Ce document contient 12 pages.

## 1.1 ARCHITECTURE TECHNIQUE

CGX propose une offre en mode SaaS (Software As A Service) reposant sur une infrastructure virtualisée au sein de Datacenters haute disponibilité.

Afin de répondre aux exigences de ses clients et aux normes actuelles, les moyens mis en œuvre par CGX sont :

- Des infrastructures Datacenters hautement sécurisées et normalisées
- Un réseau IP consolidé auprès des grands acteurs du marché,
- Un socle sécuritaire conforme aux règles de l'art,
- Des équipes professionnelles rigoureuses et consciencieuses.

Toute application demandant aujourd'hui un niveau de disponibilité élevé doit disposer d'une couche de virtualisation. La solution proposée par CGX s'appuie donc sur la performance du matériel et sur les couches de virtualisation.

Ainsi CGX choisi des serveurs physiques supportant spécifiquement la couche de virtualisation.

L'espace de stockage est supporté par des baies SAN reconnues pour leurs performances et leur fiabilité.

Le but de cette architecture est de pouvoir augmenter les espaces de stockage de manière quasi infinie. Dans ce cas, les volumétries peuvent atteindre plusieurs téraoctets de données.

## 1.2 LE DATACENTER

La plateforme d'hébergement CGX, située à Castres est un Data Center constituée de deux salles blanches destinées à l'exploitation des applications hébergées. L'équipe en charge du Datacenter est certifiée ISO 27001.

### 1.2.1 Alimentation en énergie

Le site est rattaché en deux points distincts au réseau de distribution EDF (réseau bouclé), ceux-ci étant alimentés par deux sources électriques indépendantes.

De plus, un groupe électrogène permet de secourir les accès EDF et assure à l'ensemble du site une autonomie de fonctionnement de 24 heures. La continuité de fonctionnement durant le temps nécessaire au basculement sur le groupe électrogène est assurée par un onduleur.

## 1.2.2 Interconnexion réseau

Notre FAI territorial, est connecté (en BGP4) aux backbones de l'Internet. Ce positionnement multi-FAI vise la continuité de service pour les fournisseurs hébergés en zone DMZ. Tout système hébergé dispose d'une bande passante Internet mutualisée (entre 100 Mbps et 2,5 Gbps symétrique).

## 1.2.3 Climatisation

La régulation thermique et hygrométrique des salles d'hébergement est assurée par un groupe froid et deux climatisations indépendantes, garantissant une température ambiante constante et une humidité relative pour assurer un fonctionnement optimal des appareillages électriques.

## 1.2.4 Sécurisation incendie

La détection incendie du Datacenter est conforme à la règle 7 APSAD (Assemblée plénière des Sociétés d'Assurances Dommages) relative à la détection automatique d'incendie, au code du travail et à la loi du 19 juillet 1976 concernant les installations classées pour la protection de l'environnement. Les salles blanches sont équipées d'un système de détection d'incendie et d'un système d'extinction automatique à base de gaz internes (FM 200), non destructifs pour les équipements et non dangereux pour l'homme.

La protection incendie du Datacenter est conforme à la règle R2 APSAD relative à l'extinction automatique par gaz avec des adaptations propres au NFPA 2001 concernant les produits de substitution à l'Halon et à l'ensemble des règles concernant la protection des personnes. Le système garantit l'extinction des débuts d'incendie sans dommages pour les équipements.

Les process et la méthodologie mise en place dans le Datacenter pour le compartimentage, la sécurité et l'évacuation des personnes est conforme à la norme NFS 61 930. Une procédure d'évacuation rapide dès le déclenchement de l'alarme incendie permet au personnel de quitter la salle avant le lancement du système d'extinction.

## 1.2.5 Protection anti-intrusion

Le Data Center est équipé d'un système d'alarmes sur détection de mouvements, d'ouverture de porte avec effraction (contacts magnétiques), et de bris de glace.

Les Datacenters sont équipés d'un système de vidéosurveillance afin de superviser en temps réel les espaces d'hébergement et zones d'accès. L'enregistrement d'images est déclenché automatiquement sur détection de mouvement. La gestion de la vidéosurveillance est associée à un enregistrement avec stockage des images sur 30 jours.

Seul le personnel technique habilité peut entrer dans les salles (Zones d'accès restreint à certains employés spécifiques correspondant à la norme EN 50600-1 de classe 3).

L'ouverture de la porte d'accès aux salles blanches est soumise à une demande d'accès et est actionnée par badge associé, chaque badge permettant d'identifier son porteur de manière unique. Une centrale de contrôle des accès réalise des enregistrements hebdomadaires de tous les accès.

Tout branchement de support mobile est interdit sur notre infrastructure. Dans tous les cas, les accès aux différents ports des matériels physiques (USB ou autre) sont désactivés dans les couches de virtualisation.

La sécurité logique se définit par les trois points suivants :

- Sécurisation des accès en administration (authentification, traçabilité, audit et conformité)
- Politique de sécurisation des réseaux (FIREWALL, SSH, HTTPS, VPN, VLAN)
- Plan de sauvegarde (réplication chiffrée externalisée)

Le Data Center est doté d'un NOC (Network Operations Center). Il s'agit d'un mur d'écran visible par l'ensemble de l'équipe technique. Celui-ci reçoit les alertes et affiche en temps réel tout type de problème pouvant survenir (sauvegarde, indisponibilité d'un service, saturation réseau, bande passante…).

## 1.3 LA VIRTUALISATION DES SERVEURS

### 1.3.1 Vecteur de performances

La solution mise en place repose sur une architecture virtualisée. La virtualisation permet d'optimiser la répartition de la charge de travail entre les différents serveurs. Il est possible de moduler la puissance des machines virtuelles en fonction de la criticité de la tâche à exécuter. Ainsi leur attribuer plus ou moins de cœurs de CPU virtuels, ou plus ou moins d'espace disque. Cela permet d'optimiser les ressources du parc informatique.

La migration à chaud des machines virtuelles entre serveurs physiques permet également de répartir la charge de travail entre les serveurs. Lorsqu'une machine virtuelle monte en charge de façon extrême, les autres pourront se replier sur un serveur physique moins sollicité.

La performance de la virtualisation est donc liée en premier lieu au socle matériel ou chaque machine physique doit avoir des caractéristiques performantes. L'infrastructure matérielle doit être capable de répondre aux charges de traitement des machines virtuelles qui utilisent les fonctionnalités du système avec des configurations par défaut.

Par exemple, une configuration où le serveur de site et le serveur SQL sont installés sur la même ressource matérielle peut limiter les performances. Nous conseillons d'utiliser une configuration avec une machine serveur SQL séparé.

En règle générale, les facteurs clés qui limitent les performances de l'ensemble du système sont les suivants, par ordre d'importance :

1. Performances d'E/S du disque
2. Mémoire disponible
3. L'équilibrage des ressources Processeur

#### 1.3.1.1 Soigner l'espace de stockage

L'espace de stockage doit être pensé et réparti en fonction des flux des différents serveurs au risque de provoquer de la contention. Il conviendra de minimiser les appels simultanés au même volume de stockage et positionner les machines virtuelles en conséquence pour éviter ainsi les baisses de performance.

Pour des performances optimales, on préfèrera des configurations RAID 10 pour tous les lecteurs de données et une connectivité réseau Ethernet 1 Gbit/s. La technologie RAID basée sur le matériel requiert des contrôleurs spéciaux (ISCSI, SATA, SAS, …) qui sont recommandés. L'utilisation de SSD favorise grandement les performances.

#### 1.3.1.2 Dimensionner la mémoire

La quantité de mémoire nécessaire est directement liée au nombre de machines virtuelles.

Il est particulièrement important d'essayer d'éliminer autant que possible l'utilisation de fichiers d'échange (*swap*). Augmenter la mémoire vive d'un serveur Web augmente directement ses performances. Il est important d'ajuster au mieux la quantité de mémoire vive à une machine virtuelle.

La performance de la mémoire est dépendante de son débit de transfert de données. Les mémoires de type DDR4 sont à privilégier.

#### 1.3.1.3 Répartir les cœurs

Une machine virtuelle peut être allouée avec des sockets virtuels et plusieurs cœurs par socket. L'accroissement des besoins en ressources CPU a permis l'émergence des architectures multicœurs. De plus, les hyperviseurs actuels savent parfaitement gérer un système multiprocesseur dans lequel les zones mémoire sont séparées et placées en différents endroits. Il est fortement recommandé que l'infrastructure virtualisée repose sur des processeurs 64 bits permettant l'accès direct aux différents périphériques de la carte mère de l'hôte pour une utilisation plus efficace des processeurs virtuels (vCPU) des machines virtuelles.

Le processeur devrait disposer de la technologie Hyper-Threading pour augmenter le nombre de cœurs disponibles.

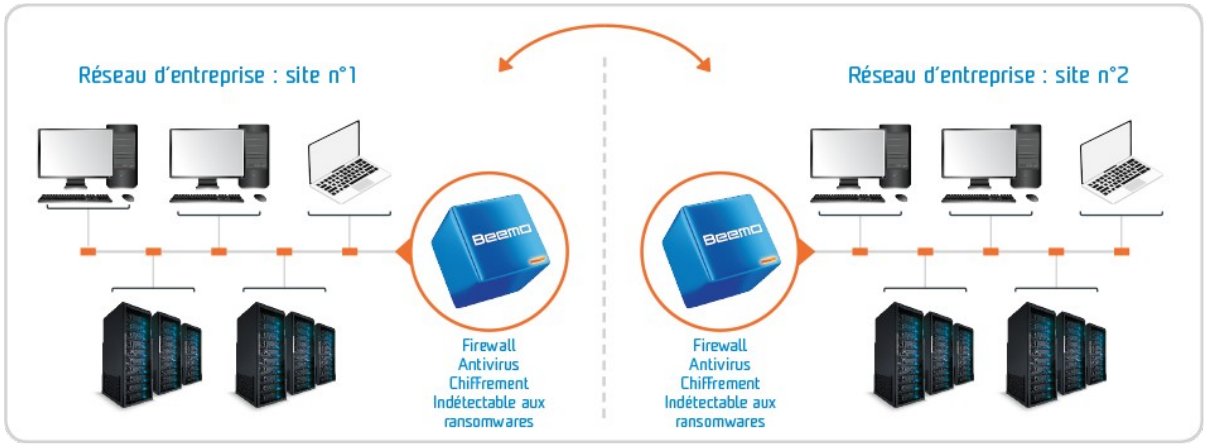
Les machines virtuelles hébergeant une base de données qui gèrent en règle générale le « multithreading », se verront affecter plusieurs vCPU. Il conviendra d'analyser les allocations de vCpu alloués aux machines virtuelles et veiller à limiter cette allocation sous 6 vCPU par cœur logique pour préserver le pourcentage de *cpu ready*.

## 1.3.2 Solution de sauvegarde

Beemo Technologie propose des solutions complètes et fiables pour assurer la sauvegarde des données et la reprise d'activité en cas de sinistre. La technologie de sauvegarde Data Safe Restore conçue par Beemo fournit un ensemble de fonctionnalités et de services qui en font une technologie de référence sur le marché de la sauvegarde informatique. Là où d'autres solutions proposent une sauvegarde des données soit locale soit externe, la technologie Data Safe Restore réunit ces deux niveaux afin de garantir une sécurité optimale des données.

La solution Beemo2Beemo permet de conserver le contrôle des données. D'abord sauvegardées sur une Beemo placée sur un premier site de l'entreprise, les données sont ensuite externalisées sur une seconde Beemo placée sur un site distant. Il n'y a aucun hébergement externe, toutes les données restent au sein de l'entreprise.

Plusieurs configurations sont également possibles en fonction des besoins de sauvegarde. Beemo2Beemo permet d'installer autant de Beemo que nécessaire qui pourront se sauvegarder les unes sur les autres ou de centraliser toutes les sauvegardes des différentes Beemo sur une seule. La solution Beemo2Beemo est modulable et s'adapte à toutes les architectures réseaux, de la plus simple à la plus complexe.




Les principales fonctionnalités sont :

- Compatible tous systèmes d'exploitation
- Sauvegarde à chaud de bases de données SQL

- Sauvegarde à chaud de machines virtuelles
- Sauvegarde MS Exchange en mode feuille à feuille
- Sauvegarde d'un nombre illimité de versions
- Restauration Universal *Bare Metal*
- Restauration 24h/24, 7j/7
- Restauration sélective des fichiers sauvegardés
- Restaurations illimitées

## 1.3.3 Supervision de l'architecture

La totalité des serveurs dispose des modèles de supervisions déployés habituellement complétés par une métrologie dédiée à ce projet.

Les bases de données bénéficient d'une surveillance toute particulière, tout comme les liens inter-serveurs. Il en va de même sur les liens réseaux reliant les serveurs aux équipements de stockage.

CGX assure la maintenance de toutes les machines hébergées. Un monitoring continu (24h/24) permet d'observer et de conserver la qualité de service. Les graphes générés permettent d'apprécier l'utilisation des différentes ressources au cours du temps (trafic, bande passante, cpu, espace disque, …).

De plus, le service exploitation est averti en temps réel de tout incident afin de réduire au maximum les temps d'intervention.

### *1.3.3.1 Solution logicielle pour la supervision*

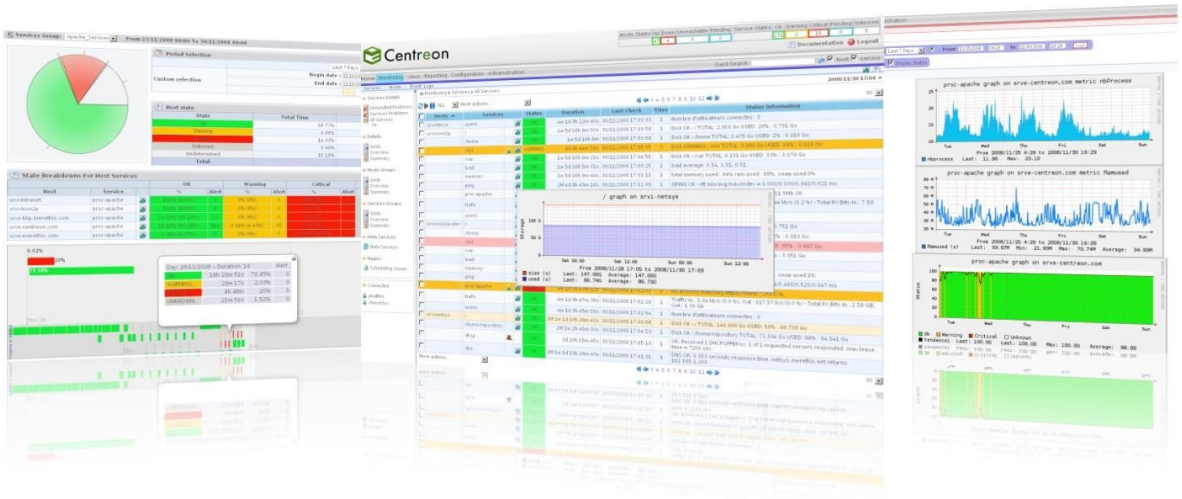
La surveillance du système est assurée avec le logiciel de surveillance Centreon. Centreon est un logiciel de surveillance Open Source gratuit, publié par société Centreon French. Il mesure la disponibilité et les performances des couches d'application, l'expérience utilisateur aux ressources matérielles.

Centreon offre de nombreuses fonctionnalités telles que la consultation des états des services et des équipements surveillés, la métrologie, le *reporting*, l'accès aux événements de surveillance, la gestion avancée des utilisateurs via des listes de contrôle d'accès (ACLs).

Mature, fiable et innovant, Centreon se distingue par sa capacité à offrir une plateforme adaptée à la vision « métier » requise par le responsable, tout en structurant les données de base informatiques (disponibilité, capacité, maintenabilité, fiabilité).

La distribution et les performances illimitées du système de collecte de données sont également parmi les points forts de la suite logicielle. Centreon répond aux contraintes d'évolutivité, de partitionnement réseau, de sites géographiquement fragmentés et de bande de passe limitée.




**CONFIGURATION PRÊTE** : Centreon est entièrement intégré avec CentOS, les composants système et les éléments interdépendants associés aux systèmes RHEL - tous emballés en utilisant le format RPM ; inclut des plugins essentiels comme la gestion via SNMP.

**ÉVOLUTIF** : intégrant à des sites, des appareils et leurs dépendances supplémentaires tout en maintenant une surveillance homogène des opérations distribuées, couvrant jusqu'à 500 000 points de contrôle de service.

**ILLIMITÉ** : Centreon peut incorporer à autant de ressources informatiques et de sites que nécessaire (aucune limite d'hôte ou d'appareil).

**COMPLET** : plate-forme opérationnellement robuste qui inclut des composants préconfigurés et des hiérarchies d'objets parent-enfant logiques, ainsi qu'une console Web conviviale pour un suivi large ou granulaire.

**GRATUIT** : installer et déployer en quelques minutes – sans tabou.

### *1.3.3.2 Architecture*

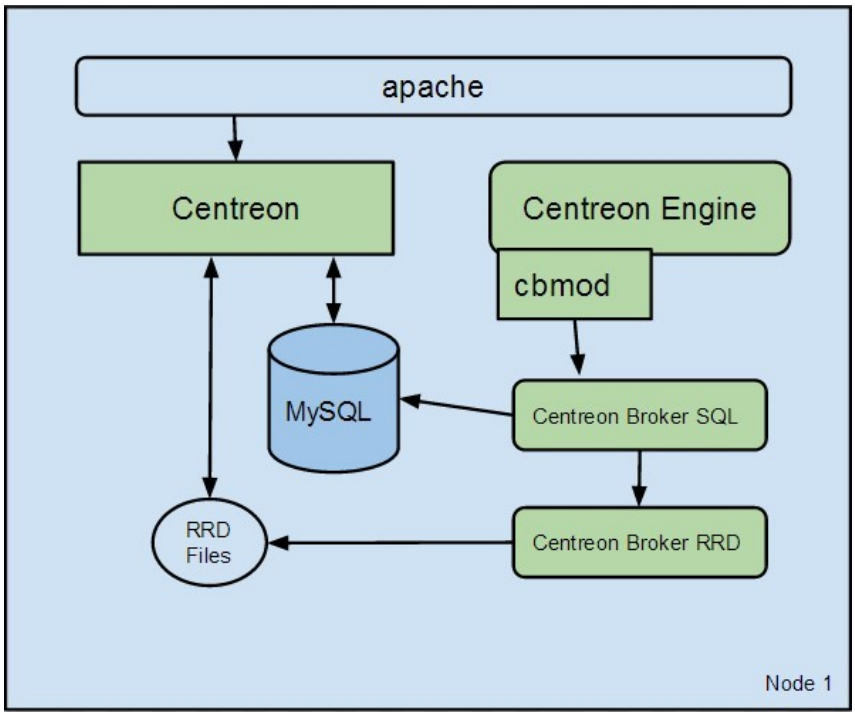
L'architecture simple de Centreon consiste à avoir toutes les entités de supervision au sein du même serveur, c'est-à-dire :

1. Centreon web interface
2. Base de données (MySQL + RRD)

3. Moteur de Supervision
4. Le connecteur entre les différents ordonnanceurs de collecte (*Broker*)

Cette architecture est la plus simple qu'un utilisateur puisse rencontrer.




Modulaire et ouvert, la plate-forme de surveillance complète de Centreon comprend trois composants logiciels *open source* majeurs, entièrement optimisés pour fonctionner au mieux ensemble : **Centreon Engine**, **Centreon Broker** et **Centreon Web**. Une API native facilite la configuration automatisée ; par exemple, pour ajouter, supprimer ou mettre à jour des objets hôte et service, ainsi que pour les synchroniser ou redémarrer un *poller* de surveillance à distance.

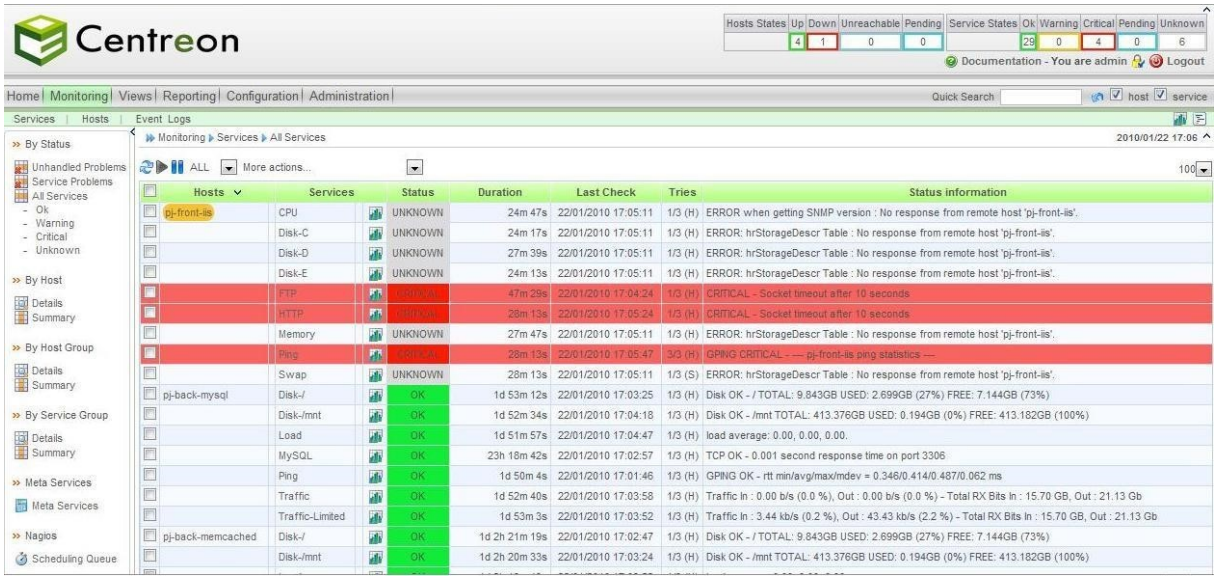
**Centreon Engine** est un puissant système de collecte de données d'indicateurs de surveillance universels pour les principaux systèmes d'exploitation, serveurs, actifs d'infrastructure et ressources. Il couvre des mesures système étendues, des équipements réseau, des protocoles, des applications et des services. Initialement développé sur Nagios® 3.2.3, Centreon Engine assure la continuité de la surveillance pour les utilisateurs de Nagios® environnement et de protocoles open source similaires, mais avec des performances et des fonctionnalités qui surpassent les meilleures performances de l'industrie. Cela est particulièrement vrai en termes d'efficacité des ressources, d'empreinte de consommation et d'intégration avec les systèmes existants dans le cloud et les machines virtuelles.

**Centreon Broker** est le multiplexeur qui assure des transmissions de données fluides et autonomes vers la console de surveillance tout en traitant les événements et en analysant les corrélations pertinentes. Il a été préparé et testé pour traiter jusqu'à 500 000 vérifications de service toutes les 5 minutes, hébergées avec une instance du *daemon broker* - l'une des plus étendues de l'industrie.

Cette innovation Centreon permet un mécanisme de basculement en cas de liaisons de chute pour garantir aucune perte de données pour les environnements surveillés par Centreon. Il offre également un moyen efficace de stocker et de communiquer les résultats surveillés via une base de données centrale et structurée de manière autonome avec des fonctionnalités de cryptage de sécurité alignées sur DMZ. Centreon Broker est compatible avec les bases de données backend telles que MySQL, MariaDB, RRDTool et InfluxDB.

**Centreon Web** est la console de surveillance universelle offrant des vues opérationnelles concises, faciles à comprendre et à gérer. Les administrateurs système, les gestionnaires de réseau, l'équipe des opérations ou les décideurs informatiques maîtrisent instantanément leur environnement surveillé et de façon globale grâce à l'interface conviviale et solide, à des tableaux de bord simples, à des commandes et widgets à l'écran pour afficher les informations. Garder un œil sur la transmission de l'état, le trafic réseau, les événements et les journaux de performances, les données historiques du journal, les transactions du serveur, etc… devient sans effort pour une surveillance fiable en continu.




## 1.3.4 Audit de l'infrastructure

Tous les services d'infrastructures (électricité, CVC, Incendie…) sont régulièrement testés afin d'améliorer continuellement le niveau de qualité fourni.

Ces tests sont réalisés par les personnels en charge du maintien des datacenters afin de valider le bon fonctionnement des solutions mises en place, et, le cas échéant, procéder aux modifications nécessaires.

Si le client le souhaite, nous pouvons faire visiter nos installations afin d'apprécier le niveau de sécurité fourni par notre infrastructure.

Nos infrastructures peuvent être auditées sur demande.

De plus, le service exploitation est averti en temps réel de tout incident afin de réduire au maximum les temps d'intervention.

### 1.3.5 Interruption du service à des fins de maintenance préventive et corrective

CGX pourra interrompre le service à des fins de maintenance de ses centres serveurs ou de leurs systèmes d'exploitation. Ces interruptions ont lieu aux moments de la journée ou de la nuit, les moins préjudiciables au trafic du serveur.

L'horaire prévu pour l'interruption sera déterminé d'un commun accord entre le Client et CGX, tenant compte de la fréquentation du serveur.

Dans le cas d'application automatique de patchs logiciels (OS ou application), nous utilisons par défaut une programmation hebdomadaire nocturne. Il peut être déterminé un horaire ad-hoc.

En cas de nécessité absolue, notamment pour des problématiques de sécurité, CGX se réserve le droit d'une intervention immédiate sur tout matériel de sa plateforme technique.

Le Client sera alors prévenu des indisponibilités (au moins deux jours à l'avance pour les opérations préventives).

### 1.3.6 Confidentialité

L'article 6-I-2° de la loi pour la confiance dans l'économie numérique stipule que l'hébergeur a pour obligation la collecte des données permettant l'identification des personnes insérant du contenu dans un site et la suppression de tous contenus illicites qui lui auraient été signalés.

Le client et CGX peuvent, dans le cadre de leur collaboration, avoir accès à des informations confidentielles appartenant à l'une ou l'autre des parties et s'engagent à protéger ces informations confidentielles comme s'il s'agissait de leurs propres informations.

« Informations confidentielles » s'appliquent à tout document écrit, données ou informations indiquées comme confidentiels par la partie qui remet cette information à l'autre partie et ce, en accord avec les règles habituelles de la profession.

CGX certifie que les employés ou préposés à son service ont accepté ces règles et principes de confidentialité.

CGX s'engage donc à respecter les obligations suivantes et à les faire respecter par son personnel :

- Ne réaliser aucune copie des documents et support d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la prestation.
- Ne pas utiliser les documents et informations traités à d'autres fins que celles prévues au titre du présent marché.
- Ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales.
- Prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des données informatiques gérées.
- Prendre toutes mesures de sécurité, notamment matérielles, pour assurer la conservation et l'intégrité des documents et informations traités.

## 1.3.7 Plan de gestion de la sureté de l'information

### *1.3.7.1 Introduction*

La protection des données et des informations ne se réduit pas à une réponse technique du département informatique. Aujourd'hui, les informations critiques et confidentielles peuvent être dispersées. En outre, une organisation peut se voir confier des informations sur des employés, des dossiers de santé, des données financières, des propriétés intellectuelles, etc., sans en être propriétaire. Il faut plus que des pares-feux et des équipements avancés même couplés à des sauvegardes pour assurer la sécurité des données.

CGX SYSTEM a relevé ce défi depuis plusieurs années en impliquant tout le personnel, la direction et les cadres pour développer une culture de la sécurité de l'information qui utilise judicieusement les actifs technologiques, forme le personnel à traiter les informations confidentielles avec intégrité et prévoit une amélioration continue face à l'escalade des menaces.

### *1.3.7.2 La gestion de la sûreté de l'information*

La gestion de la sûreté des informations (ISMS) définit les contrôles qui protègent les informations confidentielles, sensibles et personnelles contre les dommages, le vol ou l'utilisation abusive, ainsi que les rôles et responsabilités liées à ces activités.

Les informations se présentent sous de nombreuses formes, présentent des degrés de risque variables et exigent des méthodes de protection adaptées. Il faut considérer à la fois les éléments humains et comportementaux dans ces contrôles, ainsi que la technologie mise en œuvre pour contrecarrer les attaques, les violations et les abus.

La gestion de la sûreté de l'information aide à rester au fait des menaces et des vulnérabilités, à minimiser et à atténuer les risques et à assurer la continuité des activités. Avec l'augmentation des risques de cybersécurité, la gestion de la sûreté de l'information est devenue encore plus importante. Ce qui conduit à imposer des exigences en matière de stockage, d'utilisation, de transmission et de mise au rebus qui sont surveillées et améliorées régulièrement pour répondre aux exigences organisationnelles, managériales et techniques qui empêchent la divulgation d'information de façon accidentelle ou intentionnelle.

Les systèmes de gestion de la sûreté de l'information (ISMS) sont constitués de contrôles, de processus, de plans et de politiques continuellement mis à jour au fur et à mesure que les besoins en matière de sécurité changent. Les politiques doivent tenir compte de la culture de l'organisation et de ses facteurs de risque, et doivent également considérer les influences extérieures, comme par exemple l'environnement réglementaire.

Un ISMS n'est pas une structure universelle, mais il est construit en considérant les besoins organisationnels, l'évaluation des risques et les vulnérabilités connues. La taille des entreprises, les réglementations de l'industrie et les exigences en matière de sécurité, les processus et les objectifs globaux sont également pris en compte dans l'élaboration de l'ISMS. L'ISMS fournit un niveau d'assurance des risques fondé sur la maturité des processus et l'étendue de leur mise en œuvre.

Le Plan de Gestion Sûreté de l'information (ISMP) décrit le Système de Gestion de la Sûreté de l'information mis en place dans le cadre de ce projet, de la notification du marché, jusqu'à la fin de l'exécution du marché et plus largement pendant toute la durée contractuelle. Il définit et met en œuvre des contrôles axés sur l'exécution du système d'information, des méthodes de sécurité et des contrôles techniques associés aux solutions technologiques.

Ce plan de gestion de la sûreté de l'information comprend des garanties de gestion, opérationnelles et techniques. Vous trouverez en annexe une proposition décrivant le contenu de notre plan de gestion de sûreté de l'information. Cette trame sera révisée, validée en début de projet. Il servira de référence pour l'exécution du processus de sûreté, en cohérence avec le processus de développement de la solution.

**Fin du document**