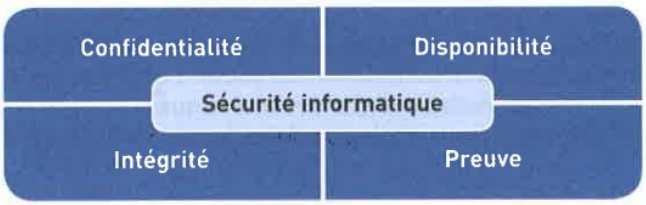
La configuration du système : quelques règles à respecter

Système d'exploitation	– Configurer les mises à jour automatiques – Installer les correctifs et les patchs
Applications	– Autoriser les applications vérifiées (signature) – Isoler les applications obsolètes – Interdire les téléchargements de sources inconnues – Limiter les modules optionnelles
Exécution automatique	Désactiver les ports et lecteurs
***Boot* sur périphériques externes**	Désactiver le *boot* et insérer un mot de passe

Antivirus	Logiciel chargé de détecter et de stopper les *malwares* connus : virus, vers, *keylogger*, chevaux de Troie, etc. Il fonctionne avec une base de données qui contient les signatures des *malware* connus. **Exemples :** Bitdefender, Avast, Norton, Kapersky.
Antispam	Le *spam* (ou courriel indésirable, ou pourriel) est une communication électronique non sollicitée. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires. **Exemples :** Altospam, Postbox, McAfee.
Pare-feu (*firewall*)	Il inspecte les paquets réseaux entrants et sortants et implémente un mécanisme de filtrage basé sur des règles. Il ne transmet pas les paquets qui ne les respectent pas. On distingue les pare-feux matériels (pour un réseau) et les pare-feux logiciels (pour un poste de travail). **Exemples :** Sophos, Stormshield, ZoneAlarm.
Coffre-fort numérique (ou portefeuille de mots de passe)	Il permet de centraliser ses mots de passe en les protégeant par un seul mot de passe fort. **Exemples :** KeyPass ou 1Password.
Système d'authentification unique (en anglais *Single Sign-On*, SSO)	Un seul formulaire d'authentification permet d'accéder à l'ensemble des services de sa session utilisateur.

Les principes de la sécurité

La sécurité des systèmes d'information repose sur quatre principes fondamentaux :



La confidentialité

La **confidentialité** vise à assurer que les données ne sont accessibles qu'aux seules personnes autorisées.

> **Exemple :** la connexion d'un utilisateur au réseau de l'organisation par son identifiant et son mot de passe personnel ne donne accès qu'aux données qu'il est autorisé à consulter ou à modifier.

La disponibilité

La **disponibilité** doit rendre les données accessibles et utilisables par les personnes autorisées sans interruption.

> **Exemple :** la redondance des connexions réseaux permet d'accéder aux données de manière continue, même si une connexion est rompue.

L'intégrité

Le principe d'**intégrité** s'assure que les données ne peuvent pas être modifiées pendant leur transfert, leur traitement ou leur stockage.

> **Exemple :** des protocoles de cryptage, comme le protocole SSL, permettent de s'assurer que les données ne sont pas modifiées pendant leur transfert sur le réseau.

La preuve

Le principe de non-répudiation consiste à apporter la preuve non réfutable d'un acte malveillant. La non-répudiation est assurée par la combinaison de trois éléments : l'authentification, l'imputabilité et la traçabilité.

Disponibilité	Utilisation de solutions de hautes disponibilités (*High Availability*, HA) permettant de garantir une continuité de service en cas de défaillance d'un serveur ou d'une application. **Exemple :** redonder un serveur pour l'accès à un service.
Intégrité	Utilisation d'algorithmes de sommes de contrôles, qui calculent un condensé unique à partir d'une information donnée. La moindre modification de contenu entraîne un changement du résultat de la somme de contrôle. **Exemple :** l'algorithme MD5 (*Message Digest 5*) ou le SHA-256 (*Secure Hash Algorithm*).
Confidentialité	Utilisation d'algorithmes de chiffrement récents et robustes. **Exemple :** l'algorithme AES (*Advanced Encryption Standard*), qui est approuvé par la NSA (*National Security Agency*) aux États-Unis.

Plan de continuité d'activité	L'objectif est d'assurer la continuité des activités en cas d'incident. Un PCA peut, par exemple, prévoir des sauvegardes, qui permettent des restaurations en cas de pertes de données.
Plan de reprise d'activité	L'objectif est d'assurer la reprise des activités en cas de sinistre important (incendie, inondations, etc.). Par exemple, une entreprise peut prévoir un site de secours.