La sécurité du système d'information

La sécurisation du SI consiste à protéger ce dernier des pannes, des accidents, des intrusions, des malveillances et des maladresses.

Préoccupation partagée dans l'organisation, la sécurité informatique passe par la **communication et le rappel des règles**, **procédures de sauvegarde de données, l'organisation de systèmes de secours, les procédures d'urgence** qui sont autant de moyens pour mettre en place et promouvoir une démarche globale.
La sécurisation absolue (risque zéro) est toutefois impossible. Une agence nationale = **l'ANSSI**

1) L’identification des risques et menaces pesant sur la sécurité du SI

Les conséquences d’un défaut de sécurité

Discontinuité de service	Indisponibilité du réseau, des applications, interruption totale ou partielle du travail sur les sites de l’entreprise ou à distance (télétravail).
Perte de données	Destruction ou altération de tout ou partie des données enregistrées pouvant entraîner une altération de la réputation Web de l’entreprise. Vol de données avec demande de rançon (cyber-rançonnage).
Divulgation intempestive d’informations	Communication d’informations confidentielles (DCP ou stratégiques) à la concurrence, à la presse, aux partenaires ou encore au public sans consentement ni légitimité.
Perte de temps	Temps passé à rétablir le fonctionnement du SI après un incident, à partir de sauvegardes ou en reconstituant des données.
Responsabilité civile et pénale de l’entreprise	Mise en cause de l’entreprise sur le plan civil ou pénal pour usage illégal de logiciels ou de données, publication d’informations erronées, négligence dans la protection des données à caractère personnel.
Coût	Charge occasionnée par les dysfonctionnements et leur réparation technique, commerciale et/ou juridique. Ces coûts peuvent être élevés et nuire à la survie même de l’entreprise.

A) Les risques d'origine matérielle

La sécurité peut être menacée par des problèmes affectant le matériel :

– **sinistre** sur les ordinateurs, serveurs, onduleurs, câbles, supports de sauvegarde (incendie, dégât des eaux, surtension) ;
– **vol** par une personne extérieure à l'entreprise ou un salarié (ordinateur fixe/nomade, supports de sauvegarde)
– **panne** (disque dur, équipements d'interconnexion tels que des routeurs, commutateurs, câblage) ;
– **coupure d'alimentation électrique** (qui peut avoir une incidence sur les supports de données) ;
– **maladresse humaine** (chute d'un ordinateur, mauvaise manipulation d'un support de sauvegarde) ;
– **dégradation volontaire, perte.**

B) Les malveillances d'origine humaine

Les actes malveillants touchent notamment le logiciel et les données enregistrées sur les supports de sauvegarde et d'archivage informatiques. Leurs origines sont variées.

Programme malveillant propagé par un fichier, un réseau, des courriels…	• Virus (s'exécute et/ou s'installe lorsque l'utilisateur réalise une action). Il peut effacer des données, détériorer le système d'exploitation. • Ver ou *worm* (se réplique sur un réseau, provoquant l'effacement de fichiers, de programmes, la saturation du réseau…). • Cheval de Troie ou *trojan* (collecte et/ou altère des données personnelles à l'insu de l'utilisateur, divulgue des données privées via les courriers électroniques…). • Logiciel-espion ou *spyware* (collecte des données personnelles afin d'en tirer profit, exploitation à des fins commerciales…). • Porte dérobée ou *backdoor* (permet d'accéder à un ordinateur ou d'en prendre le contrôle à distance). • Enregistreur de frappe ou *keylogger* (enregistre les touches utilisées par un utilisateur afin de récupérer des mots de passe, des identifiants…).
Fraude ou malveillance	• Agissements volontaires des salariés ou ex-salariés en vue d'en tirer un profit personnel ou de nuire à l'entreprise (introduction d'un programme malveillant, transmission ou falsification de données sensibles, détournement de fonds…). • Actes souvent cachés par les entreprises elles-mêmes pour ne pas effrayer les clients, déclencher un climat de suspicion interne ou ternir leur e-réputation. • Vol de données avec demande de rançon.
Exploitation indésirable de la messagerie	• Pourriel ou *spam* (courrier électronique non sollicité encombrant les réseaux). • Hameçonnage, *fishing* ou *phishing* (redirection de l'internaute vers une page d'écran factice pour lui soutirer des informations personnelles). • Canular ou *hoax* (courrier électronique contenant une information alarmante poussant l'internaute à une action injustifiée).

C) Les carences hypothéquant la sécurité du SI

Les carences proviennent d'actes résultant de l'incompétence, de la négligence ou de l'ignorance :

• **Le non-respect d'une procédure** sécuritaire (accès limité aux bureaux, au local des serveurs), la mise à jour irrégulière des logiciels de protection peuvent favoriser des intrusions frauduleuses ou des vols de matériel.

• **La méconnaissance de la loi** sur les droits d'auteur, du règlement général sur la protection des données (RGPD), de la loi Informatique et Libertés peut aboutir à des poursuites civiles et/ou pénales de l'entreprise.

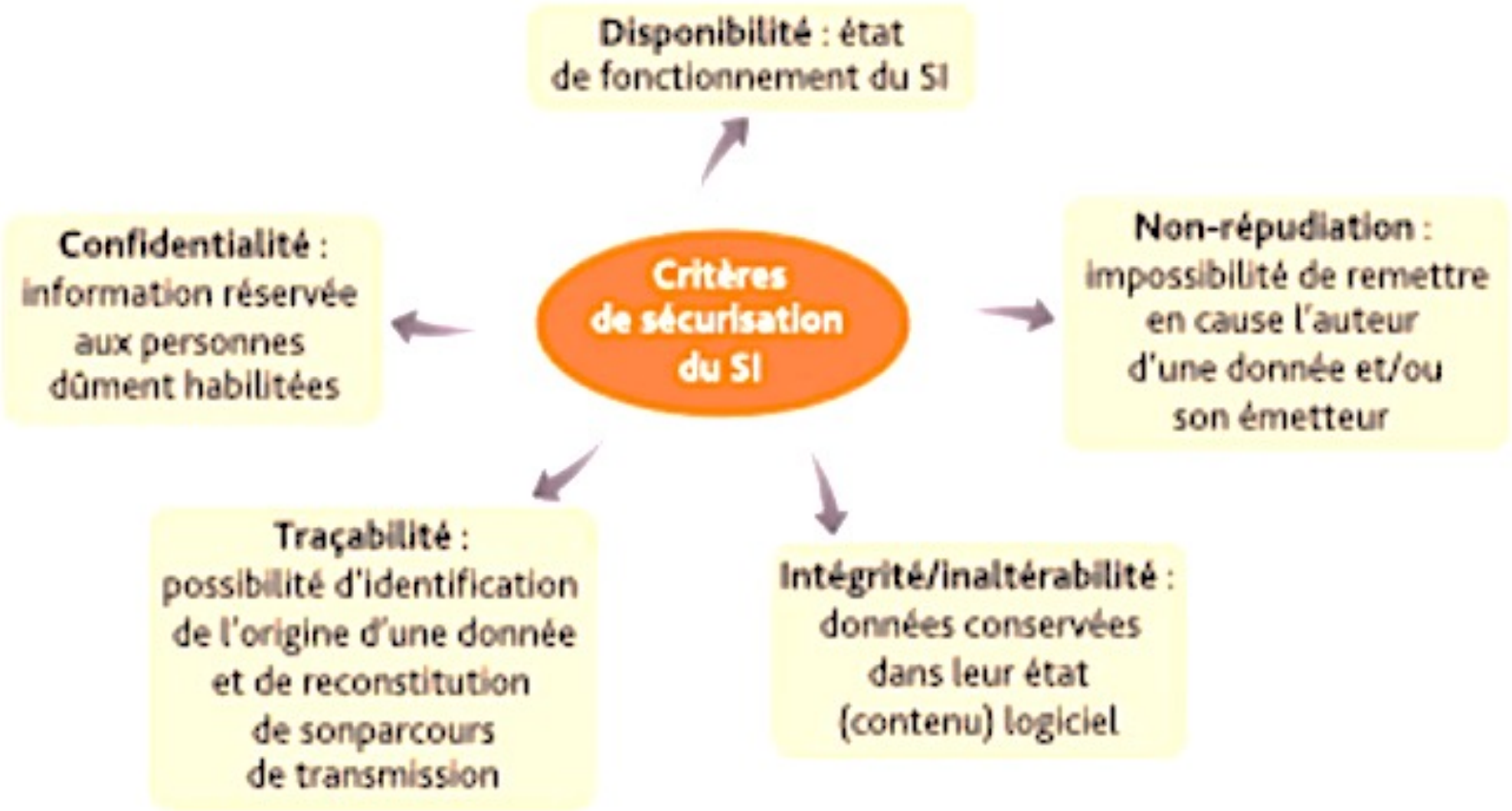
• **Le manque de suivi du SI**. Selon le rapport 2020 des « Menaces informatiques et pratiques de sécurité en France » du Club de sécurité de l'information français (CLUSIF), seules 66 % des entreprises interrogées ont réalisé un audit de leur SI au cours des deux dernières années.

• **Des maladresses dans la manipulation des logiciels**, du progiciel de gestion intégré (PGI), des fichiers, dans la saisie des données et des accès à Internet peuvent conduire à des effacements de données, des divulgations d'informations confidentielles ou à une dégradation de la qualité des données enregistrées.

• **Mauvaises pratiques** : Transmission d'identifiants et de mots de passe entre salariés.

D) Les critères de sécurité

Pour s’assurer du niveau optimum de sécurité du SI, plusieurs critères sont mobilisables



2) La prévention des risques de sécurité

La prévention des risques doit reposer sur une analyse initiale objective et précise des risques possibles (notamment un audit du système d'information) puis sur l'établissement et la mise à jour régulière de plans de sécurisation.

A) Identifier la vulnérabilité du SI : recenser et hiérarchiser les risques

Une fois les risques identifiés, l'entreprise doit les hiérarchiser afin d'apporter des solutions adaptées au degré d'urgence. Un audit sécuritaire du SI de l'entreprise permet de recenser les risques et d'estimer leur gravité ou leur acceptabilité. Plus le niveau de vulnérabilité est élevé, plus il y a urgence à déclencher une mise en conformité sécuritaire

Niveaux de vulnérabilité (par ordre croissant)	1	2	3	4	5	6	7	8	9	10
Domaines recensés										
Équipements, ordinateurs fixes et nomades, serveurs, routeurs, câblages		■								
Gestion de la maintenance matérielle et logicielle				■						
Gestion des bases de données, gestion des sauvegardes et archivages					■					
Locaux techniques, mode de protection des accès physiques	■									
Logiciels métiers, PGI, suite logicielle sécuritaire, réseau privé virtuel (VPN)						■				
Droits d'accès, mises à jour des identifiants et mots de passe										■
Architecture réseau, connexion Internet, gestion du réseau local									■	
Test des procédures de sécurité, du plan de sauvegarde et restauration										■
Gestion et suivi des ESN afin de respecter le cahier des charges et les consignes				■						
Planification des formations à dispenser auprès des salariés								■		
Sensibilisation des salariés aux risques pour le SI, mise à jour de la charte informatique								■		

B) Traiter les risques

Une fois que les priorités sont établies, l'entreprise met en conformité les domaines identifiés comme menacés, l'objectif étant d'intervenir avant que survienne la panne et sur les points les plus graves et urgents.

C) Prévenir les menaces

1. La prévention des risques matériels

Les procédures à mettre en place sont les suivantes :

– **sécuriser les locaux** (badges, caméras de surveillance, digicodes), suivre les accès aux sites sensibles et aux dispositifs d'extinction automatique d'étanchéité au feu, à l'eau, suivi de la température, de l'hygrométrie ;

– **réaliser un inventaire périodique des matériels** ;

– **archiver les données et les logiciels** dans un lieu autre que celui qui héberge les ordinateurs, externaliser les sauvegardes ;

– **bloquer les accès à certains périphériques externes** (lecteurs de CD, ports USB) ;

– **installer un onduleur** pour protéger les matériels des coupures de courant ;

– **prévoir des serveurs redondants ou partenaires** pour basculer l'exploitation en cas de panne du ou des serveurs principaux.

2. La prévention des risques logiciels et de données

Les procédures à mettre en place sont les suivantes :
– **définir des actions de sécurisation** (logiciel antivirus, anti-spyware, pare-feu, DMZ (zone démilitarisée) sur le réseau local. Un pare-feu ou firewall est un dispositif capable de filtrer les échanges d'information entre deux réseaux, notamment entre un réseau local et l'extérieur, afin de bloquer les communications indésirables. Une DMZ est une partie de réseau local protégée de l'extérieur par un pare-feu ;
– **gérer les droits d'accès** (identifiants et mots de passe) et définir des profils d'utilisateurs cohérents au regard des postes occupés ;
– **identifier le degré de sensibilité des données** et prévoir des politiques de sécurisation ad hoc ainsi que le chiffrement de certains échanges ou stockages de données ;
– **retreindre les droits administrateurs** sur les postes nomades ;
– **chiffrer les disques durs**, les données lors des transmissions internes ;
– **effacer les données** sur les disques durs et supports de sauvegardes mis au rebut

3. La prévention des risques organisationnels et humains

Les procédures à mettre en place sont les suivantes :

– **sensibiliser le personnel** aux risques informatiques, former ; (Cyber wargames)
– **mettre régulièrement à jour les droits d'accès**, administrer les droits des utilisateurs et les accès aux répertoires en fonction des profils de poste, mettre en place des mots de passe tournants (rolling code) et lecteurs biométriques (empreintes digitales) ;
– **rédiger une charte informatique** précisant les règles de sécurité interne ;
– préconiser une fermeture de session automatique au-delà d'un certain délai d'inutilisation (lock de session) ;
– **définir un plan de sauvegarde des données** et l'actualiser périodiquement, prévoir des procédures de restauration des données si celles-ci ont été volées ou détruites ;
– **vérifier la conformité** entre les pratiques liées aux données et la législation (loi Informatique et Libertés et RGPD
– **synchroniser les données** lors de déplacements professionnels avec ordinateurs nomades ;
– **assurer un suivi régulier** avec les prestataires du SI (ESN) ;
– **prévoir des informations et des formations** relatives aux modalités de télétravail.

3) L'organisation d'un SI fiable = comment fiabiliser son système d'information ?

A) La politique de définition des plans de sécurité

Il est possible de dégager les dix commandements de la politique de sauvegarde suivants :

• Les travaux effectués au quotidien sur chaque poste de travail et sur les serveurs doivent faire l'objet d'une **sauvegarde** (une recopie) afin de permettre la continuité du travail en cas d'incident.

• Les serveurs peuvent être équipés de dispositifs de **sauvegarde spécifique** pour reprendre l'exploitation rapidement et sans perte de données en cas de panne, notamment grâce à un serveur de secours.

• Des **systèmes doublés** et fonctionnant en miroir peuvent assurer une reprise instantanée.

• La sauvegarde permet de **restaurer** tout ou partie des données à la suite d'un dysfonctionnement.

• Sauvegarde et restauration des données doivent être orchestrées par des **procédures utilitaires** préétablies par un technicien ou par l'administrateur du système d'information.

• Un **plan de reprise d'activité (PRA)**, à partir de sauvegardes, ou un **plan de continuité d'activité (PCA),** basé sur des infrastructures informatiques redondantes peut être défini quand le SI est vital.

• Un **PCA** efficace s'exécute de façon **transparente (**neutre) pour les utilisateurs.

• Les **choix** en matière de sauvegarde, de restauration et de reprise, sont gradués, en fonction de l'importance du système concerné.

• Les **supports de sauvegarde sont choisis** en fonction de leur capacité, de leur coût, de leur rapidité de mise en œuvre et de leur fiabilité, en cohérence avec un contexte organisationnel.

• Les **lieux de conservation** des sauvegardes doivent être sécurisés (local technique), pluriels (en cas de défaillance) et diversifiés (afin de prévenir les risques).

B) Le choix des procédures de sauvegarde et ses conséquences

Les procédures de sauvegarde ont un impact direct sur les résultats et le fonctionnement de l'entreprise au quotidien

Procédures de sauvegarde	Conséquences
Périodicité	Importance des données perdues entre deux sauvegardes
Sauvegarde complète ou différentielle	Volume sauvegardé important, restauration intégrale (parfois longue) • Volume de sauvegarde réduit, restauration à l'aide de deux sauvegardes (complète et dernière sauvegarde différentielle)
Externalisation des sauvegardes sur un autre site ou dans un cloud	• Sollicitation du prestataire pour réimplanter les données perdues • Délai de reprise supérieur
Tests du plan de sauvegarde	Simulation périodique des procédures sécuritaires

4) Les rôles des responsables de la sécurité

Le responsable de la sécurité du système d'information (**RSSI**) met en œuvre toutes les actions permettant de sécuriser le SI. Selon la taille, le secteur d'activité et l'âge de l'entreprise, le RSSI est en fonction à temps plein ou non, rattaché à la DSI ou à la direction générale.

A) La remise en état du SI après un incident

Quand un problème affecte le SI, les responsables de la sécurité doivent mettre en œuvre les plans précédemment définis, de manière graduelle en fonction de la gravité de la situation et des dommages constatés :

– **plan de restauration** des données permettant de remettre les données perdues ou volées ;
– **plan de reprise d'activité** (PRA) ;
– **plan de continuité d'activité** (PCA).

B) La mise en œuvre des conditions d'un SI sécurisé

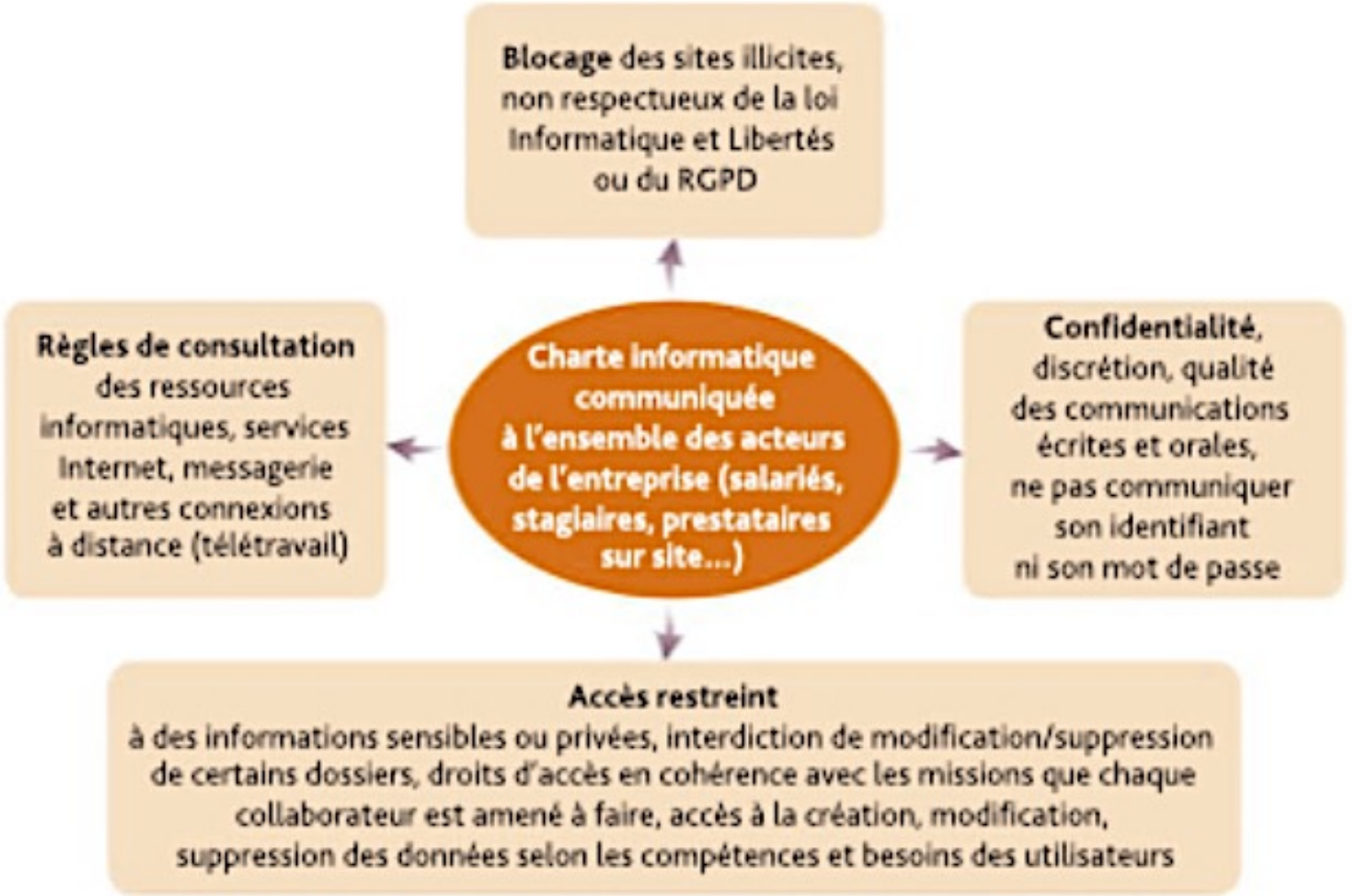
Les missions du responsable de la sécurité du SI ont vocation à s'assurer que le système d'information est fiable et répond aux besoins de l'entreprise :

– il assure une **veille technologique** et réglementaire concernant la sécurité ;
– il pratique un **audit** régulier de la sécurité et alerte sur les risques éventuels ;
– il propose des **solutions** (notamment concernant l'architecture du SI et l'organisation des locaux en vue de leur sécurisation) ;
– il **sensibilise** l'ensemble du personnel à la sécurité du système d'information (formation, charte de sécurité partagée, piqûres de rappel) ;
– il s'assure de la **bonne installation des logiciels anti-virus, des pare-feu et autres dispositifs de sécurisation** ;
– il définit le **plan de sauvegarde des données et le PRA** ;
– il met en place les conditions **d'organisation du télétravail**.

C) La prise en compte du facteur humain

1. La charte informatique, un outil de sensibilisation des salariés

La charte informatique comporte diverses consignes et instructions. C'est un document essentiel permettant de guider les utilisateurs vers de bonnes pratiques sur le système d'information



2) Le cas du Départ d’un salarié

À la suite du départ d’un salarié (préavis échu, licenciement, mutation, départ à la retraite, démission), les **droits d’accès au réseau doivent être actualisés**. Il est fondamental qu’un ex-salarié ne puisse plus accéder au réseau privé de l’entreprise (messagerie professionnelle, base de données, intranet, etc.). De même, ses outils de travail liés au SI à des fins exclusivement professionnelles, tels qu’un ordinateur portable, un téléphone mobile ou une tablette, doivent être restitués.