un audit des processus et des contrôles de développement;

j) documentation efficace sur l'environnement servant à créer les livrables;

k) l'organisation demeure responsable de la conformité aux lois en vigueur et de la vérification

de l'efficacité des mesures.

16.2.8 Phase de test de la sécurité du système

L'organisation doit réaliser les tests de fonctionnalité de la sécurité pendant le développement.

Les systèmes, nouveaux et mis à jour, nécessitent d'être soumis à des tests et à des vérifications rigoureux pendant les processus de développement, requérant la mise en place d'un programme détaillé des tâches et des données de test d'entrée, avec les résultats attendus en sortie sous un certain nombre de conditions.

En ce qui concerne les développements in situ, il convient que ces tests soient réalisés dès le début par l'équipe de développement. Ensuite, il convient de procéder à des tests de conformité indépendants (à la fois pour les développements in situ et externalisés) pour garantir que le système fonctionne comme prévu et uniquement comme prévu. Il convient que l'étendue du programme de test soit cohérente avec l'importance et la nature du système.

16.2.9 Test de conformité du système

Il convient de déterminer des programmes de test de conformité et des critères associés pour les nouveaux systèmes d'information, les mises à jour et les nouvelles versions.

Il convient que les tests de conformité du système testent les exigences liées à la sécurité de l'information et le respect des pratiques de développement sécurisé des systèmes.

Il convient que des tests soient également menés sur les systèmes intégrés et les composants reçus. Les organisations peuvent recourir à des outils automatiques, tels que des outils d'analyse de code ou des scanneurs de vulnérabilités : il convient qu'elles vérifient les actions correctives apportées aux défauts liés à la sécurité.

Il convient de réaliser les tests dans un environnement réaliste pour garantir que le système n'introduira pas de vulnérabilités dans l'environnement de l'organisation et que les tests sont fiables.

16.3 Données de test

Chaque organisation doit garantir la protection des données utilisées pour les tests.

16.3.1 Protection des données de test

Il convient que les données de test soient sélectionnées avec soin, protégées et contrôlées.

Dans le cadre de tests, il convient d'éviter d'utiliser des données d'exploitation contenant de l'information personnelle ou toute autre information confidentielle. Si une information personnelle ou toute autre information confidentielle est utilisée dans le cadre de tests, il convient de supprimer tous les détails et contenus sensibles ou de les modifier.

Lorsque des données d'exploitation sont utilisées pour les besoins d'un test, il convient d'appliquer les lignes directrices suivantes afin de les protéger :

a) il convient que les procédures de contrôle d'accès, qui s'appliquent aux systèmes d'applications en exploitation, s'appliquent également aux systèmes d'applications de test;

b) il convient d'obtenir une nouvelle autorisation chaque fois qu'une information d'exploitation

est copiée dans un environnement de test;

c) il convient d'effacer les informations d'exploitation d'un environnement de test immédiatement après la fin des tests;

d) il convient de journaliser toute reproduction et utilisation de l'information d'exploitation, afin de créer un système de traçabilité.

Les tests de système et de conformité nécessitent généralement d'importants volumes de données de test qui soient aussi représentatives que possible des données d'exploitation.

17. Relations avec les fournisseurs (D13)

17.1 Sécurité de l'information dans les relations avec les fournisseurs

Caque organisation doit garantir la protection de ses actifs accessibles aux fournisseurs.

17.1.1 Politique de sécurité de l'information dans les relations avec les fournisseurs

L'organisation doit convenir avec le fournisseur les exigences de sécurité de l'information pour limiter les risques résultant de l'accès du fournisseur aux actifs de l'organisation et de les documenter.

Il convient que les organisations établissent une politique identifiant et imposant des mesures de sécurité spécifiques aux accès des fournisseurs à l'information de l'organisation. Il convient que ces mesures tiennent compte des processus et des procédures mis en œuvre par l'organisation, ainsi que des processus et des procédures qu'il convient que l'organisation demande au fournisseur de mettre en œuvre, notamment :

a) l'identification et la documentation du type de fournisseurs, par exemple services informatiques, services logistiques, services financiers, composants de l'infrastructure informatique, auxquels l'organisation accordera un accès à son information;

b) un processus et un cycle normalisés de gestion des relations avec les fournisseurs;

c) une définition des types d'accès à l'information que les différents types de fournisseurs se verront accorder, ainsi qu'une surveillance et un contrôle de ces accès;

d) les exigences minimales de sécurité de l'information pour chaque type d'information et chaque type d'accès servant de fondement aux accords conclus avec chaque fournisseur, qui reposeront sur les besoins et les exigences de l'organisation et son profil de risque;

e) les processus et les procédures permettant de surveiller la conformité aux exigences de sécurité de l'information établies pour chaque type de fournisseur et chaque type d'accès, incluant une revue et une validation des produits par une tierce partie;

f) des contrôles de précision et d'exhaustivité pour garantir l'intégrité de l'information ou du traitement de l'information assurés par l'une ou l'autre partie;

g) les types d'obligations applicables aux fournisseurs pour protéger l'information de l'organisation;

h) le traitement des incidents et des impondérables associés aux accès fournisseurs,

incluant les responsabilités de l'organisation et celles des fournisseurs;

i) les dispositions de résistance et, si nécessaire, de récupération et de secours pour garantir la disponibilité de l'information ou du traitement de l'information assurés par l'une ou l'autre partie;

j) une formation à la sensibilisation aux politiques, aux processus et aux procédures applicables pour le personnel de l'organisation impliqué dans les achats;

k) une formation à la sensibilisation du personnel de l'organisation en interaction avec le personnel du fournisseur, sur les règles appropriées d'engagement et de comportement en fonction du type de fournisseur et du niveau d'accès du fournisseur aux systèmes et à l'information de l'organisation;

l) les conditions dans lesquelles les exigences et les mesures de sécurité de l'information seront documentées dans un accord signé par les deux parties;

m) la gestion des transitions nécessaires de l'information, des moyens de traitement de l'information et tout ce qui transite en général, et l'assurance que la sécurité de l'information est maintenue tout au long de la période de transition.

17.1.2 La sécurité dans les accords conclus avec les fournisseurs

Il convient que les exigences applicables liées à la sécurité de l'information soient établies et convenues avec chaque fournisseur pouvant avoir accès, traiter, stocker, communiquer ou fournir des composants de l'infrastructure informatique destinés à l'information de l'organisation.

Il convient de rédiger et de documenter les accords de fournisseur de sorte à s'assurer qu'il n'y ait aucun malentendu entre l'organisation et le fournisseur concernant les devoirs des deux parties à répondre aux exigences de sécurité de l'information applicables.

Pour répondre aux exigences de sécurité de l'information identifiées, il convient d'envisager d'inclure les conditions suivantes dans l'accord :

a) description de l'information à fournir ou à laquelle l'accès doit être rendu possible et des méthodes utilisées pour fournir ces informations ou y accéder;

b) la classification de l'information selon le plan de classification de l'organisation (voir 8.2): si nécessaire, en outre, la mise en correspondance du plan de classification de l'organisation et du plan de classification du fournisseur;

c) les exigences légales et réglementaires, y compris la protection des données, les droits de propriété intellectuelle et les droits d'auteur, et la description de la méthode servant à garantir qu'elles sont respectées;

d) obligation pour chaque partie au contrat de mettre en œuvre un ensemble convenu de contrôles, incluant le contrôle d'accès, la revue des performances, la surveillance, la rédaction de rapport et l'audit;

e) les règles d'utilisation acceptable de l'information, y compris, si nécessaire, les conditions d'utilisation inacceptables;

f) soit une liste explicite des salariés du fournisseur autorisés à recevoir ou à accéder à l'information de l'organisation, soit des procédures ou conditions liées à l'octroi et au retrait d'autorisations pour l'accès à l'information de l'organisation ou la réception d'information de l'organisation à destination des salariés du fournisseur;

g) les politiques de sécurité de l'information pertinentes pour le contrat spécifique;

h) les exigences et les procédures de gestion des incidents (notamment la notification et la collaboration lors de l'action corrective);

i) les exigences de formation et de sensibilisation aux procédures spécifiques et aux exigences de sécurité de l'information, par exemple la réponse aux incidents, les procédures d'autorisation;

j) les règlementations à prendre en compte concernant la sous-traitance, y compris les mesures qu'il est nécessaire de mettre en œuvre;

k) les partenaires signataires de l'accord, avec une personne de contact pour les questions de sécurité liées à l'information;

l) les exigences de sélection, le cas échéant, des salariés du fournisseur, incluant les responsabilités liées aux procédures de sélection et de notification si la sélection n'a pas abouti ou si les résultats sont source d'inquiétude ou de doute;

m) le droit d'auditer les processus et les mesures de sécurité du fournisseur en rapport avec le contrat;

n) les processus de résolution des défauts et de résolution des conflits;

o) l'obligation du fournisseur à communiquer périodiquement un rapport indépendant sur l'efficacité des mesures et son accord pour apporter en temps opportun les actions correctives aux problèmes soulevés dans le rapport;

p) l'obligation du fournisseur à se conformer aux exigences de sécurité de l'organisation.

Les accords peuvent différer considérablement d'une organisation à l'autre et selon les types de fournisseurs.

Il convient, par conséquent, de veiller à bien inclure tous les risques et toutes les exigences pertinentes liés à la sécurité de l'information. Les accords conclus avec les fournisseurs peuvent également impliquer d'autres parties (par exemple des sous-traitants).

17.1.3 Chaine d'approvisionnement informatique

L'organisation doit conclure les accords avec les fournisseurs qui incluent des exigences sur le traitement des risques de sécurité de l'information associés à la chaîne d'approvisionnement des produits et des services informatiques.

Il convient d'étudier l'intégration aux accords des fournisseurs des aspects suivants relatifs à la sécurité de la chaîne d'approvisionnement :

a) la définition des exigences de sécurité de l'information à appliquer à l'achat de produits ou de services informatiques, en plus des exigences de sécurité de l'information générales applicables aux relations avec les fournisseurs;

b) en ce qui concerne les services informatiques, l'obligation pour les fournisseurs de diffuser les exigences de sécurité de l'organisation jusqu'au dernier maillon de la chaîne d'approvisionnement si le fournisseur sous-traite des parties des services informatiques qu'il fournit à l'organisation;

c) en ce qui concerne les produits informatiques, l'obligation pour les fournisseurs de diffuser les pratiques de sécurité appropriées jusqu'au dernier maillon de la chaîne d'approvisionnement si ces produits comportent des composants achetés chez d'autres

fournisseurs;

d) la mise en œuvre d'un processus de surveillance et de méthodes acceptables permettant de confirmer que les produits et les services informatiques livrés respectent les exigences de sécurité stipulées;

e) la mise en œuvre d'un processus d'identification des composants d'un produit ou d'un service critiques pour le maintien des fonctionnalités et qui nécessitent, par conséquent, plus d'attention et de soins lorsqu'ils sont élaborés en dehors de l'organisation, notamment si le fournisseur principal sous-traite certains aspects des composants du produit ou du service à d'autres fournisseurs;

f) la garantie que les composants critiques et leur origine peuvent être tracés tout au long de la chaîne d'approvisionnement;

g) la garantie que les produits informatiques livrés fonctionnent comme prévu et ne présentent aucune fonctionnalité inattendue ou indésirable;

h) la définition de règles de partage de l'information concernant la chaîne d'approvisionnement et tous les problèmes et compromis possibles entre l'organisation et les fournisseurs;

i) la mise en œuvre de processus spécifiques de gestion du cycle de vie des composants informatiques et de leur disponibilité, ainsi que les risques associés liés à la sécurité. Cela inclut la gestion des risques présentés par la rupture de stock de composants, les fournisseurs ayant cessé leur activité ou ayant arrêté de produire ces composants en raison des avancées technologiques.

Les pratiques spécifiques de gestion des risques de la chaîne d'approvisionnement informatique consolident les pratiques générales de sécurité de l'information, de qualité, de gestion de projet et d'ingénierie de systèmes, mais ne les remplacent pas.

Il est conseillé aux organisations de travailler avec les fournisseurs pour appréhender la chaîne d'approvisionnement informatique et tous les éléments qui présentent des conséquences importantes sur les produits et les services à fournir.

Les organisations peuvent influer sur les pratiques en matière de sécurité de l'information dans les chaînes d'approvisionnement informatique, en stipulant clairement dans les accords conclus avec les fournisseurs les problèmes qu'il convient que d'autres fournisseurs de la chaîne d'approvisionnement informatique résolvent.

La chaîne d'approvisionnement informatique étudiée ici intègre les services d'informatique en nuage.

17.2 Gestion de la prestation du service

Chaque organisation doit maintenir un niveau convenu de sécurité de l'information et de prestation de services, conformément aux accords conclus avec les fournisseurs.

17.2.1 Surveillance et revue des services des fournisseurs

Il convient que les organisations surveillent, revoient et auditent à intervalles réguliers la prestation des services assurés par les fournisseurs.

Il convient que la surveillance et la revue des services des fournisseurs garantissent que les conditions générales sur la sécurité de l'information prévues dans les accords sont respectées et que les incidents et les problèmes liés à la sécurité de l'information sont gérés correctement.

Il convient qu'il existe, à cet effet, un processus relationnel de gestion des services entre l'organisation et le fournisseur en vue de :

a) surveiller les niveaux de performance des services et vérifier ainsi qu'ils sont conformes aux accords;

b) revoir les rapports de service produits par le fournisseur et organiser des réunions régulières sur l'avancement comme l'exigent les accords;

c) mener des audits des fournisseurs conjointement à la revue de rapports d'audits indépendants, s'ils existent, et assurer un suivi des problèmes identifiés;

d) fournir l'information relative aux incidents liés à la sécurité de l'information et assurer une revue de cette information comme l'exigent les accords et toutes les lignes directrices et procédures d'accompagnement;

e) revoir les systèmes de traçabilité et les enregistrements du fournisseur concernant les événements liés à la sécurité de l'information, les problèmes d'exploitation, les défaillances et le suivi des pannes et des interruptions liées au service fourni;

f) résoudre et gérer tout problème identifié;

g) revoir les aspects liés à la sécurité de l'information dans les relations du fournisseur avec ses propres fournisseurs;

h) s'assurer que le fournisseur maintient une capacité de service suffisante ainsi que des plans exploitables conçus pour garantir le maintien du niveau de continuité de service convenu en cas de défaillance majeure du service ou de sinistre.

Il convient d'attribuer la responsabilité de la gestion des relations avec les fournisseurs à une personne désignée ou à une équipe de gestion des services. En outre, il convient que l'organisation s'assure que les fournisseurs nomment les personnes chargées de contrôler le respect et l'application des exigences stipulées dans les accords.

Il convient de prévoir les compétences et ressources techniques suffisantes pour veiller à ce que les exigences du contrat, et en particulier celles qui traitent de la sécurité de l'information, sont respectées.

Il convient de prendre les mesures adéquates lorsque des insuffisances sont observées dans la prestation du service.

Il convient que l'organisation conserve une visibilité et un contrôle global suffisant sur tous les aspects de la sécurité ayant trait à l'information ou aux moyens de traitement de l'information sensible ou critique auxquels le fournisseur a accès, qu'il traite ou qu'il gère.

Il convient que l'organisation veille à conserver, par un processus de signalement défini, une visibilité sur les activités liées à la sécurité, telles que la gestion des changements, l'identification des vulnérabilités et le signalement des incidents liés à la sécurité de l'information et les réponses qui y sont apportées.

17.2.2 Gestion des changements apportés dans les services des fournisseurs

L'organisation doit gérer les changements effectués dans les prestations de service des fournisseurs, y compris le maintien et l'amélioration des politiques, procédures et mesures

existant en matière de sécurité de l'information, en tenant compte du caractère critique de l'information, des systèmes et des processus concernés et de la réappréciation du risque.

Il convient de tenir compte des facteurs suivants :

a) les changements apportés aux accords passés avec les fournisseurs;

b) les changements effectués par l'organisation pour mettre en œuvre:

   1) des améliorations aux services offerts;

   2) le développement d'applications et de systèmes nouveaux;

   3) des changements ou des mises à jour des politiques et des procédures de l'organisation;

   4) des mesures nouvelles ou modifiées permettant de résoudre les incidents liés à la sécurité de l'information et d'améliorer la sécurité;

c) les changements dans les services assurés par les fournisseurs pour mettre en œuvre:

   1) des changements et des améliorations apportées aux réseaux;

   2) l'utilisation de nouvelles technologies;

   3) l'adoption de nouveaux produits ou des versions/des éditions plus récentes;

   4) des outils et des environnements de développement nouveaux;

   5) des changements apportés à l'emplacement physique des équipements de dépannage;

   6) des changements de fournisseurs;

   7) la sous-traitance à un autre fournisseur.

18. Gestion des incidents liés à la sécurité de l'information (D14)

18.1 Gestion des incidents liés à la sécurité de l'information et améliorations

Chaque organisation doit garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information, incluant la communication des événements et des failles liés à la sécurité.

18.1.1 Responsabilités et procédures

L'organisation doit établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.

Il convient d'examiner les recommandations suivantes en matière de responsabilités et de procédures de gestion des incidents liés à la sécurité de l'information :

a) il convient d'établir des responsabilités de gestion pour garantir que les procédures suivantes sont développées et communiquées de manière adéquate au sein de l'organisation :

   1) procédures de planification et de préparation des réponses aux incidents ;

   2) procédures de surveillance, de détection, d'analyse et de signalement des événements

et des incidents liés à la sécurité de l'information ;

3) procédures de journalisation des activités de gestion des incidents ;

4) procédures de traitement des preuves scientifiques ;

5) procédures d'appréciation et de prise de décision relatives aux événements liés à la sécurité de l'information et d'appréciation des failles liées à la sécurité de l'information ;

6) procédures de réponse, incluant les procédures de remontée d'information, de récupération contrôlée de l'incident et de communication aux organisations ou aux personnes internes ou extérieures à l'organisation ;

b) il convient que les procédures établies garantissent :

1) qu'un personnel compétent au sein de l'organisation traite les questions relatives aux incidents liés à la sécurité de l'information ;

2) qu'un point de contact pour la détection et le signalement des incidents liés à la sécurité existe ;

3) que des contacts appropriés sont entretenus avec les autorités, les groupes d'intérêts externes ou les forums qui traitent des questions relatives aux incidents liés à la sécurité de l'information.

c) il convient que les procédures de signalement prévoient :

1) des formulaires spécifiques destinés à faciliter le signalement, récapitulant toutes les actions à mettre en œuvre lorsqu'un événement lié à la sécurité de l'information est détecté ;

2) la procédure à engager lorsqu'un événement lié à la sécurité de l'information se produit, à savoir: noter immédiatement tous les détails (par exemple le type de non-conformité ou de défaillance, le dysfonctionnement constaté, les messages apparaissant à l'écran) et en informer immédiatement le responsable servant de point de contact et n'exécuter que des actions concertées;

3) une référence à un processus disciplinaire formel pour les salariés ayant enfreint les règles de sécurité;

4) des processus de retour d'information adéquats, afin de communiquer les détails de la résolution du problème aux personnes ayant signalé un événement, une fois que le problème a été réglé et clôturé.

Il convient que les objectifs de la gestion des incidents liés à la sécurité de l'information fassent l'objet d'un accord avec la direction. Il convient également de s'assurer que les personnes responsables de la gestion des incidents liés à la sécurité de l'information connaissent les priorités de l'organisation dans ce domaine.

18.1.2 Signalement des événements liés à la sécurité de l'information

Il convient de signaler, dans les meilleurs délais, les événements liés à la sécurité de l'information, par les voies hiérarchiques appropriées.

Il convient d'informer tous les salariés et contractants de leur obligation de signaler les événements liés à la sécurité de l'information dans les meilleurs délais. Il convient de les informer de l'existence d'une procédure de signalement des événements liés à la sécurité de l'information et d'un responsable servant de point de contact auprès duquel effectuer le signalement.

Aussi les éventuels dysfonctionnements ou autres comportements anormaux du système peuvent révéler une attaque ou une brèche dans la sécurité et il convient, par conséquent, de toujours signaler ces phénomènes comme des événements liés à la sécurité de l'information.

18.1.3 Signalement des failles liées à la sécurité de l'information

Il convient d'enjoindre tous les salariés et contractants utilisant les systèmes et services d'information de l'organisation à noter et à signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.

Il convient que tous les salariés et contractants signalent ce type de problème au responsable servant de point de contact dans les meilleurs délais, afin d'éviter des incidents liés à la sécurité de l'information. Il convient que le mécanisme de signalement soit aussi simple, accessible et disponible que possible.

Il convient de recommander aux salariés et contractants de ne pas tenter de démontrer l'existence des failles de sécurité soupçonnées. Rechercher les failles pourrait être interprété comme un mauvais usage potentiel du système. La recherche pourrait en outre endommager le système ou le service d'information et exposer la personne la réalisant à des poursuites judiciaires.

18.1.4 Appréciation des événements liés à la sécurité de l'information et prise de décision

Il convient d'apprécier les événements liés à la sécurité de l'information et de décider s'ils doivent être classés comme incidents liés à la sécurité de l'information.

Il convient que le responsable servant de point de contact apprécie chaque événement lié à la sécurité de l'information en utilisant l'échelle de classification des incidents et des événements liés à la sécurité de l'information convenue et qu'il décide s'il convient de classer l'événement comme tel.

La classification et la hiérarchisation des incidents peuvent permettre d'identifier les conséquences et l'étendue d'un incident.

18.1.5 Réponse aux incidents liés à la sécurité de l'information

Il convient de répondre aux incidents liés à la sécurité de l'information conformément aux procédures documentées.

Il convient que ce soit le responsable servant de point de contact et les autres personnes concernées de l'organisation, ou relevant des tiers, qui répondent aux incidents liés à la sécurité de l'information.

Il convient que la réponse comporte :

a) le recueil de preuves aussitôt que possible après l'incident ;

b) une analyse scientifique de la sécurité de l'information, le cas échéant ;

c) une remontée d'informations, le cas échéant ;

d) l'assurance que toutes les tâches concernant la réponse sont correctement journalisées en vue d'une analyse ultérieure ;

e) la communication de l'existence d'un incident lié à la sécurité de l'information ou de tout détail pertinent qui s'y rapporte aux autres personnes internes et externes à l'organisation

ou aux organisations ayant besoin d'en connaître ;

f) le traitement de la ou des failles constatées dans la sécurité de l'information causant ou contribuant à l'incident ;

g) une fois que l'incident a été résolu avec succès, la clôture formelle de l'incident et son enregistrement. Il convient de procéder à une analyse postérieure à l'incident, le cas échéant, pour identifier la source de l'incident.

Le premier objectif de la réponse à l'incident est de retrouver un « niveau de sécurité normal », puis d'initier la récupération nécessaire.

18.1.6 Tirer des enseignements des incidents liés à la sécurité de l'information

Il convient de tirer parti des connaissances recueillies suite à l'analyse et la résolution des incidents liés à la sécurité de l'information pour réduire la probabilité ou les conséquences d'incidents ultérieurs.

Il convient de mettre en place des mécanismes permettant de quantifier et surveiller les différents types d'incidents liés à la sécurité de l'information, ainsi que leur volume et les coûts associés. Il convient de se servir de l'information recueillie lors de cette évaluation pour identifier les incidents récurrents ou ayant des conséquences graves.

L'évaluation des incidents liés à la sécurité de l'information peut faire apparaître la nécessité d'améliorer les mesures existantes ou d'en créer de nouvelles, afin de limiter la fréquence des futurs incidents, ainsi que les dommages et les coûts associés, ou afin d'intégrer ces mesures dans le processus de revue de la politique de sécurité.

18.2 Recueil de preuves

L''organisation doit définir et appliquer des procédures d'identification, de recueil, d'acquisition et de protection de l'information pouvant servir de preuve.

Il convient de mettre au point et d'appliquer des procédures internes de traitement des preuves dans le cadre d'une action judiciaire et disciplinaire.

Il convient, en général, que les procédures relatives aux preuves prévoient des processus d'identification, de recueil, d'acquisition et de protection selon les différents types de supports, de dispositifs et d'état des dispositifs, par exemple allumé ou éteint. Il convient que les procédures prennent en compte :

a) la chaîne de traçabilité ;

b) la sécurité des preuves ;

c) la sécurité du personnel ;

d) les fonctions et les responsabilités du personnel impliqué ;

e) les aptitudes du personnel ;

f) la documentation ;

g) les séances d'information.

S'il en existe, il convient de rechercher les certifications et autres justificatifs de la qualification du personnel et des outils, de sorte à renforcer la valeur des preuves protégées.

Les preuves scientifiques peuvent dépasser les limites de l'organisation ou les frontières juridictionnelles. Dans ce cas, il convient de s'assurer que l'organisation est habilitée à recueillir les informations devant servir de preuve scientifique.

Il convient de tenir compte des exigences des diverses juridictions afin d'optimiser l'admissibilité de la preuve auprès des juridictions compétentes.

19. *Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité (D15)*

19.1 Continuité de la sécurité de l'information

Chaque organisation doit intégrer la continuité de la sécurité de l'information dans les systèmes de gestion de la continuité de son activité.

19.1.1 Organisation de la continuité de la sécurité de l'information

L'organisation doit déterminer ses exigences en matière de sécurité de l'information et de continuité du management de la sécurité de l'information dans des situations défavorables, comme lors d'une crise ou d'un sinistre.

Il convient que l'organisation détermine si la continuité de la sécurité de l'information est intégrée au processus de gestion de la continuité de l'activité ou au processus de gestion de la récupération après sinistre.

Il convient de déterminer les exigences de sécurité de l'information lors de l'élaboration du programme de récupération en cas de sinistre et de continuité de l'activité.

En l'absence de programme formel de récupération en cas de sinistre et de continuité de l'activité, il convient que le management de la sécurité de l'information parte du principe que les exigences de sécurité de l'information restent les mêmes dans des situations défavorables que dans des conditions d'exploitation normales.

Il est également possible qu'une organisation réalise une analyse de l'impact sur l'activité des aspects liés à la sécurité de l'information pour déterminer les exigences de sécurité de l'information applicables aux situations défavorables.

Afin de réduire le temps passé et les efforts consacrés à une analyse « supplémentaire » d'impact sur l'activité concernant la sécurité de l'information, il est recommandé d'intégrer les aspects de la sécurité de l'information dans l'analyse ordinaire d'impact sur l'activité de la gestion de la continuité de l'activité et de la gestion de la récupération après sinistre.

Cela implique que les exigences de continuité de la sécurité de l'information sont formulées de manière explicite dans les processus de gestion de la continuité de l'activité et de gestion de la récupération après sinistre.

19.1.2 Mise en œuvre de la continuité de la sécurité de l'information

L'organisation doit établir, documenter, mettre en œuvre et maintenir à jour des processus, des procédures et des mesures permettant de garantir le niveau requis de continuité de la sécurité de l'information au cours d'une situation défavorable.

Il convient que l'organisation s'assure :

a) qu'il existe une structure de gestion adéquate pour se préparer, atténuer et réagir à un événement perturbant en mobilisant du personnel possédant l'autorité, l'expérience et les compétences nécessaires;

b) que les membres du personnel chargés de la réponse à apporter aux incidents, et qui possèdent les responsabilités, l'autorité et les compétences nécessaires pour gérer les incidents et maintenir la sécurité de l'information, sont nommées ;

c) qu'il existe des plans documentés, des procédures de réponse et de récupération approuvés, détaillant la manière dont l'organisation gère un événement perturbant et maintient la sécurité de son information à un niveau prédéterminé, reposant sur des objectifs de continuité de la sécurité de l'information approuvés par la direction.

Conformément aux exigences de continuité de la sécurité de l'information, il convient que l'organisation établisse, documente, mette en œuvre et tienne à jour :

a) des mesures de sécurité de l'information intégrées aux processus de continuité de l'activité ou de récupération après un sinistre, aux procédures et aux outils et systèmes associés ;

b) des processus, des procédures et des changements à mettre en œuvre pour maintenir les mesures de sécurité de l'information existantes lors d'une situation défavorable ;

c) des mesures destinées à contrebalancer les mesures de sécurité de l'information qu'il est impossible de maintenir dans une situation défavorable.

Dans le contexte de la continuité de l'activité ou de la récupération après un sinistre, des processus et des procédures spécifiques ont pu être définis. Il convient de protéger l'information manipulée dans le cadre de ces processus et de ces procédures ou dans le cadre de systèmes d'information dédiés à cet effet.

Il convient que l'organisation fasse appel à des spécialistes de la sécurité de l'information lorsqu'elle établit, met en œuvre et maintient à jour des processus de continuité de l'activité ou de récupération après un sinistre et des procédures.

Il convient que les mesures de sécurité de l'information mises en œuvre continuent d'opérer lors d'une situation défavorable. Si les mesures de sécurité ne sont pas en mesure de maintenir la sécurité de l'information, il convient d'établir, de mettre en œuvre et de maintenir d'autres mesures en vue de conserver un niveau acceptable de sécurité de l'information.

19.1.3 Vérifier, revoir et évaluer la continuité de la sécurité de l'information

Il convient que l'organisation vérifie à intervalles réguliers les mesures de continuité de la sécurité de l'information déterminées et mises en œuvre, afin que s'assurer qu'elles restent valables et efficaces dans des situations défavorables.

Les changements organisationnels, techniques, liés aux procédures et aux processus, que ce soit dans le contexte habituel d'exploitation ou dans un contexte de continuité, peuvent entraîner des changements dans les exigences de continuité de la sécurité de l'information. Dans ce cas, il convient de revoir la continuité des processus, des procédures et des mesures de la sécurité de l'information en tenant compte des changements apportés aux exigences.

Il convient que les organisations vérifient la continuité de management de la sécurité de l'information :

a) en exerçant et en testant les fonctionnalités des processus, des procédures et des mesures de continuité de la sécurité de l'information pour s'assurer qu'elles sont cohérentes avec les objectifs de continuité de la sécurité de l'information;

b) en exerçant et en testant les connaissances et les tâches de routine pour appliquer les processus, les procédures et les mesures de continuité de la sécurité de l'information afin de s'assurer que leurs performances sont cohérentes avec les objectifs de continuité de la sécurité de l'information;

c) en revoyant la validité et l'efficacité des mesures de continuité de la sécurité de l'information lorsque les systèmes d'information, les processus, les procédures et les mesures de sécurité de l'information ou les solutions et les processus de gestion de la continuité de l'activité/gestion de la récupération après sinistre connaissent des changements.

La vérification des mesures de continuité de la sécurité de l'information diffère des tests généraux et de la vérification de la sécurité de l'information. Il convient qu'elle soit réalisée en dehors des tests concernant les changements. Il est préférable, dans la mesure du possible, d'intégrer la vérification des mesures de continuité de la sécurité de l'information aux tests de continuité de l'activité de l'organisation ou de récupération après un sinistre.

19.2 Redondances

Chaque organisation doit garantir la disponibilité des moyens de traitement de l'information.

19.2.1 Disponibilité des moyens de traitement de l'information

Il convient de mettre en œuvre des moyens de traitement de l'information avec suffisamment de redondances pour répondre aux exigences de disponibilité.

Il convient que les organisations identifient les exigences de l'activité en matière de disponibilité des systèmes d'information.

Il convient de tester les systèmes d'information redondants pour s'assurer que le basculement d'un composant à un autre fonctionne comme prévu.

La mise en œuvre de redondances peut entraîner des risques pour l'intégrité ou la confidentialité de l'information et des systèmes d'information, qu'il est nécessaire d'étudier à la conception des systèmes d'information.

20. Conformité (D16)

20.1 Conformité aux obligations légales et réglementaires

Chaque organisation doit éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité.

20.1.1 Identification de la législation et des exigences contractuelles applicables

Il convient, pour chaque système d'information et pour l'organisation elle-même, de définir, documenter et mettre à jour explicitement toutes les exigences légales, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisation pour satisfaire à ces exigences.

De la même façon, il convient de définir et de documenter les mesures spécifiques et les responsabilités individuelles mises en place pour répondre à ces exigences.

Il convient que les responsables identifient toutes les législations applicables à l'organisation afin de répondre aux exigences liées à leur type d'activité. Si l'organisation mène des activités dans d'autres pays, il convient que les responsables étudient la conformité aux règles des pays concernés.

20.1.2 Droits de propriété intellectuelle

Il convient de mettre en œuvre des procédures appropriées visant à garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives aux droits de propriété intellectuelle et à l'utilisation de logiciels propriétaires.

Il convient de prendre en compte les directives suivantes en vue de protéger tout matériel pouvant être soumis à des droits de propriété intellectuelle :

a) publier une politique de conformité relative aux droits de propriété intellectuelle définissant l'utilisation légale des logiciels et des produits liés à l'information;

b) acquérir des logiciels uniquement à partir de sources connues et réputées afin de s'assurer du respect des droits d'auteur;

c) maintenir la sensibilisation aux politiques appliquées en matière de protection des droits de propriété intellectuelle et prévenir le personnel de l'intention de prendre des mesures disciplinaires à l'encontre des personnes enfreignant cette politique;

d) tenir à jour des registres des actifs appropriés et identifier tous les actifs soumis à des exigences de protection des droits de propriété intellectuelle;

e) conserver les preuves tangibles de la propriété des licences, des disques maîtres, des manuels, etc.;

f) mettre en œuvre des contrôles permettant de s'assurer que le nombre maximal d'utilisateurs autorisé par la licence n'est pas dépassé;

g) effectuer des revues permettant de s'assurer que seuls des logiciels autorisés et sous licence sont installés;

h) mettre en œuvre une politique de gestion des conditions de licence appropriées;

i) mettre en œuvre une politique permettant de céder des logiciels ou de les transmettre à des tiers;

j) se conformer aux conditions générales régissant les logiciels et l'information obtenus à partir des réseaux publics;

k) ne pas reproduire, convertir dans un autre format ou extraire de l'information à partir d'enregistrements du commerce (film, enregistrement audio) en dehors de ce qui est permis par la législation sur les droits d'auteur;

l) ne pas copier, intégralement ou en partie, des livres, articles, rapports ou autres documents en dehors de ce qui est permis par la législation sur les droits d'auteur.

Les droits de propriété intellectuelle incluent les droits d'auteur régissant les logiciels et les documents, les droits des dessins et modèles, les marques, les brevets et les licences régissant le code source. Les logiciels propriétaires sont généralement dotés d'une licence d'utilisation stipulant les conditions générales de la licence, telles que la limitation de l'utilisation des produits à des ordinateurs spécifiques ou la limitation de la reproduction à la seule création de copies de sauvegarde.

Il convient que l'importance des droits de propriété intellectuelle soit communiquée à l'équipe responsable du logiciel développé par l'organisation, et qu'elle soit sensibilisée à ces droits.

Les exigences légales, réglementaires et contractuelles peuvent restreindre la copie du matériel propriétaire. Les exigences applicables peuvent notamment stipuler que seul un matériel développé par l'organisation ou un matériel pour lequel l'organisation dispose de licences, ou encore qui est fourni par un développeur à l'organisation, peut être utilisé. La violation des droits d'auteur peut déclencher une action judiciaire pouvant aboutir à des poursuites pénales.

20.1.3 Protection des enregistrements

Il convient de protéger les enregistrements de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisées conformément aux exigences légales, réglementaires, contractuelles et aux exigences métier.

Au moment de décider de la protection spécifique des enregistrements de l'organisation, il convient de tenir compte de leur classification, proposée par le plan de classification de l'organisation. Il convient de classer les enregistrements par types, tels que documents comptables, enregistrements de base de données, journaux de transactions, journaux d'audit et procédures d'exploitation ; chaque type comporte des détails sur les périodes de conservation et le type de support de stockage permis, par exemple papier, microfiche, support magnétique, support optique.

Il convient également de stocker les clés cryptographiques qui s'y rapportent et les programmes associés à des archives ou des signatures électroniques chiffrées, afin de permettre le déchiffrement des enregistrements pendant leur durée de conservation.

Il convient d'envisager l'éventualité d'une dégradation du support utilisé pour le stockage des enregistrements. Il convient de mettre en œuvre les procédures de stockage et de manipulation conformément aux recommandations du fabricant.

Si le choix se porte sur des supports de stockage électroniques, il convient d'établir des procédures visant à garantir l'accès aux données (lisibilité du support et du format) tout au long de la période de conservation afin de protéger les données contre toute perte due à l'évolution de la technologie.

Il convient de choisir les systèmes de stockage des données de sorte qu'ils permettent la récupération des données requises dans un délai raisonnable et sous un format lisible selon les exigences à respecter.

Il convient que le système de stockage et de manipulation garantisse l'identification des enregistrements et de leur durée de conservation telles que définies par la législation nationale ou régionale ou par les réglementations, le cas échéant.

Il convient que ce système permette la destruction appropriée des enregistrements à l'issue de cette période si l'organisation n'en a plus besoin.

Pour remplir ces objectifs de sauvegarde des enregistrements, il convient que l'organisation suive les étapes suivantes :

a) il convient d'établir des directives relatives à la conservation, au stockage, à la manipulation et à l'élimination des enregistrements et de l'information;

b) il convient d'établir un programme de conservation identifiant les enregistrements et leur durée de conservation;

c) il convient de tenir à jour un inventaire des sources de l'information clé.

Certains enregistrements peuvent nécessiter une conservation sécurisée afin de satisfaire aux exigences légales, réglementaires ou contractuelles et soutenir les activités essentielles de l'organisation.

Il peut s'agir d'enregistrements pouvant être requis dans le but de prouver qu'une organisation se conforme aux règles légales ou réglementaires, d'offrir une défense dans toute action civile ou pénale éventuelle ou de confirmer le statut financier d'une organisation auprès d'actionnaires, de tiers et de commissaires aux comptes.

La réglementation ou la loi en Côte d'Ivoire peuvent déterminer la période de conservation de l'information, ainsi que son contenu.

20.1.4 Protection de la vie privée et protection des données à caractère personnel

Il convient de garantir la protection de la vie privée et la protection des données à caractère personnel telles que l'exigent la législation et les réglementations applicables, le cas échéant.

Il convient de développer et de mettre en œuvre une politique des données de l'organisation pour assurer la protection de la vie privée et la protection des données à caractère personnel.

Il convient de communiquer cette politique à toutes les personnes impliquées dans le traitement des données à caractère personnel.

La conformité à cette politique et à toutes les législations et réglementations pertinentes en matière de protection de la vie privée des personnes et de protection des données à caractère personnel exige une structure et des mesures de gestion appropriées.

La meilleure façon de mettre en place une telle structure est de désigner un responsable, par exemple un administrateur de la protection de la vie privée.

Il convient que cet administrateur conseille les responsables, les utilisateurs et les prestataires de services sur leurs responsabilités individuelles et les procédures spécifiques qu'il convient de respecter.

Il convient que la responsabilité afférente au traitement des données à caractère personnel et à la sensibilisation aux principes de protection de la vie privée prenne en compte la législation et les réglementations applicables.

Il convient de mettre en œuvre des mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel.

20.1.5 Réglementation relative aux mesures cryptographiques

Il convient de prendre des mesures cryptographiques conformément aux accords, lois et réglementations applicables.

En vue de se conformer aux accords, lois et réglementations applicables, il convient de prendre en compte les éléments suivants:

a) les restrictions en matière d'importation ou d'exportation de matériels et de logiciels destinés à l'exécution de fonctions cryptographiques;

b) les restrictions en matière d'importation ou d'exportation de matériels et de logiciels intégrant des fonctions cryptographiques;

c) les restrictions en matière d'utilisation du chiffrement;

d) les méthodes non discrétionnaires ou non dont disposent les autorités nationales pour accéder aux informations chiffrées par des moyens matériels ou logiciels dans le but de préserver la confidentialité du contenu.

Il convient de demander un avis juridique afin de s'assurer de la conformité aux lois et réglementations nationales. Il convient également de solliciter un avis juridique avant de transmettre de l'information chiffrée ou des mesures cryptographiques au-delà des limites juridictionnelles.

20.2 Revue de la sécurité de l'information

Chaque organisation doit garantir que la sécurité de l'information est mise en œuvre et appliquée conformément aux politiques et procédures organisationnelles.

20.2.1 Revue indépendante de la sécurité de l'information

Il convient de procéder à des revues régulières et indépendantes de l'approche retenue par l'organisation pour gérer et mettre en œuvre la sécurité de l'information (à savoir le suivi des objectifs, les mesures, les politiques, les procédures et les processus relatifs à la sécurité de l'information) à intervalles définis ou lorsque des changements importants sont intervenus.

Il convient que la direction instaure une revue indépendante. Des revues indépendantes sont nécessaires pour veiller à la pérennité de l'applicabilité, de l'adéquation et de l'efficacité de l'approche de l'organisation en matière de management de la sécurité de l'information.

Il convient que la revue permette d'analyser les opportunités d'amélioration et les changements éventuels à apporter à l'approche adoptée en matière de sécurité, en particulier à la politique et aux objectifs.

Il convient qu'une telle revue soit réalisée par des personnes indépendantes du domaine concerné, par exemple par des intervenants de la fonction d'audit interne, par un responsable indépendant ou une organisation tiers spécialisée dans de telles revues. Il convient que les personnes chargées de ces revues possèdent les compétences et l'expérience nécessaires.

Il convient d'enregistrer et de communiquer les résultats de la revue indépendante à la direction à l'origine de la demande. Il convient de conserver ces enregistrements.

20.2.2 Conformité avec les politiques et les normes de sécurité

Il convient que les responsables revoient régulièrement la conformité du traitement de l'information et des procédures dont ils sont chargés au regard des politiques, des normes de sécurité applicables et autres exigences de sécurité.

Il convient que les responsables déterminent la manière de vérifier que les exigences de sécurité de l'information définies dans les politiques, les normes et autres règlementations applicables, sont respectées.

Il convient d'envisager l'utilisation d'outils de mesure et d'enregistrement automatisés pour procéder à des revues régulières efficaces.

Si la revue détecte une non-conformité, il convient que les responsables :

a) déterminent les causes de la non-conformité;

b) évaluent la nécessité d'engager des actions pour établir la conformité;

c) mettent en œuvre l'action corrective appropriée;

d) revoient l'action corrective entreprise pour vérifier son efficacité et identifier toute insuffisance ou faille.

Il convient que les résultats des revues et des actions correctives réalisées par les responsables soient enregistrés et que ces enregistrements soient tenus à jour.

Il convient que ces résultats soient communiqués aux personnes réalisant des revues indépendantes par le responsable concerné lorsqu'une revue indépendante est menée dans son domaine de responsabilité.

20.2.3 Examen de la conformité technique

Il convient que les systèmes d'information soient régulièrement revus pour vérifier leur conformité avec les politiques et les normes de sécurité de l'information de l'organisation.

Il convient que la revue de conformité technique soit réalisée de préférence à l'aide d'outils automatiques, générant des rapports techniques à soumettre à l'interprétation d'un spécialiste. Il

est également possible de faire procéder à une revue manuelle (avec l'appui, si nécessaire d'outils logiciels appropriés) par un ingénieur systèmes expérimenté.

Lors de tests d'intrusion ou d'appréciations des vulnérabilités, il convient de procéder avec la plus grande prudence, car de telles activités peuvent compromettre la sécurité du système. Il convient de planifier et de documenter ces tests qui doivent pouvoir être répétés.

Il convient que toute revue de conformité technique soit effectuée par des personnes compétentes, autorisées ou sous la supervision de telles personnes.

La revue de conformité technique implique l'examen des systèmes en exploitation en vue de garantir que les contrôles matériels et logiciels ont été correctement mis en œuvre. Ce type d'examen de la conformité requiert l'expertise d'un spécialiste.

Les revues de conformité englobent, par exemple, les tests d'intrusion et les appréciations des vulnérabilités pouvant être effectués par des experts indépendants engagés à cette fin exclusivement. Ces tests et appréciations peuvent aider à détecter les vulnérabilités du système et à vérifier l'efficacité des mesures prises pour empêcher les accès non autorisés en raison de ces vulnérabilités.

Fait à Abidjan, le 22 décembre 2021

Alassane OUATTARA

Copie certifiée conforme à l'original
Le Secrétaire Général du Gouvernement

Eliane Atté BIMANAGBO
Préfet