L'AGENCE PUBLICITAIRE-PANNEAU MOBILE TCHAD
ET
LE RÉSEAU DE TRANSPORT ET LOGISTIQUE AU TCHAD (RTLT)

NOVEMBRE NUMÉRIQUE

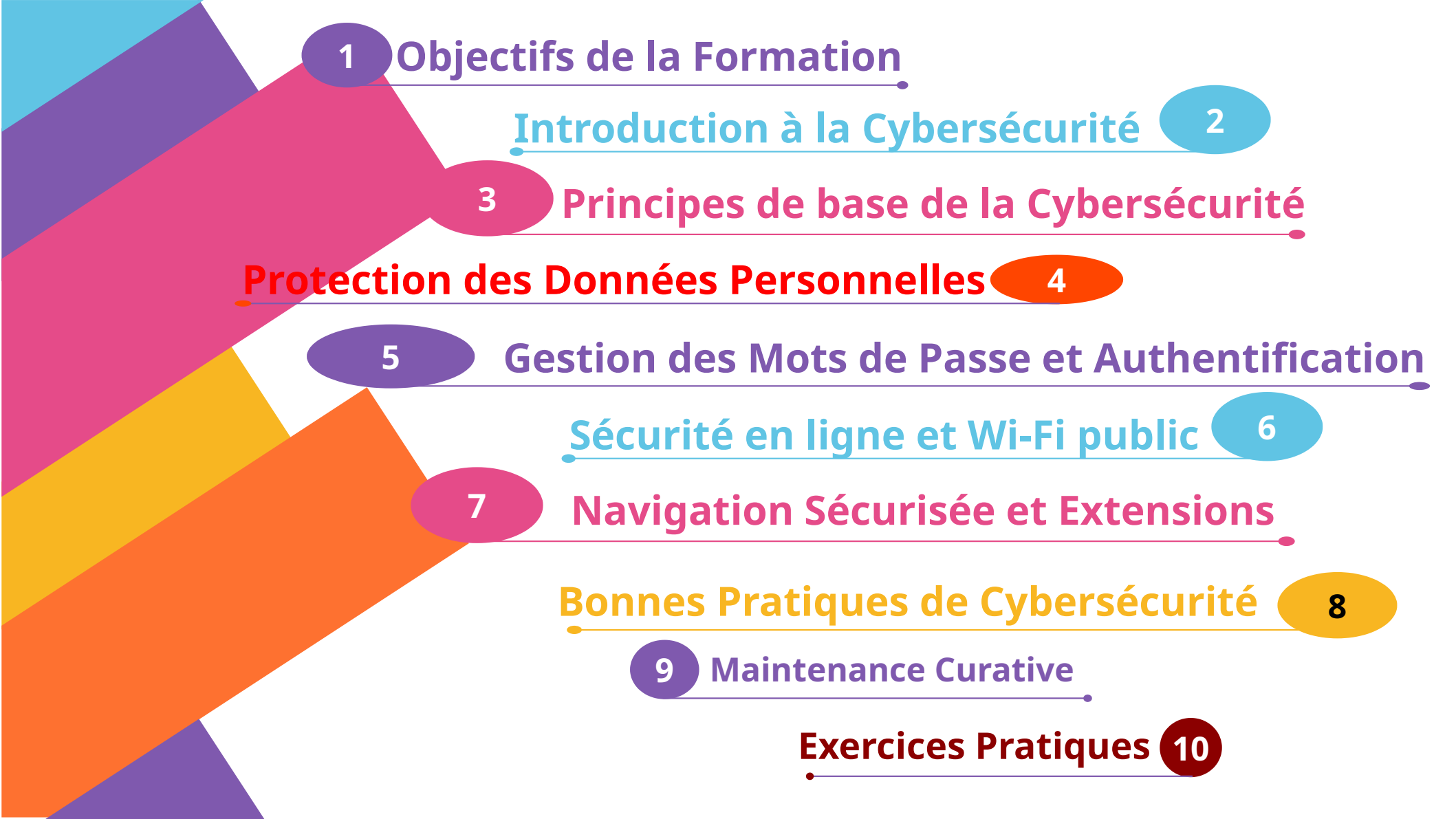
Philippe ALIFA
philipalifa.tpa@gmail.com

N'Djamena
Moundou
Abéché
Amdjarass

Formation en :

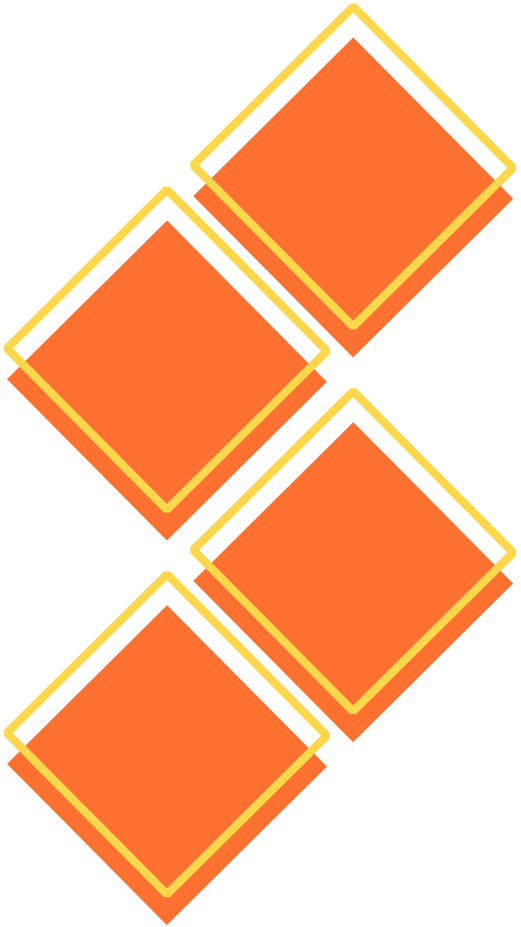
Initiation au Cyber sécurité : principes de sécurité en ligne, protection des données et bonnes pratiques

Maintenance Curative


1 Objectifs de la Formation
Introduction à la Cybersécurité 2
3 Principes de base de la Cybersécurité
Protection des Données Personnelles 4
5 Gestion des Mots de Passe et Authentification
Sécurité en ligne et Wi-Fi public 6
7 Navigation Sécurisée et Extensions
Bonnes Pratiques de Cybersécurité 8
9 Maintenance Curative
Exercices Pratiques 10

1

Objectifs de La formation



1. Comprendre les bases de la cybersécurité
2. Apprendre à protéger ses données en ligne
3. Adopter des bonnes pratiques de sécurité en ligne

2

Introduction à la Cybersécurité

Le mot cybersécurité est un néologisme désignant le rôle de l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques matériels et immatériels (connectés directement ou indirectement à un réseau) des États et des organisations (avec un objectif de disponibilité, intégrité et authenticité, confidentialité, preuve et non-répudiation). Quand nous parlons de la cybersécurité, nous faisons allusion à la cyberdéfense.

La cyberdéfense regroupe l'ensemble des moyens physiques et virtuels mis en place par un pays dans le cadre de la guerre informatique menée dans le cyberespace. Selon le ministère français des armées, elle est « l’ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d’informations jugés essentiels » et comme « l’ensemble des activités qu’il conduit afin d’intervenir militairement ou non dans le cyberespace pour garantir l’efficacité de l’action des forces armées, la réalisation des missions confiées et le bon fonctionnement du ministère » .

Objectifs de la session

L'objectif est de comprendre les fondamentaux de la cybersécurité pour protéger efficacement ses données en ligne et adopter de bonnes pratiques de sécurité.

Importance actuelle

La cybersécurité est cruciale pour protéger contre la montée des cyberattaques de plus en plus sophistiquées qui menacent les données personnelles, les entreprises, et les infrastructures critiques. Elle assure la confidentialité des informations, la continuité des activités et la confiance des utilisateurs dans les services numériques.

Conséquences d'une mauvaise sécurité

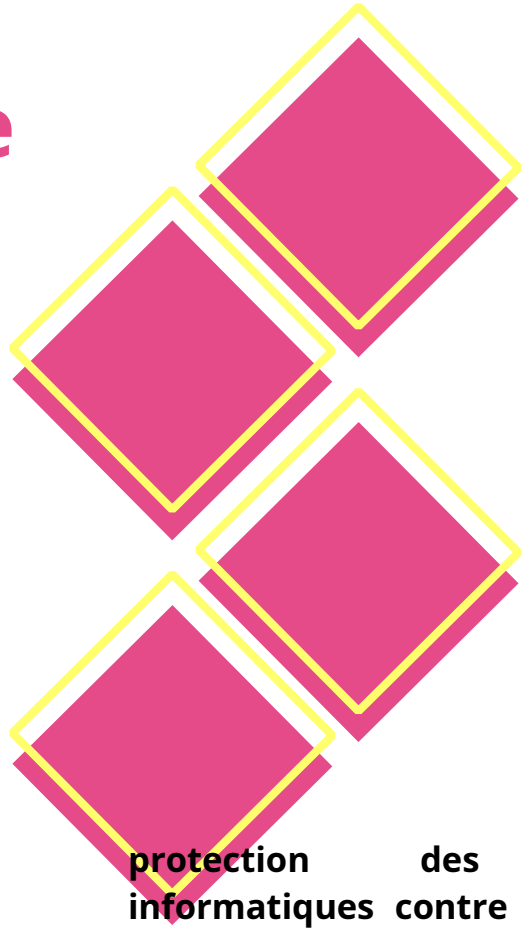
Une mauvaise sécurité expose les données sensibles aux vols et aux violations, compromettant la confidentialité des utilisateurs et des organisations. Elle peut entraîner des interruptions de service, perturbant les opérations et impactant la productivité et la rentabilité des entreprises. Les infrastructures critiques deviennent vulnérables aux attaques, ce qui peut entraîner des impacts graves pour la santé publique et la sécurité nationale. De plus, les organisations risquent des amendes légales et une perte de confiance de leurs clients, nuisant à leur réputation.

3

Principes de base de la Cybersécurité

Définition :

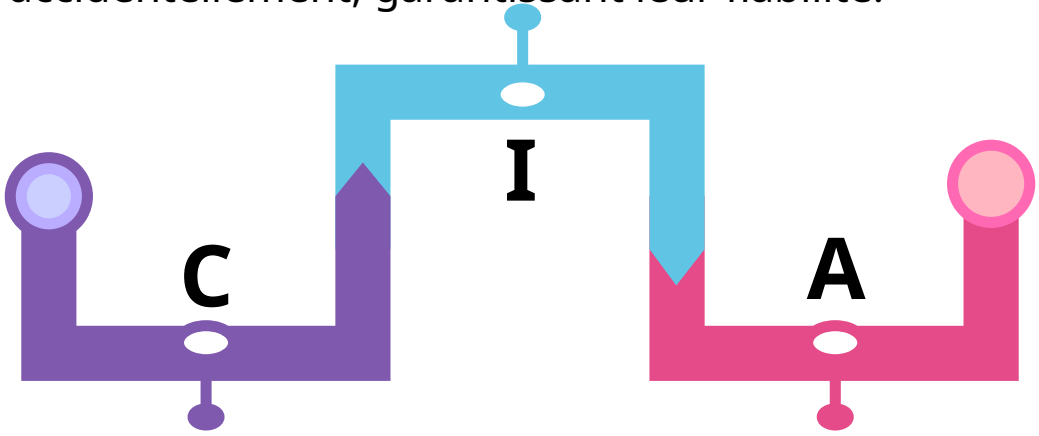
La cybersécurité consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes. On l'appelle également sécurité informatique ou sécurité des systèmes d'information. Vous pouvez la rencontrer dans de nombreux contextes, de l'informatique d'entreprise aux terminaux mobiles. Elle peut être divisée en plusieurs catégories.



protection des systèmes informatiques contre les attaques numériques.

Principe de base de la sécurité

Intégrité : Maintenir l'exactitude et la cohérence des données, en empêchant toute modification non autorisée. Les contrôles d'intégrité permettent de vérifier que les données n'ont pas été altérées, délibérément ou accidentellement, garantissant leur fiabilité.



Confidentialité : Assurer que seules les personnes autorisées ont accès aux informations sensibles. Cela implique des contrôles d'accès, le chiffrement des données et des méthodes d'authentification pour protéger les informations contre l'accès non autorisé.

Disponibilité : Assurer que les informations et les systèmes sont accessibles aux utilisateurs autorisés lorsqu'ils en ont besoin. Cela comprend la protection contre les pannes de système, les cyberattaques (comme les attaques par déni de service), et l'optimisation des performances des systèmes.

3

Types de menaces

virus, logiciels malveillants, phishing, ransomware.

L'hameçonnage ou phishing est une forme d'escroquerie sur internet.

Le fraudeur se fait passer pour un organisme que vous connaissez (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme.

Il vous envoie un mail vous demandant généralement de "mettre à jour" ou de "confirmer vos informations suite à un incident technique", notamment vos coordonnées bancaires (numéro de compte, codes personnels, etc.).

Exemples d'attaques récentes : discutons brièvement D'incidents notables pour sensibiliser.

4 Protection des données personnelles

Ce que sont les données personnelles

informations personnelles, financières, professionnelles.

1. **Chiffrement des données** :

Qu'est-ce que le chiffrement des données ?

- Le chiffrement des données est une technique utilisée pour protéger les informations en les transformant en une forme codée que seules les personnes autorisées peuvent lire.
- Cela empêche les personnes non autorisées d'accéder aux informations sensibles.

4

Comment ça marche ?

Chiffrement : Lorsque vous voulez protéger des données, vous utilisez un **algorithme de chiffrement** et une **clé de chiffrement** pour convertir les données en un code incompréhensible, appelé **texte chiffré**.

Algorithme de chiffrement : Une méthode ou une procédure mathématique qui transforme les données.

Clé de chiffrement : Une séquence de bits utilisée par l'algorithme pour chiffrer et déchiffrer les données.

Transmission sécurisée :

Le texte chiffré peut être transmis ou stocké en toute sécurité, car même s'il est intercepté, il ne peut pas être compris sans la clé appropriée.

Déchiffrement :

Lorsque les données doivent être lues par une personne autorisée, le texte chiffré est reconverti en **texte en clair** (forme originale lisible) à l'aide de l'algorithme de chiffrement et de la clé de déchiffrement.

Exemple simplifié

Texte en clair : "Bonjour"

Algorithme de chiffrement : Une règle qui remplace chaque lettre par une autre lettre.

Clé de chiffrement : La règle spécifique, par exemple, décaler chaque lettre de 3 positions dans l'alphabet (A devient D, B devient E, etc.).

Texte chiffré : "Erqmrxu"

Seule une personne avec la clé de déchiffrement (ici, la règle de décalage inverse) pourra lire le message original "Bonjour".

Pourquoi est-ce important ?

Le chiffrement des données est essentiel pour protéger les informations sensibles telles que les mots de passe, les informations bancaires et les communications privées contre les cybercriminels et les accès non autorisés.

5 Gestion des mots de passe

Importance des mots de passe forts et de leur renouvellement régulier.

Présentation des gestionnaires de mots de passe (ex. **LastPass**, **Bitwarden**, **1Password**).

Authentification à deux facteurs (2FA) : essayons une activation de la 2FA sur un compte.

6 Sécurité en ligne et Wi-Fi public

Risques des Wi-Fi publics

Les réseaux Wi-Fi publics, comme leur nom l'indique, restent des réseaux dont vous ne connaissez pas le niveau sécurité, ni qui le gère.

Sniffing de Paquets (Un cybercriminel utilise un logiciel de sniffing pour intercepter et surveiller le trafic des utilisateurs**)**

Attaques de l'homme du milieu (MitM: Man in the Middle) : Vos données peuvent être interceptées par des individus malveillants qui se positionnent entre vous et le point d'accès Wifi.

Faux réseaux Wi-Fi ou piégés : Les pirates informatiques peuvent créer de faux réseaux Wi-Fi qui ressemblent à des réseaux légitimes mais qui sont en réalité conçus pour voler vos informations.

VPN (Virtual Private Network) :

solutions

Un VPN est une technologie qui crée une connexion sécurisée et cryptée entre votre appareil (ordinateur, smartphone, etc.) et un serveur distant. Cette connexion permet de masquer votre adresse IP, de sécuriser vos données et d'accéder à des ressources sur le réseau privé comme si vous étiez physiquement présent à cet emplacement.
expliquer son fonctionnement de base et recommander des outils comme **NordVPN**, **ProtonVPN**, ou **OpenVPN**. Naviguer uniquement dans des cites securiser (https)

7 Navigation Sécurisée et Extensions

Utilisation de navigateurs sécurisés (ex. **Brave, Mozilla Firefox)**

Brave et Firefox sont réputés pour leur sécurité car ils bloquent les traqueurs et les cookies tiers par défaut, protégeant ainsi la vie privée. Leur code open source permet des vérifications publiques pour identifier et corriger rapidement les failles. Enfin, ils surveillent les permissions des extensions pour limiter les risques d'intrusion et de malware.

Activation de la protection anti-phishing.

Kasperky, Avast, ... (Il faut mettre tous les fonctionnalités des antivirus : plus precisement le ENDpoint security. La version 11 est la plus rescente.)

8 Bonnes Pratiques de Cybersécurité

Mises à jour régulières : importance de garder les logiciels et systèmes d'exploitation à jour.
Courriels et phishing : comment détecter les courriels suspects, analyser les liens et pièces jointes.
Utilisation sécurisée des réseaux sociaux : paramétrage de la confidentialité, éviter de partager des informations sensibles.
Sécurité des appareils : installation d'un antivirus (ex. **Windows Defender**, **Avast**, **Kaspersky**), sécurisation des appareils mobiles.
Sauvegarde des données : stratégie de sauvegarde en 3-2-1 (3 copies, 2 emplacements différents, 1 copie hors site) avec des solutions comme **Google Drive**, **Dropbox**, **iCloud**, ou des disques durs externes.

9 Maintenance Curative

La maintenance des systèmes est un terme général qui comprend divers types de maintenance informatique, nécessaires pour assurer le bon fonctionnement d'un système. Certains des différents types de maintenance comprennent des soins curatifs, correctifs et préventifs. Ces trois branches ont toutes le même objectif, mais sont utilisées dans des circonstances et des situations différentes.

Si vous voulez optimiser les performances de votre système, et donc in fine le rendre plus fiable, une maintenance régulière est indispensable.

Différents types de maintenance

Maintenance corrective

En cas de défaillance du système, la maintenance corrective vise à remettre cette partie du système en état de fonctionnement. La maintenance corrective consiste à réparer certaines pièces lorsqu'elles se cassent. Cela peut être mis en œuvre de manière aléatoire en cas de défaillance des pièces, ou faire partie d'un plan de maintenance plus large. Il existe deux formes différentes de maintenance corrective : planifiée et non planifiée.

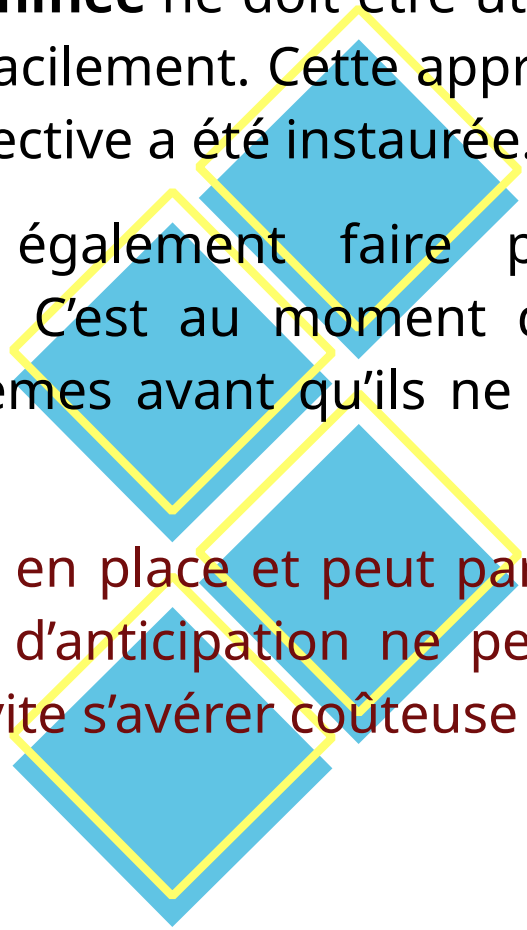
Maintenance corrective planifiée

Dans une stratégie de maintenance corrective planifiée, il existe deux types de maintenance. Le premier consiste à laisser la machine tomber en panne, et d'appliquer une stratégie de maintenance corrective classique : un élément du système tombe en panne, vous choisissez de le réparer ou de le remplacer.

Une **stratégie de maintenance corrective planifiée** ne doit être utilisée qu'avec des actifs que vous pouvez remplacer facilement. Cette approche est utilisée lorsque seule une maintenance corrective a été instaurée.

La **maintenance corrective planifiée** peut également faire partie d'une **stratégie de maintenance préventive**. C'est au moment de la panne que vous essayez d'identifier les problèmes avant qu'ils ne vous surprennent, et les résolvez en cours de route.

La maintenance corrective est simple à mettre en place et peut paraître avantageuse financièrement, mais le manque d'anticipation ne permet parfois pas d'aller au plus économique et peut vite s'avérer coûteuse pour les entreprises.



Maintenance corrective non planifiée

La maintenance corrective non planifiée peut se présenter de deux façons :

1. Lorsqu'une partie de votre système échoue de manière inattendue ou commence à montrer des signes de défaillance, cette partie est ciblée et corrigée
2. Lorsque quelque chose se rompt entre les opérations de maintenance planifiées, lors d'une opération de maintenance préventive, des mesures de maintenance corrective sont mises en œuvre pour réparer cette pièce.

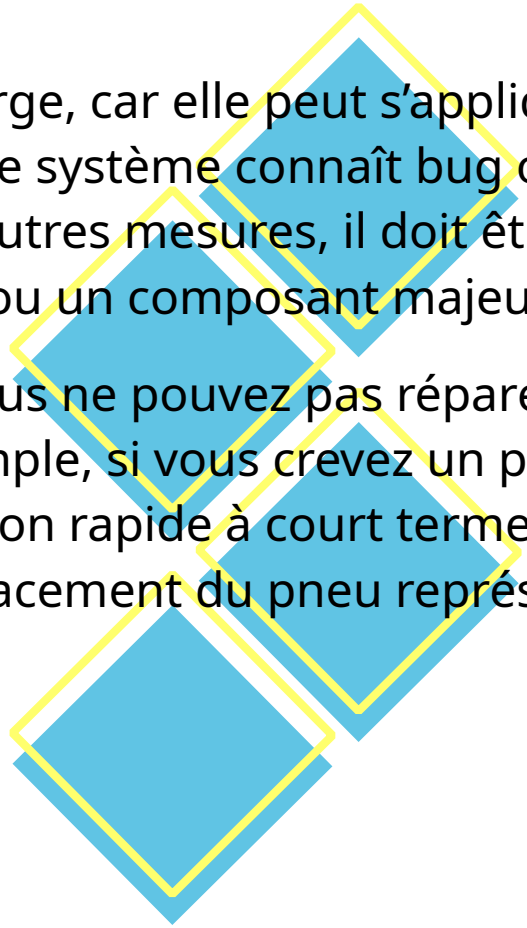
On parle également ici de maintenance curative.

Maintenance curative

Une maintenance curative est nécessaire lorsque votre machine est panne et qu'elle se trouve en très mauvais état. Après avoir instauré des **mesures correctives et préventives** sans succès, il est temps de mettre en place une **maintenance curative**. C'est le dernier recours de maintenance. En effet, la maintenance curative vous oblige à remplacer les pièces cassées voire l'ensemble du système.

La **maintenance curative** couvre un domaine assez large, car elle peut s'appliquer à des travaux mineurs ou majeurs. Si un élément de votre système connaît bug ou présente un défaut qui ne peut pas être corrigé par d'autres mesures, il doit être remplacé. Cela peut être une petite partie du système ou un composant majeur.

La **méthode curative** s'applique également lorsque vous ne pouvez pas réparer l'élément cassé par une solution permanente. Par exemple, si vous crevez un pneu de vélo, vous pouvez le réparer, mais ce n'est qu'une solution rapide à court terme. En fin de compte, le pneu a besoin d'être remplacé. Ce remplacement du pneu représente la méthode curative.

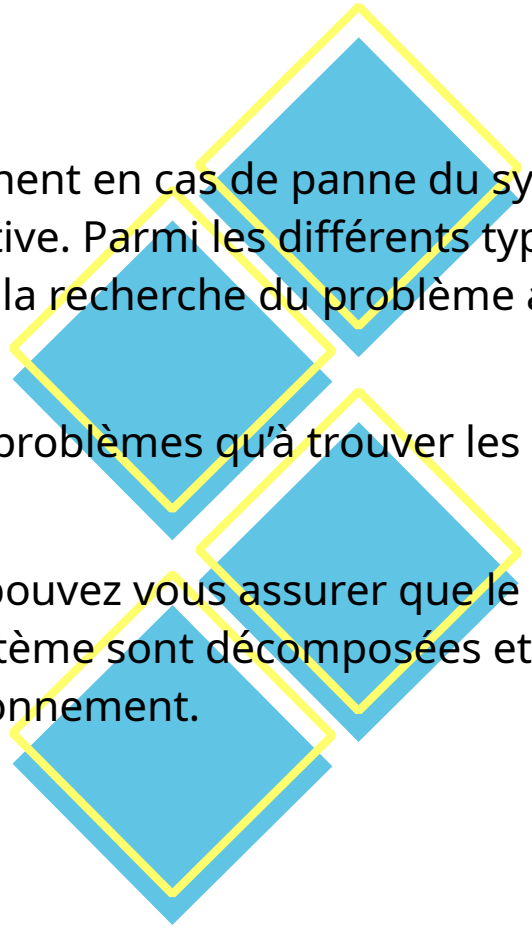


Maintenance préventive

Alors que les **maintenances corrective** et **curative** surviennent en cas de panne du système, la maintenance préventive adopte une approche plus proactive. Parmi les différents types de maintenance, la **maintenance préventive** se concentre sur la recherche du problème avant qu'il ne survienne ou avant qu'il ne devienne problème.

La **maintenance préventive** consiste moins à résoudre les problèmes qu'à trouver les faiblesses du système.

Avec des contrôles réguliers et des tâches de routine, vous pouvez vous assurer que le système fonctionne au mieux. Les différentes parties du système sont décomposées et observées pour s'assurer qu'elles sont en bon état de fonctionnement.



La **maintenance préventive** d’un système informatique est généralement réalisée via différentes plateformes logicielles. Il s’agit notamment des contrôles antivirus, des programmes d’exécution et de nettoyage et des programmes de mise à jour automatique.

D’autres formes de maintenance préventive peuvent également inclure la sauvegarde de vos fichiers et le nettoyage régulier de votre machine. Fondamentalement, tout ce qui prend une mesure de précaution pour éviter les problèmes avant qu’ils ne surviennent entre dans cette catégorie. Il s’agit de prendre certaines mesures pour aider le système à fonctionner au mieux.

En bref, les **maintenances corrective et curative** résolvent les problèmes tandis que la maintenance préventive les évite en premier lieu. C’est la différence majeure entre ces types de maintenance.

https://alifa-ing.github.io/monportfolio-github/activite.html

Merci pour votre généreuse attention et votre esprit participative

#PhilippeAlifa #TaïwèPhilippeAlifa @philipalifa.tpa