Partie 3 :

Gouvernance et conformité

Formateur : Azer Zairi
(azer.zairi@gnet.tn)

Partie 3 – Sections et objectifs

3.1 Gouvernance

Créer des documents de politiques de cybersécurité.

3.2 L'éthique de la cybersécurité

Créer un code de conduite personnel éthique.

3.3 Le cadre de gestion de la sécurité IT

Évaluer les contrôles de sécurité.

3.1 Gouvernance

Gouvernance

Gouvernance

- La **gouvernance** de la sécurité IT détermine **qui est autorisé** à **prendre** des **décisions** concernant les **risques** liés à la cybersécurité au sein d'une entreprise.
- Il démontre la **responsabilité** et **assure** la **surveillance** pour s'assurer que les **risques** sont **suffisamment atténués** et que les **stratégies** de **sécurité** sont **alignées** sur les **objectifs** de **l'entreprise** et **conformes** aux **réglementations**.
- Les **programmes** de **bonne gouvernance** des données ont **plusieurs rôles** clés.

Propriétaire des données	Une personne qui assure la conformité avec les politiques et les procédures, attribue la classification appropriée aux ressources d'information et détermine les critères d'accès aux ressources d'information.
Contrôleur des données	Une personne qui détermine les finalités et la manière dont les données personnelles sont traitées.
Traitement des données	Une personne ou une entreprise qui traite des données personnelles pour le compte du responsable du traitement.
Dépositaire des données	Personne qui met en œuvre la classification et les contrôles de sécurité des données conformément aux règles définies par le propriétaire des données. En d'autres termes, les dépositaires des données sont responsables du contrôle technique des données.
Intendant des données	Personne qui s'assure que les données répondent aux besoins de l'entreprise et aux exigences réglementaires.
Responsable de la protection des données	Personne qui supervise la stratégie de protection des données d'une entreprise.

Gouvernance

Politiques de cybersécurité

- Une politique de cybersécurité est un **document général** qui **décrit** la **vision** d'une entreprise en matière de **cybersécurité**,
  - y compris ses **objectifs**, ses **besoins**, son **champ d'application** et ses **responsabilités**.
- Plus précisément, il :
  - Montre **l'engagement** de l'entreprise **envers** la **sécurité**.
  - Définit les **normes** de **comportement** et les **exigences** en matière de sécurité pour la mise en œuvre des activités, des processus et des opérations, ainsi que pour la protection des technologies et des informations au sein d'une entreprise.
  - Veille à ce que **l'acquisition**, **l'utilisation** et la **maintenance** des **opérations**, des **logiciels** et du **matériel** du système soient **cohérentes** dans toute **l'organisation**
  - Définit les **conséquences juridiques** des violations de la politique.
  - Offre à l'équipe de sécurité le **soutien** dont elle a besoin de la part de la **direction**.

Gouvernance

Politiques de cybersécurité (suite)

- Il existe **différents types** de politiques de cybersécurité.
- Les plus courantes sont les suivantes :
  - **Maîtriser la politique de cybersécurité**
    - Plan directeur du programme de cybersécurité d'une entreprise.
    - Cette politique sert de plan stratégique pour la mise en œuvre des contrôles de cybersécurité.
  - **Politique spécifique au système**
    - Ce type de politique est développé pour des périphériques ou des systèmes informatiques spécifiques et vise à normaliser les applications, les logiciels, les configurations de système d'exploitation, le matériel et les contre-mesures de renforcement approuvés au sein d'une entreprise.
  - **Politique spécifique à un problème**
    - Ce type de politique est développé pour certains problèmes opérationnels, circonstances ou conditions qui peuvent nécessiter des exigences et des instructions plus détaillées.

Gouvernance

Types de politiques de sécurité

- Une entreprise **doit établir** des **politiques** de **sécurité claires** et **détaillées** que tous les **collaborateurs** connaissent.
- Voici certaines des politiques liées à la sécurité qu'une organisation peut avoir en place :

Politique d'identification et d'authentification	Spécifie qui doit être autorisé à accéder aux ressources du réseau et quelles procédures de vérification sont en place pour faciliter cet accès.
Politique de mot de passe	Définit les exigences minimales en matière de mot de passe.
Stratégie des règles de bon usage	Met en évidence un ensemble de règles qui déterminent l'accès aux ressources réseau et leur utilisation.
Stratégie d'accès à distance	Explique comment se connecter à distance au réseau interne d'une entreprise et quelles informations sont accessibles à distance.
Politique de maintenance du réseau	Décrit les procédures de mise à jour des systèmes d'exploitation et des applications des utilisateurs finaux d'une entreprise.
Politique de gestion des incidents	Fournit des conseils sur la façon de signaler et de répondre aux incidents liés à la sécurité dans une entreprise.
Politique de données	Définit des règles mesurables pour le traitement des données au sein d'une organisation, par exemple en précisant où les données sont stockées, comment elles sont classées et comment elles sont traitées et éliminées.
Politique d'authentification	Applique les règles de composition des informations d'identification.
Politique organisationnelle	Fournit des conseils sur la façon dont le travail doit être effectué dans une entreprise.

3.2 Éthique de la cybersécurité

L'éthique de la cybersécurité

Éthique d'un spécialiste de la cybersécurité

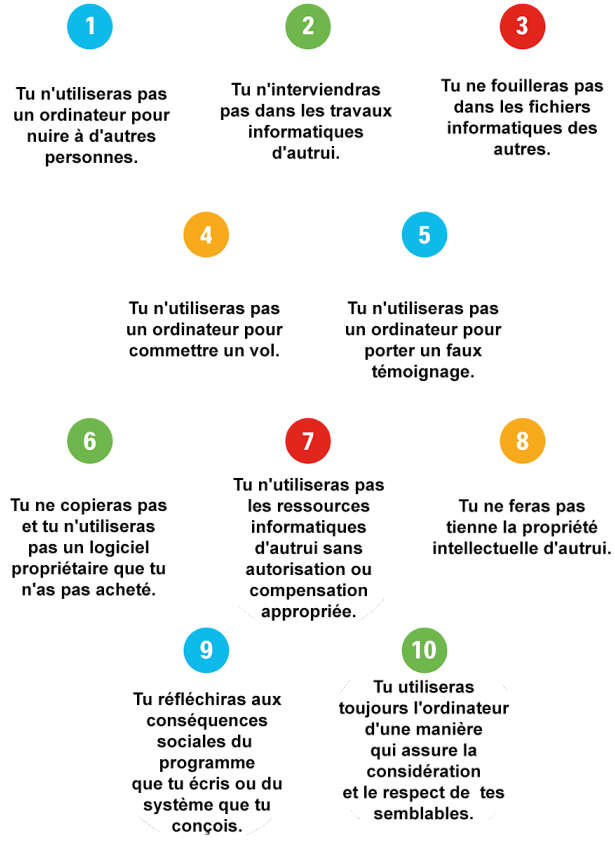
- **L'éthique** est la **petite voix** dans votre **tête** qui vous dit ce qui est **bien** et ce qui ne **l'est pas**, vous guidant pour prendre les **bonnes décisions**.
- En tant que **spécialiste** de la **cybersécurité**, vous devez **connaître** à la fois **la loi** et les **intérêts** d'une entreprise pour prendre de telles **décisions**.
- **L'éthique** peut être considérée sous **différents angles**.

Éthique utilitariste	Cela repose sur le principe directeur selon lequel la conséquence d'une action est le facteur le plus important pour déterminer si l'action est morale ou non. Par exemple, une action qui maximise le bien-être du plus grand nombre est un choix éthique.
Approche des droits	L'approche fondée sur les droits est guidée par le principe selon lequel un individu a le droit de faire ses propres choix, qui ne peuvent être violés par la décision d'une autre personne. Cette décision doit respecter et prendre en compte les droits fondamentaux de l'individu. Ces droits fondamentaux comprennent le droit à la vérité, à la vie privée, à la sécurité et à ce que la société applique les lois de manière équitable à tous ses membres.
L'approche du bien commun	Elle que les actions éthiques soient celles qui bénéficient à l'ensemble de la communauté. Elle met les individus au défi de reconnaître et de poursuivre les valeurs et les objectifs partagés avec les autres membres de la communauté.

L'éthique de la cybersécurité

Il existe dix commandements d'éthique informatique.

- Basé à Washington, DC, le **Computer Ethics Institute** est une ressource permettant **d'identifier**, **d'évaluer** et de **répondre** aux **questions éthiques** dans l'ensemble du secteur des technologies de l'information.
- Elle a été l'une des premières organisations à **reconnaître** les **problèmes d'éthique** et de **politique publique** découlant de la croissance rapide du domaine des technologies de l'information.
- Ils ont créé les **dix commandements de l'éthique** informatique présentés ici.



L'éthique de la cybersécurité

Cyber crime

La **cybercriminalité** se divise en **trois catégories** :

1. **La cybercriminalité** est l'endroit où un ordinateur est la cible d'une activité criminelle.
   - Les exemples incluent les attaques de malwares, le piratage ou les attaques par déni de service.

2. **La criminalité assistée par ordinateur** se produit lorsqu'un ordinateur est utilisé pour commettre un crime, comme un vol ou une fraude.

3. **La criminalité liée aux ordinateurs** désigne la transmission par un ordinateur d'informations qui sont accessoires à une infraction réelle. Par exemple, un ordinateur est utilisé pour stocker des vidéos téléchargées illégalement, et non l'outil utilisé pour commettre le crime.

L'éthique de la cybersécurité

Le Cybercrime (suite)

- De **nombreux outils connectés** à **Internet**, dont beaucoup **ne nécessitent pas** une **grande expertise**, contribuent à la **croissance exponentielle** de la cybercriminalité.

- En fait, la **cybercriminalité** se **développe** beaucoup plus **vite** que la capacité du système **juridique** à créer des lois et des réglementations qui l'interdisent.

- Plusieurs organismes luttent contre la cybercriminalité, notamment
  - le Federal Bureau of Investigation (FBI)
  - Internet Crime Complaint Center (IC3),
  - InfraGard
  - et la Software and Information Industry Association (SIIA) aux États-Unis.

L'éthique de la cybersécurité

Lois sur la cybercriminalité

Des **lois** sont en place pour **interdire** les **comportements indésirables**.
Aux États-Unis, il existe **trois sources principales** de **lois** et de **réglementations**, qui impliquent toutes des aspects de la **sécurité informatique**.

Droit statutaire	Le Congrès des États-Unis a mis en place des agences administratives fédérales et un cadre réglementaire qui comprend des sanctions civiles et pénales en cas de manquement aux règles.Le droit pénal applique un code moral généralement accepté et soutenu par le gouvernement.Par exemple, le Computer Fraud and Abuse Act est une loi qui interdit l'accès à un ordinateur sans autorisation, ou au-delà de l'autorisation. Enfreindre ces règles est passible d'une amende ou d'une peine de prison.
Droit administratif	Cadre juridique qui régit les activités des organismes administratifs du gouvernement, le droit administratif garantit que les organismes publics agissent conformément à la loi.Par exemple, la Commission fédérale des communications (FCC) et la Commission fédérale du commerce (FTC) se sont préoccupées de questions telles que le vol de propriété intellectuelle et la fraude.
Uni sous le régime du droit commun	Les affaires de common law suivent leur cours dans le système judiciaire et fournissent des précédents et des bases constitutionnelles pour l'élaboration des lois.

L'éthique de la cybersécurité

Federal Information Security Management Act (FISMA)

- Les **systèmes IT fédéraux** contiennent et utilisent une **grande quantité d'informations précieuses** et sont donc considérés comme des **cibles** de choix pour les **cybercriminels**.

- En **2002**, le **Congrès** américain a créé la **FISMA** pour couvrir les systèmes IT des organismes fédéraux.

- Plus précisément, la **FISMA stipule** que les **organismes fédéraux doivent** créer un **programme** de **sécurité** des **informations** qui inclut :
  - **Évaluation** des risques
  - **Inventaire annuel** des systèmes informatiques
  - Politiques et procédures de **réduction** des risques
  - **Formation** sur la sensibilisation aux questions de sécurité
  - **Test** et **évaluation** de tous les contrôles de systèmes informatiques
  - **Procédure** de gestion des incidents
  - **Plan** de **continuité** des opérations

L'éthique de la cybersécurité

Législation sectorielle

Il **existe plusieurs lois** et les **normes** auxquelles les entreprises travaillant dans ces secteurs aux États-Unis doivent se conformer.

Finance	La loi **Gramm-Leach-Bliley (GLBA)** est un texte législatif qui touche principalement le secteur financier. Cependant, une partie de cette législation prévoit également des dispositions de refus pour les individus, leur donnant le contrôle de la façon dont les informations qu'ils partagent avec une entreprise lors d'une transaction commerciale sont utilisées. Le GLBA restreint le partage d'informations avec des organisations tierces.
Comptabilité d'entreprise	À la suite de plusieurs scandales comptables très médiatisés aux États-Unis, le Congrès a adopté la loi **Sarbanes-Oxley (SOX)** en 2002 afin de réviser les normes de comptabilité financière et d'entreprise. Plus précisément, elle ciblait les normes et les pratiques financières des entreprises cotées en bourse du pays.
Les cartes de crédit	La norme **PCI DSS (Payment Card Industry Data Security Standard)** est un ensemble de règles contractuelles qui visent à protéger les données de paiement des titulaires de carte de paiement pendant une transaction et à réduire la fraude. En théorie, la norme PCI DSS est une norme volontaire. Cependant, dans la pratique, toute entreprise qui stocke, traite ou transmet des données de titulaires de carte non conformes à la norme PCI DSS s'expose à des frais de transaction beaucoup plus élevés, à des amendes pouvant atteindre 500 000 $ et, dans des circonstances extrêmes, ne peut plus traiter les cartes de paiement.
Cryptographie	Les entreprises qui **importent ou exportent des produits de chiffrement commerciaux** sont soumises à des réglementations supervisées par le Bureau of Industry and Security du département du Commerce.Des restrictions à l'exportation vers des États voyous et des organisations terroristes peuvent être en place pour des raisons de sécurité nationale.En outre, certains pays peuvent décider de restreindre l'importation des technologies de cryptographie en raison des préoccupations suivantes : • La technologie contient une porte dérobée ou une faille de sécurité. • Les citoyens peuvent utiliser cette technologie pour communiquer de manière anonyme et échapper à la surveillance des autorités. • Les niveaux de confidentialité pourraient augmenter au-delà d'un niveau acceptable.

L'éthique de la cybersécurité

Lois sur l'avis de manquement à la sécurité (Security Breach Notification Laws)

- Les entreprises, grandes et petites, **reconnaissent l'importance** de la **collecte** et de **l'analyse** des données
  - et, par **conséquent**, **collectent** toujours **plus d'informations personnelles** sur leurs clients.
- Les **cybercriminels** sont toujours à la recherche de **moyens d'accéder** à ces **données** précieuses et de les **exploiter** à leur avantage personnel.
- Par **conséquent**, **toutes** les **organisations** qui **recueillent** des **données sensibles** doivent être de bons **gardiens** des **données**.

L'éthique de la cybersécurité

Lois sur l'avis de manquement à la sécurité (Security Breach Notification Laws) (suite)

- Aux États-Unis, plusieurs lois obligent les entreprises à notifier les individus en cas de violation de leurs données personnelles.
  - **Loi sur la confidentialité des communications électroniques (Electronic Communications Privacy Act - ECPA)**
    - L'ECPA vise à garantir la confidentialité des informations sur le lieu de travail et protège un large éventail de communications électroniques, telles que les e-mails et les conversations téléphoniques, contre les interceptions, les accès, les utilisations et les divulgations non autorisés.
  - **Loi américaine de répression des fraudes et des abus liés à l'informatique (Computer Fraud and Abuse Act - CFAA)**
    - Adoptée en 1986 en tant qu'amendement à la loi de 1984 sur la lutte contre la criminalité, la loi CFAA interdit tout accès non autorisé aux systèmes informatiques.
    - Le fait d'accéder sciemment à un ordinateur public sans autorisation ou d'accéder à un ordinateur utilisé dans le cadre du commerce entre États ou à l'étranger ou ayant une incidence sur celui-ci est une infraction pénale.
    - La loi criminalise également le trafic de mots de passe ou d'informations d'accès similaires, ainsi que la transmission en connaissance de cause d'un programme, d'un code ou d'une commande qui entraîne des dommages.

L'éthique de la cybersécurité

Protection de la confidentialité

Aux États-Unis, il n'existe **pas** de **loi fédérale** sur la **confidentialité**, mais un **ensemble** de **lois** et de **réglementations** qui protègent les données personnelles des citoyens américains.

Loi sur la confidentialité de 1974 (Privacy Act of 1974)	Cette loi établit un code de pratiques équitables en matière d'information qui régit la collecte, la conservation, l'utilisation et la diffusion d'informations personnelles identifiables sur les individus qui sont conservées dans les systèmes de dossiers par les agences fédérales.
Loi sur la liberté d'information (FOIA)	Le Freedom of Information Act (FOIA) permet un accès public aux dossiers du gouvernement des États-Unis.Elle comporte une présomption de divulgation, ce qui signifie qu'il incombe au gouvernement de fournir une bonne raison pour laquelle toute information ne peut être divulguée.Il existe neuf exemptions de divulgation relatives à la FOIA :
Loi pour la protection de la vie privée et des dossiers scolaires (Family Education Records and Privacy Act - FERPA)	Cette loi fédérale régit l'accès aux dossiers scolaires.Il fonctionne sur la base d'un opt-in. Cela signifie que les parents doivent approuver la divulgation des informations éducatives d'un élève à des entités publiques avant la divulgation réelle. Lorsqu'un étudiant atteint l'âge de 18 ans, ou entre dans un établissement d'enseignement postsecondaire à n'importe quel âge, ses droits en vertu de la FERPA passent des parents à l'étudiant.
Action américaine de protection de la vie privée des enfants en ligne (COPPA)	Cette loi fédérale a été créée pour protéger la vie privée des enfants de moins de 13 ans en imposant certaines exigences aux opérateurs de sites web et aux services en ligne sous juridiction américaine.Par exemple, le consentement des parents doit être obtenu avant qu'une entreprise puisse collecter et utiliser des informations auprès d'enfants de moins de 13 ans.

L'éthique de la cybersécurité

Protection de la confidentialité (suite)

Loi américaine sur la protection des enfants sur Internet (CIPA)	Le Children's Internet Protection Act a été voté en 2000 par le Congrès des États-Unis pour éviter que les enfants de moins de 17 ans n'aient accès à du contenu Internet choquant et à caractère obscène.
Loi pour la protection de la vie privée contre la surveillance vidéo (Video Privacy Protection Act - VPPA)	Cette loi a été promulguée à l'origine pour empêcher le partage d'informations sur la location de bandes vidéo, de DVD et de jeux vidéo avec une autre partie.Cette disposition a été modifiée en 2013 pour permettre à des entreprises telles que Netflix de collecter le consentement des clients qui leur permet de stocker leurs historiques de location et/ou de les rendre publics pendant une période pouvant aller jusqu'à deux ans. Cet amendement signifie que ces entreprises peuvent fournir des recommandations à leurs utilisateurs ou en leur nom.
Loi HIPAA (Health Insurance Portability and Accountability Act, loi portant entre autres sur la protection des données médicales)	Cette loi exigeait la création de normes nationales pour imposer des garanties en matière de stockage physique, de maintenance, de transmission et d'accès aux informations de santé des personnes.Toute entreprise qui utilise des signatures électroniques doit respecter ces normes, garantissant l'intégrité des informations, l'authentification des signataires et la non-répudiation (la validité de la signature ne peut donc pas être refusée).
Projet de loi du Sénat de Californie 1386 (SB 1386)	Ce projet de loi exige que toutes les personnes concernées soient informées de leurs droits et responsabilités en cas de perte ou de divulgation de leurs informations personnelles.
Règles de confidentialité	Un résultat direct de la gamme de lois relatives à la confidentialité et à la collecte des données a été la génération de politiques de confidentialité qui aident à assurer la conformité des entreprises avec la loi.
Évaluation des incidences sur la vie privée (PIA)	L'évaluation des facteurs relatifs à la vie privée est un processus qui permet de s'assurer que les informations personnelles identifiables (PII) sont correctement traitées au sein d'une organisation.

L'éthique de la cybersécurité

Législation internationale

- Avec la **croissance d'Internet**, la **cybercriminalité** est devenue un **problème** de **sécurité**, avec des conséquences à la fois **nationales** et **internationales**.
- Les **lois nationales** sur la **cybercriminalité** existent dans de **nombreux pays**, mais elles **varient considérablement**, ce qui **complique** les **enquêtes** et les **poursuites** sur les **cybercriminels transfrontaliers**.
- Les **efforts internationaux** visant à **cibler** la **cybercriminalité** se multiplient.
- Ratifiée par **65 États,** la **Convention** sur la **cybercriminalité** est le **premier traité international** qui s'attaque à la **criminalité** sur **Internet** et à la **criminalité numérique**,
  - en particulier à la **violation** des **droits d'auteur**, à la **fraude informatique**, à la **pédopornographie** et aux **atteintes** à la **sécurité** des **réseaux**.
- **Pendant ce temps, le Centre d'information électronique sur la confidentialité (EPIC)** est un **centre** de **recherche** à **but non lucratif** basé à Washington, qui vise à **promouvoir** la **confidentialité** et la **transparence** des **lois** et politiques gouvernementales.
- Fort de **liens étroits** avec des **entreprises** du **monde** entier, **EPIC** met l'accent sur la **confidentialité numérique**.

3.3 Le cadre de gestion de la sécurité IT

Le cadre de gestion de la sécurité IT

Les douze domaines de la cybersécurité

- **ISO/IEC 27000** est une **série** de **normes** de **sécurité** des **informations** ou de **bonnes pratiques** visant à aider les entreprises à **améliorer** leur **sécurité**.
- Publiées par l'Organisation internationale de normalisation (**ISO**) et la Commission électrotechnique internationale (**IEC**), les normes ISO 27000 **définissent** des **exigences** complètes en matière de système de **gestion** de la **sécurité** de **l'information** (SGSI : ISMS).
- Un système de gestion de la sécurité de l'information (**SGSI** ou **SMSI**) est **constitué** de **tous** les **contrôles administratifs**, **techniques** et **opérationnels** qui concernent la **sécurité** de **l'information** au sein d'une organisation.
- La norme **ISO 27000** est représentée par **douze domaines indépendants**.
- Ces douze domaines servent de **base** à l'élaboration de **normes** de **sécurité** et de **pratiques** efficaces de **gestion** de la **sécurité** au sein des entreprises, tout en **facilitant** la **communication** entre les **entreprises**.

Le cadre de gestion de la sécurité IT

Les douze domaines de la cybersécurité (suite)

Un résumé de ces douze domaines :

Évaluation des risques	Il s'agit de la première étape du processus de gestion des risques, qui détermine la valeur quantitative et qualitative du risque lié à une situation ou à une menace spécifique.
Stratégie de sécurité	Ce document porte sur les contraintes et les comportements des individus au sein d'une organisation et précise souvent comment les données sont accessibles, et quelles données sont accessibles par qui.
Organisation de la sécurité de l'information	Il s'agit du modèle de gouvernance établi par une entreprise pour la sécurité des informations.
Gestion des ressources	Il s'agit d'un inventaire et d'un schéma de classification des actifs informationnels au sein d'une organisation.
Sécurité liée aux ressources humaines	Il s'agit des procédures de sécurité mises en place pour les employés qui entrent dans une organisation, s'y déplacent ou la quittent.
Sécurité physique et environnementale	Il s'agit de la protection physique des installations et des informations d'une entreprise.
Communications et gestion des opérations	Il s'agit de la gestion des contrôles de sécurité techniques des systèmes et réseaux d'une organisation.

Le cadre de gestion de la sécurité IT

Les douze domaines de la cybersécurité (suite)

Acquisition, développement et maintenance de systèmes d'information	Il s'agit de la sécurité en tant que partie intégrante des systèmes d'information d'une entreprise.
Des contrôles d'accès	Il s'agit de la façon dont une entreprise restreint les droits d'accès aux réseaux, aux systèmes, aux fonctions des applications et aux données afin d'empêcher les utilisateurs non autorisés.
Gestion des incidents de sécurité de l'information	Il s'agit de l'approche d'une organisation en matière d'anticipation et de réponse aux violations de la sécurité de l'information.
Gestion de la continuité de l'activité	Il s'agit de la capacité d'une entreprise à protéger, à gérer et à restaurer les activités stratégiques après une interruption des systèmes d'information.
Conformité	Décrit le processus consistant à s'assurer du respect des politiques, des normes et des réglementations en matière de sécurité de l'information.

- La structure de ce modèle de cybersécurité ISO diffère du modèle OSI (Open System Interconnection) en ce sens qu'il s'agit d'un modèle de pairs qui utilise des domaines plutôt que des couches pour décrire les catégories de sécurité.
- **Chaque domaine a une relation directe avec les autres domaines.**

Le cadre de gestion de la sécurité IT

Objectifs des contrôles et contrôles

- Ces douze domaines sont constitués d'**objectifs de contrôle** (ISO 27001) et de **contrôles** (ISO 27002).
  - **Objectifs de contrôle**
    - Les objectifs de contrôle définissent les exigences générales pour la mise en œuvre d'un système complet de gestion de la sécurité des informations dans une entreprise et fournissent généralement une liste de contrôle à utiliser lors d'un audit du SMSI.
    - La réussite de cet audit indique qu'une entreprise est conforme à la norme ISO 27001 et garantit aux partenaires la sécurité des données et des opérations de l'entreprise.

  - **Contrôles**
    - Les contrôles expliquent comment atteindre les objectifs de contrôle d'une entreprise.
    - Ils établissent des directives pour la mise en œuvre, la maintenance et l'amélioration de la gestion de la sécurité de l'information dans une entreprise.

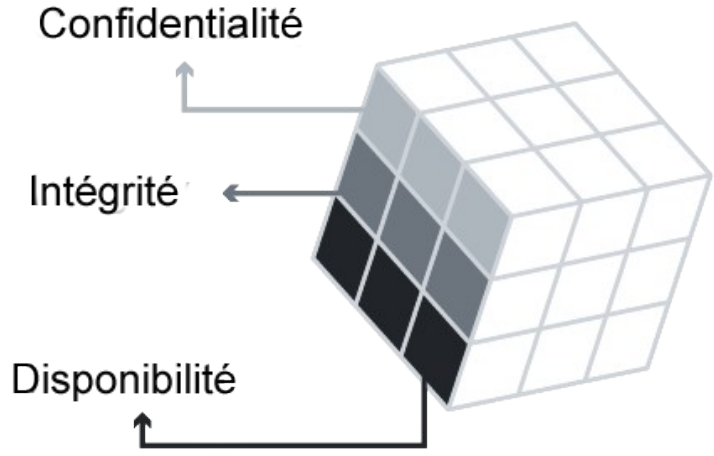
- L'**objectif de contrôle** d'une organisation est de contrôler l'accès aux réseaux en utilisant les mécanismes d'authentification appropriés pour les utilisateurs et les équipements.

- Par conséquent, un **contrôle** pertinent consiste à utiliser des mots de passe forts composés d'au moins huit caractères et d'une combinaison de lettres majuscules et minuscules, de chiffres et de symboles.

Le cadre de gestion de la sécurité IT

ISO 27000 et la triade de la CIA

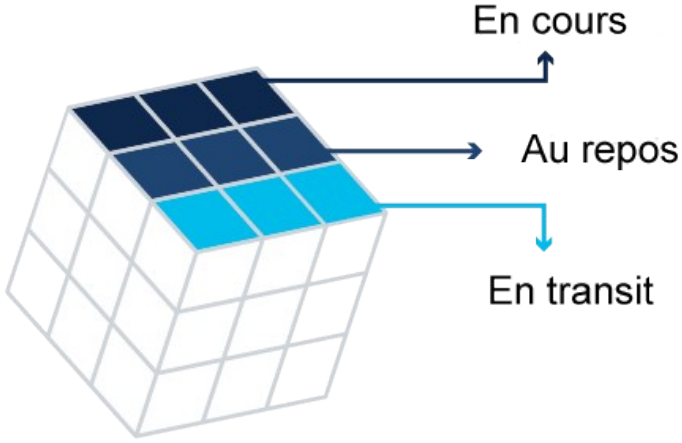
- L'**ISO 27000** est un **cadre universel** qui s'applique à tout **type d'organisation**.
- Une organisation doit **identifier** les **domaines**, les **objectifs** de contrôle et les **contrôles** qui s'appliquent à son **environnement** et à ses **opérations** les utiliser efficacement.
- Pour ce faire, la **plupart** des **entreprises** produisent une **déclaration d'applicabilité** (SOA) qui leur permet d'adapter les objectifs et les contrôles disponibles pour répondre au mieux à leurs priorités en matière de **confidentialité**, d'**intégrité** et de **disponibilité**.



Le cadre de gestion de la sécurité IT

ISO 27000 et l'état des données

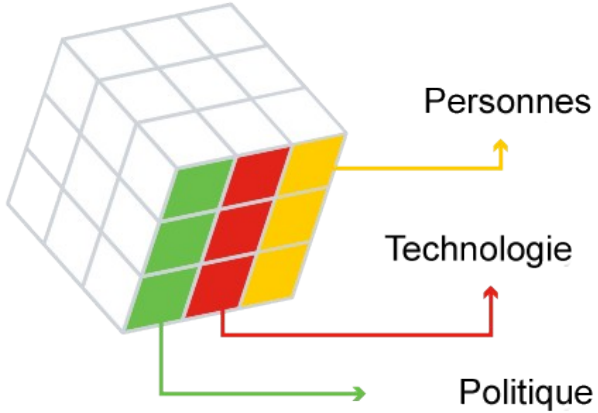
- Les contrôles ISO traitent spécifiquement des objectifs de sécurité pour les données dans chacun des trois états : **en cours de traitement**, **au repos** (en stockage) et **en transit**.
- La **responsabilité** de l'identification et de la mise en œuvre des contrôles pertinents peut incomber à **différents groupes** dans l'entreprise.
- **Par exemple**, une équipe de sécurité du réseau peut être responsable des contrôles qui assurent la confidentialité, l'intégrité et la disponibilité de toutes les données transmises (données en transit), les programmeurs et les analystes de saisie de données pour les données en cours de traitement (en cours) et les spécialistes de l'assistance matérielle pour les données stockées. données (au repos/en stockage).



Le cadre de gestion de la sécurité IT

ISO 27000 et les garanties

- Les **contrôles** ISO fournissent également une **orientation technique** pour les objectifs de **contrôle** liés aux politiques, procédures et directives de cybersécurité définies par la direction d'une entreprise.
- **Par exemple**, imaginons qu'une équipe de direction établisse une politique pour protéger toutes les données entrantes ou sortantes d'une entreprise.
- La responsabilité de la mise en œuvre et de la configuration des réseaux, des systèmes et des équipements pour respecter les directives de la politique incombe aux professionnels de l'IT compétents au sein de l'entreprise, et non à l'équipe de direction.



Le cadre de gestion de la sécurité IT

Le cadre national pour l'embauche de collaborateurs experts en cybersécurité

Le National Institute of Standards and Technologies (**NIST**) a **créé** le **National Cybersecurity Workforce Framework** pour aider les entreprises à la **recherche** de **professionnels** de la **cybersécurité**, **organiser** le travail de cybersécurité en **sept catégories** et décrire les principaux rôles, responsabilités et compétences nécessaires pour chacun d’eux :

Exploitation et maintenance	Fournir le soutien, l'administration et la maintenance nécessaires pour assurer une performance et une sécurité efficaces et efficientes des systèmes informatiques.
Protéger et défendre	Identifie, analyse et atténue les menaces qui pèsent sur les systèmes et les réseaux internes.
Enquêter	Enquête sur les événements liés à la cybersécurité et/ou les cyberattaques impliquant des ressources IT.
Collecter et exploiter	Fournit des opérations spécialisées de déni et de déception et la collecte d'informations sur la cybersécurité.
Analyser	Effectue un examen et une évaluation hautement spécialisés des informations entrantes en matière de cybersécurité afin de déterminer leur utilité pour le renseignement.
Superviser et gouverner	Assurer le leadership, la gestion, la direction ou le développement et la défense des intérêts d'une organisation afin qu'elle puisse mener efficacement des activités de cybersécurité.
Disposition sécurisée	Conceptualise, conçoit, achète ou construit des systèmes informatiques sécurisés.

Le cadre de gestion de la sécurité IT

Le CIS Contrôles de sécurité critiques

- Le Center for Internet Security (**CIS**) a développé un **ensemble** de **contrôles** de sécurité **essentiels** pour aider les entreprises disposant de différents **niveaux** de ressources et d'expertise à améliorer leurs cyberdéfenses.
  - **Contrôles de base :** les entreprises dont les ressources et l'expertise en matière de cybersécurité sont limitées doivent mettre en œuvre l'inventaire et le contrôle des ressources matérielles et logicielles, la gestion continue des vulnérabilités, l'utilisation contrôlée des privilèges administratifs, les configurations sécurisées du matériel et des logiciels, ainsi que la maintenance, la surveillance et l'analyse des journaux d'audit.
  - **Contrôles de base supplémentaire :** les entreprises disposant de ressources et d'une expertise en cybersécurité modérées doivent mettre en œuvre des contrôles de base, ainsi que des protections des e-mails et des navigateurs web, une protection contre les malwares, la limitation et le contrôle des ports réseau, des protocoles et des services, des fonctionnalités de récupération des données, des configurations sécurisées pour les périphériques réseau, la sécurité, la protection des données, le contrôle d'accès basé sur le principe du « besoin de savoir », le contrôle d'accès sans fil et la surveillance et le contrôle des comptes.
  - **Contrôles organisationnels :** les entreprises disposant de ressources importantes et d'une expertise en matière de cybersécurité doivent mettre en œuvre les contrôles de base et de base, ainsi qu'un programme de sensibilisation et de formation à la sécurité, à la sécurité des logiciels d'application, à la gestion et à la gestion des incidents, et aux tests de pénétration et aux exercices Red Team (exercices de simulation d'attaque pour évaluer les capacités de sécurité d'une entreprise).

Le cadre de gestion de la sécurité IT

La matrice de contrôle du cloud

- La Cloud Security Alliance (**CSA**) fournit des **conseils** en matière de **sécurité** à toute **entreprise** qui **utilise** le **cloud computing** ou qui souhaite évaluer les risques pour la sécurité globale d'un fournisseur de cloud.
- Leur Cloud Controls Matrix (**CCM**) est un **cadre** de **contrôle** de la **cybersécurité** qui mappe les contrôles de sécurité spécifiques au cloud aux principales **normes**, **bonnes pratiques** et **réglementations**.
- Elle se compose de **197 objectifs** de contrôle structurés en **17 domaines** couvrant **tous** les **aspects** de la technologie cloud, notamment la gouvernance et la gestion des risques, les ressources humaines et la sécurité mobile.
- Le **modèle CCM** est **considéré** comme un **standard** de facto pour l'assurance et la conformité de la sécurité du cloud.

Le cadre de gestion de la sécurité IT

Conformité

- Les **fournisseurs** de **services** peuvent avoir besoin de **fournir** à leurs **entreprises** clientes **l'assurance** que les **contrôles** de **sécurité** qu'ils mettent en œuvre sont **correctement conçus** et fonctionnent **efficacement**.
- Les exemples suivants montrent comment un fournisseur de services peut procéder.
- **Lecture typographique Déclaration sur les standards des missions d'attestation (SSAE) 18 Contrôle des organismes de services (SOC) 2 Audit**
  - Il s'agit d'un audit indépendant des contrôles de reporting d'une entreprise en ce qui concerne la sécurité, la disponibilité, l'intégrité du traitement, la confidentialité et la confidentialité d'un système.
  - Un rapport d'attestation confirme que les contrôles sont en place à un moment précis (type I) ou gérés sur une période d'au moins six mois (type II).
  - Ces rapports fournissent à l'entreprise cliente l'assurance que des contrôles sont en place et fonctionnent pour protéger les données sensibles.

Le cadre de gestion de la sécurité IT

Conformité (suite)

- **La certification du modèle de maturité de la cybersécurité (CMMC)**
  - Cette **certification** s'adresse à **toutes** les **entreprises fournissant** un **service** au département de la Défense des États-Unis (**DoD**) et vérifie que ces entreprises ont mis en place des pratiques et des processus de cybersécurité adéquats pour garantir un minimum d'hygiène « de base » en matière de cybersécurité.
  - La **CMMC** établit **cinq niveaux** de **certification** qui vont des « pratiques de base en matière de cybersécurité » aux « pratiques améliorées qui fournissent des fonctionnalités plus sophistiquées pour détecter et traiter les APT ».
  - Il est probable que les fournisseurs de services devront satisfaire aux exigences de la CMMC appropriée afin d'être pris en compte pour l'attribution d'un contrat du DoD.

3.4 Résumé de la troisième partie

Résumé de la troisième partie

Résumé

- La gouvernance de la sécurité IT détermine qui est autorisé à prendre des décisions concernant les risques liés à la cybersécurité au sein d'une entreprise.
- Les bons programmes de gouvernance des données ont un propriétaire, un contrôleur, un sous-traitant, un dépositaire, un responsable et un responsable de la protection des données.
- Une politique de cybersécurité est un document général qui décrit la vision d'une entreprise en matière de cybersécurité, y compris ses objectifs, ses besoins, son champ d'application et ses responsabilités.
- Les politiques de sécurité spécifiques incluent : l'ID et l'authentification, le mot de passe, l'utilisation acceptable, la maintenance du réseau, la gestion des incidents, les données, les informations d'identification et l'organisation.
- L'approche fondée sur les droits est guidée par le principe selon lequel un individu a le droit de faire ses propres choix, qui ne peuvent être violés par la décision d'une autre personne.
- Il existe dix commandements de l'éthique informatique couvrant généralement les choses que vous ne devez pas faire avec un ordinateur.
- Il existe trois catégories de cybercriminalité : la criminalité ciblée par l'ordinateur, la criminalité assistée par l'ordinateur et la criminalité accidentelle.
- Aux États-Unis, il existe trois sources principales de lois et de réglementations en matière de sécurité informatique : le droit législatif, le droit administratif et la common law.

Résumé du chapitre

Résumé

- Certains secteurs ont également des lois spécifiques sur la cybercriminalité : la finance, la comptabilité d'entreprise, les cartes de crédit et la cryptographie.
- Ratifiée par 65 États, la Convention sur la cybercriminalité est le premier traité international qui s'attaque à la criminalité sur Internet et à la criminalité numérique, en particulier à la violation des droits d'auteur, à la fraude informatique, à la pédopornographie et aux atteintes à la sécurité des réseaux.
- Les douze domaines de la cybersécurité
- Les objectifs de contrôle définissent les exigences générales pour la mise en œuvre d'un système complet de gestion de la sécurité des informations dans une entreprise.
- N'oubliez pas que les contrôles expliquent comment atteindre les objectifs de contrôle d'une entreprise et établissent des directives pour la mise en œuvre, le maintien et l'amélioration de la gestion de la sécurité de l'information.
- L'ISO 27000 est un cadre universel qui s'applique à tout type d'organisation.
- Une organisation doit identifier les domaines, les objectifs de contrôle et les contrôles qui s'appliquent à son environnement et à ses opérations.
- La plupart des organisations créent un SOA pour adapter les objectifs et les contrôles disponibles afin de répondre au mieux à leurs priorités en matière de confidentialité, d'intégrité et de disponibilité.
- Les contrôles ISO répondent spécifiquement aux objectifs de sécurité pour les données en cours de traitement, au repos (en stockage) et en transit.

Résumé du chapitre

Résumé

- Le NIST a créé le National Cybersecurity Workforce Framework pour aider les entreprises à la recherche de professionnels de la cybersécurité.
- CIS a développé un ensemble de contrôles de sécurité critiques (de base, fondamentaux et organisationnels) pour aider les entreprises disposant de différents niveaux de ressources et d'expertise à améliorer leurs cyberdéfenses.
- La CSA fournit des conseils en matière de sécurité à toute entreprise qui utilise le cloud computing ou qui souhaite évaluer le risque global pour la sécurité d'un fournisseur de cloud.
- Leur Matrice de contrôles du cloud (CCM) mappe les contrôles de sécurité spécifiques au cloud aux principales normes, bonnes pratiques et réglementations.
- La norme CSA CCM est considérée comme une norme de facto pour l'assurance et la conformité de la sécurité du cloud.
- Un rapport d'attestation (SSAE ou SOC) confirme que les contrôles sont en place à un moment précis (type I) ou gérés sur une période d'au moins six mois (type II).
- La CMMC établit cinq niveaux de certification qui vont des « pratiques de base en matière de cybersécurité » aux « pratiques améliorées qui fournissent des fonctionnalités plus sophistiquées pour détecter et traiter les APT ».