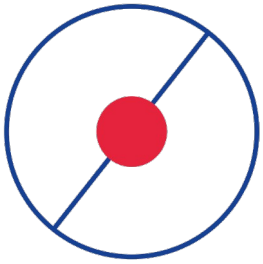
Gestion du patrimoine informatique

MARINE NATIONALE



Date de stage

Du 06/01/2025 Au 14/02/2025

Lycée Paul Louis Courrier – 37400, Tours
Arthur Duvoux 801 – BTS SIO Option SLAM
Gestion du patrimoine informatique de la DPMM Tours 06/01/2025

Sommaire

1. Introduction

La Direction du Personnel Militaire de la Marine (DPMM) de Tours est un organisme essentiel de la Marine nationale, chargé de la gestion des carrières et du suivi administratif des marins. Elle joue un rôle central dans le recrutement, la formation et l'affectation des personnels, veillant à répondre aux besoins opérationnels de la flotte. En plus de ces missions, la DPMM assure la mise en conformité réglementaire et participe à l'évolution des politiques de gestion des ressources humaines. Son implantation à Tours en fait un centre stratégique pour l'organisation et le pilotage des effectifs de la Marine.

2. Qu'est ce que la gestion du patrimoine informatique

La gestion du patrimoine informatique permet à une entreprise de prévenir les défaillances et de réduire les coûts associés aux systèmes d'information tels que les pannes, la maintenance et les consommables. C'est un ensemble de tâches administratives essentielles à la gestion et à la pérennité de l'entreprise, offrant une vue globale du système informatique et des informations qu'il contient.

3.Gestion du parc informatiques

a.Définition du parc informatique

Le parc informatique d'une entreprise désigne l'ensemble des équipements informatiques et des logiciels utilisés par celle-ci pour réaliser ses activités quotidiennes. Cela inclut les ordinateurs de bureau, les ordinateurs portables, les serveurs, les périphériques tels que les imprimantes et les scanners, ainsi que les équipements de réseau comme les routeurs et les commutateurs. En outre, le parc informatique englobe les logiciels d'exploitation, les applications métiers, les outils de productivité, et les solutions de sécurité. Une gestion efficace du parc informatique est essentielle pour assurer la continuité des opérations, la sécurité des données, et l'optimisation des ressources technologiques. Elle implique des tâches telles que l'entretien régulier des équipements, la mise à jour des logiciels, la gestion des licences, et la supervision des performances du réseau. Pour gérer son parc informatique, la DPMM de tours utilise son propre outil privé **SYMLEA**

b. Nommage des postes

La DPMM applique une politique de nommage stricte pour l'identification des postes informatiques, garantissant une gestion efficace du parc matériel et facilitant le suivi des équipements. Chaque unité centrale (UC) est nommée en fonction de l'adresse matérielle (MAC) de sa carte réseau Ethernet. (UC-AdresseMAC)

Ce système permet d'assurer une identification unique et standardisée des machines, facilitant leur intégration dans le réseau, leur maintenance et leur gestion à distance. De plus, cette méthode contribue à renforcer la sécurité et la traçabilité des équipements en limitant les risques de conflits ou d'usurpation d'identité sur le réseau interne.

c.Recensement du matériel

La DPMM assure le recensement et la gestion de son parc informatique à l'aide de son outil interne SYMLEA. Cet outil centralise l'ensemble des informations relatives aux équipements matériels et logiciels utilisés au sein de l'organisation.

SYMLEA permet d'enregistrer chaque configuration matérielle, incluant les caractéristiques détaillées des postes, serveurs et périphériques, ainsi que les composants logiciels installés sur chaque machine. De plus, il associe à chaque équipement des informations essentielles telles que l'utilisateur assigné, la date d'acquisition et l'historique d'utilisation.

Grâce à cette solution, la DPMM peut assurer un suivi précis et optimisé de son infrastructure, facilitant ainsi la maintenance, la gestion des mises à jour et le renouvellement des équipements en fonction de leur cycle de vie.

d. Déploiement des postes

Lorsqu'une commande de matériel est reçue par la DPMM, les équipements sont directement acheminés vers la **DIRISI** (Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information) de la localité concernée. À leur réception, les postes sont vierges, sans système d'exploitation ni configuration spécifique.

La DIRISI prend alors en charge la configuration initiale des machines. À partir d'un ghost national, elle déploie une image système standardisée, sélectionnée en fonction des composants matériels de chaque PC. Ce processus garantit une uniformité des installations et une compatibilité optimale avec l'environnement informatique de la Marine.

Une fois l'installation de l'OS terminée, les postes sont retournés à la DPMM, qui se charge d'installer les logiciels spécifiques nécessaires aux utilisateurs et d'effectuer les personnalisations en fonction des besoins opérationnels. Ce double processus assure à la fois une configuration sécurisée et une adaptation aux exigences métier des équipes.

e. Renouvellement du parc informatique

Le renouvellement du parc informatique de la DPMM suit un cycle d'environ cinq ans pour chaque composant. Toutefois, cette durée peut varier en fonction des besoins opérationnels et de l'état du matériel.

Dès 4,5 ans, une demande de remplacement peut être initiée afin d'anticiper le renouvellement et d'éviter toute obsolescence. Cependant, certains postes peuvent être maintenus jusqu'à six ans si leur performance reste adaptée aux usages. À l'inverse, d'autres équipements peuvent être remplacés de manière anticipée en cas de défaillance technique ou de besoin accru en ressources, notamment pour les utilisateurs nécessitant des performances spécifiques.

Cette gestion flexible permet d'optimiser le parc informatique en garantissant un équilibre entre durabilité, efficacité et adaptation aux évolutions technologiques.

f.Assistances

Pour la gestion des demandes d'assistance, la Marine nationale dispose de sa propre solution : **Diadème**. Installé sur l'ensemble des postes, cet outil fonctionne sur un système de ticketing, permettant aux utilisateurs de soumettre soit une demande de service, soit un signalement d'incident.

L'un des principaux avantages de Diadème est qu'il est directement pris en charge par une équipe dédiée, ce qui permet une résolution rapide et efficace des problèmes. Il arrive même que certaines interventions soient effectuées en arrière-plan, sans que l'utilisateur ait besoin d'interagir directement avec le support.

Cependant, quelques inconvénients sont relevés par les utilisateurs. Le principal est le manque de contact humain, rendant parfois le suivi des demandes moins intuitif. De plus, certaines assistances nécessitent d'être physiquement connecté au réseau interne de la Marine, ce qui empêche leur traitement à distance via un VPN.

g. Procédure de sauvegarde et de restauration mise en place

Pour garantir la sauvegarde des données, le gestionnaire du parc informatique de la DPMM a mis en place un script automatisé déployé sur l'ensemble des machines du réseau. Ce script, sous forme de fichier .bat, permet aux utilisateurs d'effectuer facilement une sauvegarde locale.

Le processus est simple : il suffit de brancher une clé USB formatée en NTFS, puis d'exécuter le script. Celui-ci sauvegarde alors automatiquement toutes les données utilisateur ainsi que la configuration du système. En cas de panne ou de problème majeur, la restauration est facilitée : il suffit de réinstaller l'ordinateur à partir de la clé USB pour récupérer l'ensemble des fichiers et paramètres.

Cependant, cette méthode présente une limite : la sauvegarde n'est pas automatisée et repose sur l'initiative de l'utilisateur, qui doit lancer manuellement le script. Ainsi, certains utilisateurs moins à l'aise avec l'informatique peuvent omettre de sauvegarder régulièrement, ce qui entraîne un risque de perte de données en cas d'incident. Une éventuelle évolution du système pourrait consister à automatiser ces sauvegardes pour pallier cette contrainte.

h. Mise à jour des OS

Le processus de mise à jour des systèmes d'exploitation suit la même méthodologie rigoureuse que celui des autres mises à jour logicielles. Lorsqu'une nouvelle version ou un correctif de sécurité est publié, le **Centre National de Configuration de l'Informatique (CNCI)** l'analyse afin d'évaluer son impact sur l'infrastructure informatique de la Marine. Si le test est concluant la mise à jour se donc déployé.

4.Gestion des projets et logiciels

a.Projets, externalisation?

La DPMM dispose de son propre pôle de développement, chargé de mener à bien divers projets, allant de la création de sites vitrines, comme lamarinerecrute.fr, à des solutions de gestion internes adaptées à ses besoins.

Pour structurer et piloter ces projets, la Marine utilise sa propre méthode de gestion, **PMSquare2**, qui repose sur un système de jalons. Le processus débute par une déclaration du besoin, suivie d'une demande d'autorisation visant à évaluer la viabilité et l'utilité du projet tout en vérifiant l'absence de solutions existantes. Une fois validé, le projet entre en phase de conception, avec la rédaction d'un cahier des charges détaillé. Vient ensuite la phase de développement, où l'outil Jira est principalement utilisé pour organiser les tâches, suivre l'avancement et coordonner les équipes. Une fois terminé, le projet passe en production et est maintenu jusqu'à sa fin de vie.

Pour accompagner cette méthodologie, la DPMM utilise plusieurs outils collaboratifs tels que **Tulipe, Resana et Klaxoon**, facilitant le suivi des projets, la communication entre les équipes et la gestion des différentes étapes du cycle de vie des développements.

L'externalisation est utilisée de manière occasionnelle, principalement en raison d'un manque ponctuel de personnel disponible. Avec de nombreux projets en cours, les ressources internes ne peuvent pas toujours gérer simultanément les missions les plus urgentes. L'externalisation permet également un gain de temps stratégique, comme ce fut le cas pour le projet lamarinerecrute.fr, où la DPMM a fait appel à un prestataire pour concevoir les maquettes Figma du site. À ce moment-là, aucun designer n'était disponible en interne, rendant cette externalisation nécessaire afin de permettre aux équipes de se concentrer pleinement sur le développement technique.

b.Normes

La DPMM ne suit pas strictement les normes ITIL (Information Technology Infrastructure Library), mais applique une méthodologie de gestion de projet propre à la Marine, PMSquare2. Cette méthode encadre le cycle de vie des projets en définissant des jalons précis, de la déclaration du besoin jusqu'à la fin de vie du produit.

Pour ces nombreux projets de développement la DPMM se conforme aux normes et bonnes pratiques des outils qu'elle utilise.

c. Sources des projets de développement et Versions

La gestion des sources des projets de développement au sein de la DPMM repose sur des normes et processus stricts afin de garantir la cohérence technique et la maintenabilité des solutions déployées.

Le suivi des versions des outils et programmes est encadré par plusieurs mécanismes. Les commissions SC2A jouent un rôle central en vérifiant les dossiers d'architecture technique, assurant ainsi que les logiciels utilisés respectent les normes du ministère des Armées (MinArm).

En complément, **le Cadre de Cohérence Technique (CCT)**, qui définit les standards et exigences techniques, est mis à jour tous les six mois. Cette actualisation régulière permet d'assurer une homogénéité entre les versions des logiciels et les infrastructures en place, garantissant ainsi un environnement stable et sécurisé pour le développement et le déploiement des applications.

d.Mise à jour des logiciels

Lorsqu'une mise à jour est publiée sur Internet, elle est d'abord analysée par le **Centre National de Configuration de l'Informatique (CNCI)**. Ce dernier étudie en détail la mise à jour afin d'évaluer son impact potentiel sur les systèmes de la Marine.

Le CNCI conçoit ensuite des tests approfondis pour vérifier la compatibilité et la stabilité de la mise à jour. Il élabore également des **masters** et des **packages de sécurité** adaptés aux infrastructures informatiques de la Marine.

Si les tests s'avèrent concluants, la mise à jour est validée et intégrée dans le processus de déploiement. Elle est alors diffusée de manière contrôlée à l'ensemble du parc informatique via **WSUS (Windows Server Update Services)**, garantissant ainsi une installation progressive et sécurisée sur les systèmes concernés.

5. Formations du personnel

a. Formations

La DPMM ne dispose pas d'un plan de formation fixe. Les formations sont mises en place en fonction des besoins spécifiques des postes, des exigences opérationnelles et du budget alloué. L'accès à la formation dépend donc des missions confiées à chaque membre et de l'évolution des compétences requises.

Par exemple, un personnel amené à occuper un poste exposé à des risques particuliers suivra systématiquement des formations adaptées pour renforcer ses compétences et assurer la sécurité des opérations. De même, lorsque de nouveaux outils ou technologies sont déployés, des sessions de formation peuvent être organisées afin de garantir une prise en main efficace par les équipes concernées. Toutefois, il arrive régulièrement que les membres de la DPMM apprennent à les utiliser de manière autonome, soit en-explorant les fonctionnalités par eux-mêmes, soit en s'appuyant sur la documentation fournie.

b. Veilles

Les membres de la DPMM assurent leur veille technologique de deux manières complémentaires. D'une part, la plateforme **Intradef** dispose d'un onglet dédié au partage des failles de sécurité récemment découvertes ainsi qu'aux actualités technologiques, permettant ainsi une diffusion centralisée des informations importantes.

D'autre part, chaque membre effectue également une veille personnelle, qu'il partage de façon informelle avec ses collègues. Par exemple, dans le bureau de développement, il n'est pas rare que des discussions spontanées émergent autour d'un sujet d'actualité technologique repéré par l'un des membres, favorisant ainsi un échange de connaissances en continu.

c. Utilisation de l'intelligence artificielle

L'intelligence artificielle est couramment utilisée au sein de la DPMM pour répondre à des questions et résoudre divers problèmes techniques. Toutefois, par mesure de sécurité, aucune donnée sensible ou relative à l'organisation n'est partagée avec des IA externes.

Par ailleurs, la DPMM utilise également sa propre IA, **Genial**, basée sur le modèle **Mistral**, afin de garantir un meilleur contrôle des informations traitées et une adaptation aux besoins spécifiques de l'institution.

6. La présence en ligne de la Marine nationale

a. Le site internet de la Marine nationale

La Marine nationale dispose d'un site internet officiel régulièrement mis à jour. Il sert à la fois de vitrine institutionnelle et de source d'information pour le grand public. On y retrouve les dernières actualités, les missions et engagements de la Marine, des informations sur les recrutements et carrières, ainsi que des ressources multimédias mettant en avant les opérations en cours et les événements maritimes majeurs.

b. Les réseaux sociaux où la Marine nationale est présente

La Marine nationale est présente sur plusieurs réseaux sociaux tels que Instagram, Twitter, Facebook, YouTube et LinkedIn. Elle y publie régulièrement du contenu à visée informative et promotionnelle, incluant des vidéos de ses opérations, des portraits de marins, des informations sur les exercices militaires ainsi que des conseils de prévention en matière de sécurité maritime. Grâce à sa large communauté en ligne, la gestion des réseaux sociaux est assurée par une équipe de communication dédiée, comprenant des Community Managers et des experts en stratégie digitale.

7. Protection des données

a. Responsable des données

Le responsable des données au sein de la Marine nationale est le Major général de la Marine. Bien que ses pouvoirs soient délégués à plusieurs organismes au sein de l'institution, il demeure l'autorité suprême en matière de gestion des données.

b.Métiers relatifs à la cybersécurité

Au sein de la Marine nationale, tous les métiers liés à la cybersécurité sont représentés. Parmi eux, on retrouve des **analystes en cybersécurité**, chargés de détecter et prévenir les cyberattaques, des **administrateurs systèmes et réseaux**, responsables de la sécurisation des infrastructures informatiques, ainsi que des **experts en forensic**, spécialisés dans l'analyse des incidents de sécurité et la traque des menaces.

La Marine dispose également de sa propre formation de spécialisation en cybersécurité destinée aux apprentis marins, leur permettant d'acquérir les compétences nécessaires pour protéger les systèmes d'information.

À l’issue de cette formation, un certificat en cybersécurité, délivré par la Marine, atteste de leur expertise dans ce domaine stratégique.

c. Mesures mises en place pour la protection des données personnelles

La DPMM met en place plusieurs mesures, tant légales que techniques, pour assurer la protection des données personnelles et leur conformité avec le RGPD (Règlement Général sur la Protection des Données).

Sur le plan technique, la transmission des données sensibles est sécurisée grâce à l’utilisation du logiciel de chiffrement **ACID**, qui garantit la confidentialité des informations échangées. De plus, l’accès aux données est strictement régi par un système d’habilitation, ce qui signifie que seules les personnes disposant des autorisations nécessaires peuvent y accéder.

D’un point de vue réglementaire, la DPMM applique rigoureusement les directives du RGPD en assurant une gestion responsable des données, incluant la limitation de leur accès, leur sécurisation et leur traçabilité, afin de prévenir tout risque de fuite ou d’usage inapproprié.