Sécurité = situation dans laquelle qqn/qqchose n'est exposé à aucun danger, à aucun risque d'agression physique, d'accident, de vol, de détérioration.

Risque = possibilité de survenue d'un inconvénient, d'un événement indésirable, se calcule en faisant : Somme de i (probabilité d'occurence i * conséquence i) pour un risque absolu
Pour un risque réel = risque absolu * sensibilité

Danger = ce qui constitue une menace, un risque, qui compromet l'existence de qqn/qqchose.

Menace = Cause potentielle d'un incident, qui pourrait entrainer des dommages sur un actif

Il y'a 4 menaces génériques = interruption, Interception, modification, et injection.

Sécurité informatique = Ensemble de mesures permettant de réduire les risques pesant sur le SI et de limiter leurs impacts sur les missions de l'organisation. Impact dé réputation, économique, juridique, organisationnels et perte de clients.

SI = Ensemble des ressources destinées à **collecter, classer, stocker, diffuser**

Le but de la SI est de connaitre et délimiter ce qu'il faut protéger, en considérant 3 états d'informations, traitement, stockage et transports sous tous les supports.

La SI se décompose en un ensemble d'actifs qu'il faut sécuriser (employés, patrimoine, matériels/logiciels)

Actif = tout ce qui à une valeur pour l'organisation.

Méthode d'Analyse du SI:
-Délimiter : sous-partie ou ensemble du SI ?
-Décomposer : entre actifs primordiaux et acifs supports
-Cartographier: L'organisation humaine, architecture materielle/logiciele et les infras
-Enquete auprès des usagers: clé usb, télétravail?

Sûreté de fonctionnement = Ensemble de mesures permettant d'assurer le bon fonctionnement d'un système malgré les incidents susceptibles de se produire (protection contre les accidents involontaires) vs sécurité ou on lutte contre les actions volontaires non désirées

Résilient = résistance au chocs, donc une architecture qui reste oppérationnelle face aux incidents.

Cybercriminalité = Ensemble des actes contrevenants aux traités internationaux ou aux lois nationales utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

Les failles sont dans :
-le développement

-l'hébergement
-Données vollées
-Intermédiaire financier pas fiable.

ANSII = agence nationale sécurité SI => propose des règles à appliquer pour la protection des S.I de l'état.

La CNIL (Commission Nationale de l'Informatique et des Libertés) = Autorité administrative chargée de veiller à la protection des données personnelles.

CERT (Computer Emergency Response Team) = : veille sur les vulnérabilités et informe le public de ces vulnérabilités

CSIRT (Computer Security Incident Response Team)= l'équipe d'expert qui gére les cyberattaques

Premier CERT = Quand il y'a eu le premier doS à grande échelle.

<u>Principes de base de sécurité:</u>
-Minimiser: Laisser que le nécessaire, limiter la surface d'attaque. Principe du besoin d'en connaitre et moindre privilege
-Cloisonner: Décomposer le système en sous systèmes. Séparer les tâches. DMZ Vlan VPN
-Controler: Firewall, mandataire (role d'intermediaire entre 2 hotes). Logs, privileges Authentification (cquon connait (mdp), pofssède (carte,token), sait faire (signature), on est (emprunte)) donc faire MFA. Gestion des accès IAM.
-Surveiller: Via les logs, IDS, IPS, SIEM (outil qui analyse en temps réel de façon centralisées les logs de l'entreprise)

Pentesting =
Black hat = Pas d'information sur la cible, donne idée du niveau de sécurité.
white hat = avec des conaissances sur la cible, plus rapide et ciblé, éviter

3 phases pour la mise en oeuvre **gestion incidents de sécurité**:
-Prévention : analyse de risque, veille techno, audit des systèmes, cloisonner, défense
-Action : Détecter, réagir, via IDS,IPS et SIEM. procédures
-Récupération: Restaurer et corriger, PRA (plan reprise activité)

4 exigences de sécurité (CIDP) avec les metriques pouvant évoluer:
-Disponibilité: délai d'indisponibilité accepté
-Intégrité : signature numérique lors du transfer de fichier
-Confidentialité: niveau de confidentailité des fichier: avec Confidentiel, secret, restreint..
-Preuve: les logs

Secure by design = Le système a été conçu depuis ses fondations pour être sécurisé. Application des principes de sécurité dès le départ dans la conception.

RSSI = définit la politique de sécurité du SI (PSSI) et veille à son application ; il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte
PSSI phases:
-Préalables: Organisation du projet
-Elaboration des éléments stratégiques: Définition du périmètre et identification des risques et menaces
-Selection des principes et rédaction des règles: rédaction
-Finalisation: établir plan d'action

Shadow IT = Application informatique sans la supervision/approbation de la DSI

Defacement = Modification d'un site web pour revendication, atteinte à l'image
Webworm = Faille PhP, recherche de cibles via Google.

Méthode Gestion des risques :

- 1 Identication des risques
- 2 Hiérarchisation des risques
- 3 Dénition d'un seuil d'acceptation
- 4 Traitement des risques non acceptables

Face au risque, on peut soit **diminuer** le système pour réduire la surface d'attaque, **supprimer** une partie du système ou alors **transférer** le risque auprès d'un tiers
Le niveau de risque est mesuré par les menaces, la gravité et la probabilité d'occurence.

PDCA (Planifier, développer, controler, ajuster) = méthode de gestion de la qualité.

Vulnérabilité = faiblesse au niveau d'un actif
Attaque = action malveillante de la réalisation d'une menace sur une vulnérabilité.
Sensibilité = Mesure de l'impact d'une attaque.

imputabilité = Attribuer la responsabilité d'une action à une personne

Le modèle de Bell et Lapadula propose deux règles: no read-up et no write-down, donc basé sur la confidentialité.

No write up : éviter qu'un utilisateur accède à des informations trop sensibles.
No write down : éviter qu'une information sensible fuite vers un niveau moins sécurisé.

commutation par paquets = suivent la même route
routage de paquets = pas la meme route dans le réseau maillé

Lois :

Normes = définissent des exigences et lignes directrices dans un domaine spécifique.

ISO 27001 = Norme Bonnes pratiques obligatoire en sécurité pour évaluer, détecter les menaces, et maitrier les risques.
Voici le processus:

- Identification des risques
- Elaboration de la PSSI
- Planification
- Mise en oeuvre
- Surveillance et amélioration

ISO 27002 = Donne les lignes directrices de sécurité sur les organisations à comment gérer les risques et menaces

ISO 27005 = Norme qui donne les lignes directrices spécifiquement sur la gestion des risques, sorti en 2022. Propose 4 options de traitement pour gérer un risque:
Refus, transfert, réduction, acceptation

NIS2 transposée = Texte juridique
LPM (Loi de programmation militaire) = Texte juridique qui définit sur plusieurs années les priorités, objectifs et budgets de la défense, afin de garantir les moyens nécessaires aux forces armées. Un chapitre est dédié pour la sécurité des SI. Controls annuels via des audit de sécurité donc obliger de donner la data et mettre en oeuvre les mesures fixées par l'ANSSI.

Les 5 pilliers de la mise en application de la LPM sont:

- pilotage et gouvernance: indicateurs annuel envoyés à l'ANSII et processus formalisé
- Maîtrise des risques:Homologation et plan traitement des risques
- Maîtrise du SI: Cartographier chaque SI, suivi et traitement des vulnérabilités
- Gestion des incidents: Detection des incidents, journalisation et traitement
- Protection des systèmes: IAM, défense en profondeur

RGPD (règlement général de protection des données) = Texte juridique de protection des données sur l'UE apparu en 2018. Pour les structures offrant des biens et services sur l'UE.

Sanction de 20m euros ou 4% du CA pour entreprise

Phase du traitement des données:
-collecte des donées
-stockage
-utilisation des données
-transfert des données
-destruction ou archivage des données.

NIS1 = Directive sécurité des réseaux et SI dans l'UE concernant des fournisseurs du service numérique. Inclut 7 secteurs seulement

NIS2 = Directive sécurité des réseaux et SI dans l'UE concernant les entreprises parmi 18 secteurs. S'applique aux entités essentielles et importantes.
NIS2 regroupe : Gouvernance, protection, défense et résilience

Entité essentielle = Controle automatiques et réguliers
Entité importante = Controle qu'après la conaissance d'une non conformité
Déterminé en fonction du CA/Bilan annuel et nombre d'employés.

ANSSI =Guide de bonne pratiques pour la SSI. Comme sensibiliser les users, sécuriser les postes de travail.. Propose 42 mesures d'hygiène informatique

EBIOS RM (Eexpression des besoins et identification des objectifs de sécurité) Risk manager = Methode créer en 1995 se concentre sur comment faire l'analyse de risques numériques sous forme d'ateliers, updaté en 2018. Tableau de criticité

Certification atteste qu'un résultat final est conforme, une qualification atteste de la capacité technique à réaliser une mission.

Droit pénal = règles relatives aux infractions et aux sanctions applicables à une personne
Droit civil= règles relatives à la personne ou ses rapports avec les autres.

Responsabilité civile = Réparation des dommages causés à un tiers
Responsabilité pénale = Violation d'une infraction pénale qui entraine des sanctions, faut que ça soit : légal ou matériel ou moral.

Deux ordres de juridiction :
Ordre judiciaire = il règle les litiges entre personnes
Ordre administratif = il gère que les litiges entre les citoyens et l'administration

Propriété intelectuelle = Ensemble des droits accordés aux brevets, marques, dessins..
Responsabilité des acteurs de l'internet = lois applicables aux intermediaires (plateforme, hébergeur, fournisseur d'accès..)
Droit des données = RGPD

Droits d'auteurs se décomposent en deux types:
-Moraux = Perme à un auteur de protéger sa création
-Patrimoniaux = Droit de l'auteur sur comment son oeuvre est utilisée pour gagner de l'argent
c

<u>WINDOWS:</u>

Dès qu'un processus est lancé, il est soit:
-Mode utilisateur= Executer chaque processus dans un env virtuel isolé
-Mode noyau = Accès à l'ensemble des espaces virtuels d'adressage (file system, peripherik

Mécanisme de pagination = Allouer à un processus plus de mémoire virtuelle que de mémoire physique disponible grace au disque

Adressage mémoire= Chaque processus utilisant de la données voit ses données éparpillées dans la RAM. C'est le processeur qui gère physiquement l'emplacement.

AD:
Annuaire contenant les groupes, utilisatuers et leur roles associés sous forme d'arbre.

AUtorisation par roles, groupes ou ACL.

acl = droit d'accès aux objets qui sont : users, groupes, pc, répertoires, services..

Un objet sans ACL est accesible à tous
un objet avec ACL vide est accessible à personne.