DATACENTER ASPSERVEUR LA CIOTAT
CAHIER TECHNIQUE

VERSION 03/11/2015

VOS INTERLOCUTEURS

Pour la relation commerciale

Franck ZWILLER
Responsable commercial Sud

DIGITAL DIMENSION – ASPSERVEUR
Tel. 0805 360 888
e-mail : f.zwiller@aspserveur.com

Table des matières

I. Présentation du Groupe 3
1. Digital Dimension | Econocom 3
2. ASPSERVEUR 3
II. Les services 4
1. Colocation 4
2. Suites privatives 4
3. Extranet Client dédié 4
III. Cahier technique 5
1. Le Datacenter ASPSERVEUR 5
a. Risques d'inondation 6
b. Risques sismiques 6
c. Risques de foudre 6
d. Risques incendie 6
e. Risques industriels 7
f. Transport de matières dangereuses 7
g. Risques aériens 7
h. Risques économiques 7
i. Accès humain 7
j. Accès matériel/Coffre-fort 7
k. Contrôle d'accès et anti-intrusion 8
l. Télécom 9
m. Les baies APC NetShelter 9
n. Respect de l'environnement 10
o. Dispositifs de redondance 10
p. Disponibilité contractuelle 11
IV. Sécurité (extrait du Plan Assurance Sécurité) 12
1. Organisation de la sécurité 12
a. Suivi 12
b. Gestion de la confidentialité 12
c. Révision 12
2. Sécurité physique 12
a. Gestion des accès physique 12
b. Dispositifs d'alertes 13
3. Gestion des documents 13
a. Gestion des documents électroniques 13
b. Gestion des documents papiers 13
c. Gestion des supports de stockage 14
4. Sécurité de l'exploitation 14
a. Gestion des postes de travail 14
b. Sécurité des serveurs 14
c. Gestion des sauvegardes 15
d. Gestion des traces 16
e. Sécurité réseau 16
f. Gestion des accès à distance 16
g. Accès à internet en interne 17
h. Continuité des services 17

I. Présentation du Groupe

1. Digital Dimension | Econocom

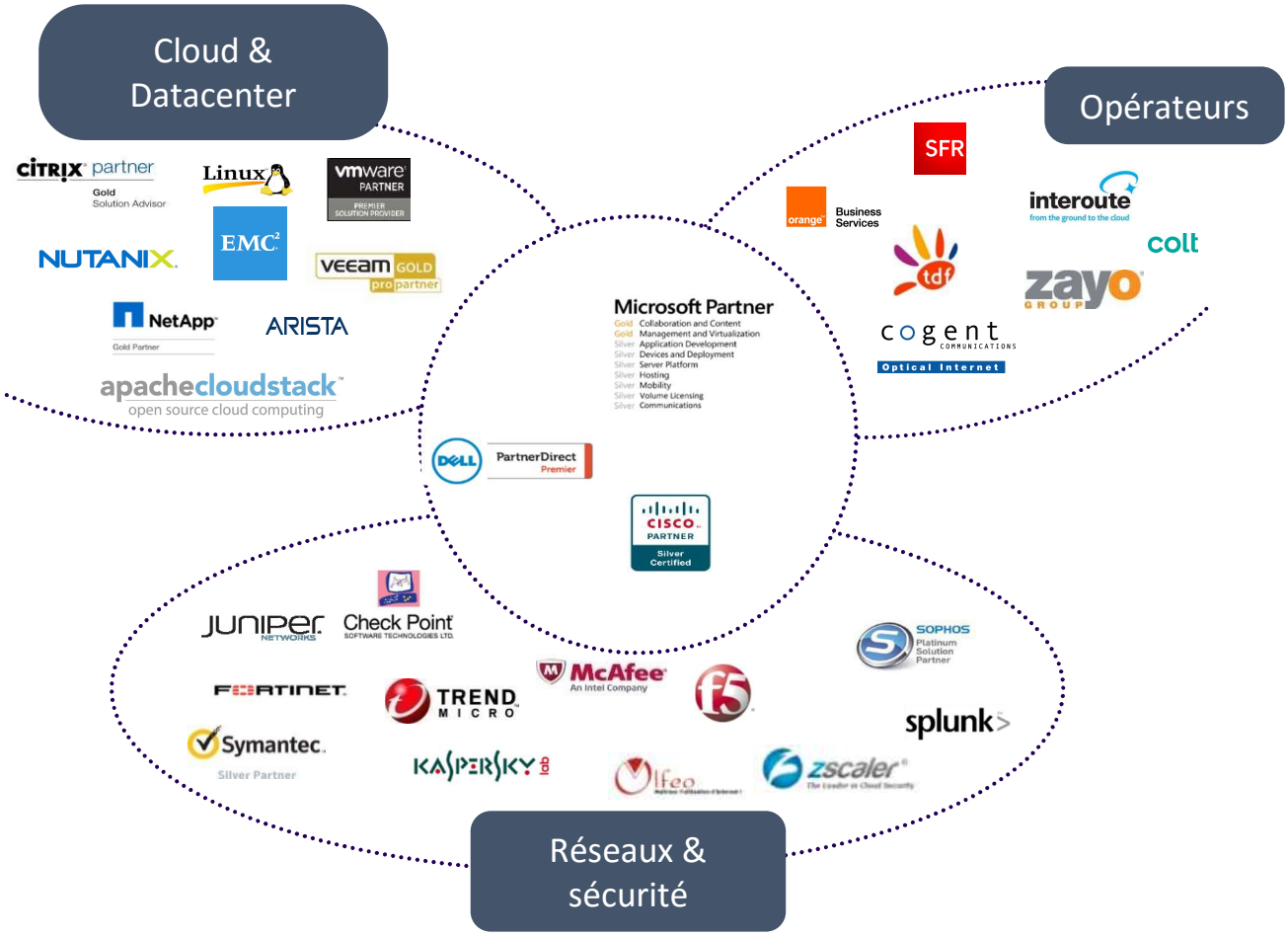
Spécialiste des services numériques pour les entreprises le groupe ECONOCOM gère 6 millions d'assets informatique dans 20 pays pour un CA de 2.1 milliards d'euros et 8000 collaborateurs.
ECONOCOM est une entreprise de droit français cotée à l'EURONEXT.
ECONOCOM est le 6ème acteur en service d'infrastructure en France (Classement SITSI PAC 2015)

Digital Dimension est une filiale du groupe ECONOCOM qui propose de faire du Digital la nouvelle clé de la performance et de l'innovation des entreprises.
Basée au départ sur une politique d'acquisition des entreprises de pointe Digital dimension propose les services de mobilité et les services d'infrastructures IT à forte valeur ajoutée.

2. ASPSERVEUR

Depuis son rachat en aout 2014 ASPSERVEUR est la « Business Unit » française du groupe spécialisée dans l'hébergement critique et l'infogérance.

Propriétaire de son propre Datacenter ASPSERVEUR est un partenaire innovant qui maitrise l'ensemble des technologies leader sur le marché.



II. Les services

1. Colocation

ASPSERVEUR propose les services de colocation en Datacenter suivants :

- Housing
- Location de baies, demi-baies
- Eyes & Hands (gestes de proximité) ou infogérance complète en 24/7
- Interconnexion fibre, MPLS, VPN, Hertzien
- Transit IP
- Gestion de classes d'adresse IP (membre du RIPE)
- Gardiennage 24/7
- Monitoring et télésurveillance

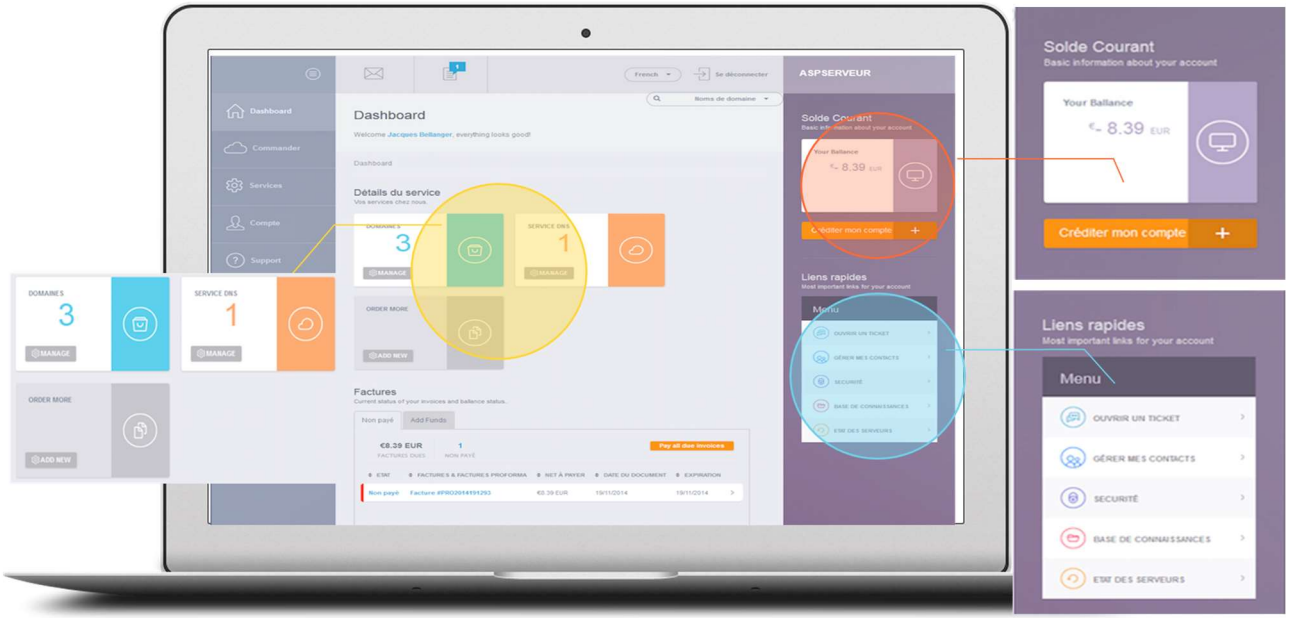
2. Suites privatives

ASPSERVEUR se propose d'étudier pour vous toutes réalisations de suites privatives au sein de son Datacenter de La Ciotat. En partenariat avec APC by SCHNEIDER (leader mondial du Datacenter) et APL France (experts depuis 32 ans dans l'audit et la conception de Datacenters) nous sommes en mesure de répondre de manière pragmatique aux cahiers des charges les plus exigeants.

Nous proposons à la demande des environnements dédiés éligibles aux certifications (ISO 27001, ISO 9001, ISO 20000, PCI-DSS, Secret défense, ZRR) et aux normes de disponibilité les plus hautes (TIER III+, TIER IV).

3. Extranet Client dédié

Notre Extranet client dédié compatible tablettes et mobiles vous permet d'administrer et de monitorer tous les services de votre Datacenter à distance.



III. Cahier technique

1. Le Datacenter ASPSERVEUR

Créé en 2009, notre Datacenter de nouvelle génération propose des spécificités uniques sur le marché.

Une disponibilité sans faille
Prouvée par un organisme indépendant depuis la mise en service en 2009 : énergie 100%, climatisation 100%, réseau 100%.
Ces résultats sont rendu possibles par l'utilisation systématique de la quadruple redondance pour tous les systèmes critiques du Datacenter (conception de type TIER IV de l'Uptime Institute).

Respect de l'environnement
Avec un PUE (Power Usage Effectiveness) inférieur à 1.4 notre Datacenter détient le record français en termes d'efficacité énergétique.
Chez nous le PUE est calculé en temps réel et validé par un projet ADEME, il ne s'agit pas d'un PUE théorique de conception.

Record de densité
Jusqu'à 28 kW disponibles par baie.
Les Datacenters traditionnels se contentent de 750 watts par m2 ce qui est largement insuffisant pour pouvoir utiliser les 42 unités d'une baie avec les serveurs actuels.
Notre Datacenter est en capacité d'accueillir les systèmes modernes les plus énergivores comme les solutions hyper-convergente (NUTANIX, UCS CISCO), les serveurs BLADE ou les supercalculateurs.

a. Risques d'inondation

Les risques sont ramenés à une valeur proche de zéro :

- Le terrain d'implantation du Netcenter est situé sur une butte (altitude 100 mètres) et n'est pas soumis au ruissellement et aux coulées de boue.
- Le terrain d'implantation du Datacenter dispose d'un réseau d'évacuation sophistiqué des eaux pluviales et de drains (VRD à votre disposition).
- La végétalisation du terrain participe à minorer les risques d'inondations.
- Le Netcenter est construit sur pilotis.

b. Risques sismiques

Situation de la commune au regard du zonage réglementaire pour la prise en compte de la sismicité (en application du décret 91-461 du 14 mai 1991 modifié relatif à la prévention du risque sismique).

- La commune est située en zone 0 (sismicité négligeable)
- Le Datacenter est de conception antisismique (piliers sur amortisseurs)
- Le bâtiment est doté de détecteurs sismiques sur alarme.

c. Risques de foudre

Les précipitations sont de 570 mm par an en moyenne. La Ciotat détient le record de durée d'ensoleillement par an en France avec 2800 heures. Le risque de foudre est négligeable.
Le bâtiment est protégé par un bardage métallique double peau.

d. Risques incendie

Conformité code des assurances (APSAD), Code des Télécommunication et Code du Travail.
Système anti-incendie SIEMENS en salles blanches, extinction par AZOTE sans danger pour les équipements avec double détection (détecteurs VESDA).
Le bâtiment est protégé par un système autonome de lutte contre les incendies. RIA, 2 bornes accès pompiers, extincteurs, brumisateurs extérieurs, cuve autonome de 3 millions de litres et sprinklers sur les bâtiments administratifs.

Cuve autonome réseau anti-incendie

e. Risques industriels

Contrairement aux Datacenters de Marseille (usine ARKEMA) notre Datacenter est situé hors zone SEVESO.

f. Transport de matières dangereuses

Le bâtiment est situé à une centaine de mètres d'un axe routier secondaire, une déflagration située sur l'axe routier n'impacte pas le bâtiment.
Le bâtiment est doté de 70 détecteurs de chocs sur alarme.

g. Risques aériens

Le bâtiment n'est pas situé dans un couloir aérien.
Nous notons cependant la présence sporadique des Canadair de la sécurité civile.

h. Risques économiques

ASPSERVEUR est une entité du groupe Digital Dimension | Econocom.

i. Accès humain

- Parking de 150 places éclairé.
- Portail et barrières automatiques gérés par le PC sécurité.
- Accès au Datacenter par SAS automatique.
- Contrôle d'accès par badges magnétiques et lecteurs biométriques.
- Badges sectorisés.
- Accueil et registre au PC sécurité en 24/7

j. Accès matériel/Coffre-fort

Le bâtiment dispose d'un quai de débarquement interne avec SAS de type BRINGS pour les camions de livraison.
Le quai de débarquement est au même niveau que la salle blanche, sans dénivelé ni marche.
La charge au sol est de 1200 Kg / m2.
Le magasin de stockage est sécurisé et surveillé, il permet d'entreposer du matériel sensible.

Notre Datacenter dispose d'un coffre-fort en béton armé de 25 m² protégé par une porte blindée. Cette dernière dispose d'un contrôle d'accès par badge avec monitoring et registre d'accès. Le coffre bénéficie d'un dispositif de surveillance composé de 4 caméras ainsi que des détecteurs de choc et sismique

k. Contrôle d'accès et anti-intrusion

- Gardiennage 24/7 par agents cynophiles
- Le bâtiment est l'ancien site de GEM+ pour la fabrication des cartes à puces classé alors secret défense.
- Le contrôle d'accès est confié à un ensemble de lecteurs de badges et de lecteurs biométriques connectés à un système de gestion des accès et à plusieurs centrales autonomes.
- Les boitiers du contrôle d'accès fonctionnent en mode autonome sur batterie, une panne du logiciel ou du serveur n'impacte pas le contrôle d'accès.
- Les accès sont sectorisés, nul ne peut accéder à un autre périmètre que celui qui lui est affecté.
- Un registre des entrées/sorties est tenu et conservé à vie.
- L'ensemble du bâtiment est sous radars anti intrusion (360° et rideaux)
- L'ensemble des parkings et abords du bâtiment est équipé de barrières anti intrusion infra rouge et de radars linéaires longue portée (cerclage périphérique complet).
- Le bâtiment est doté d'un réseau de 23 caméras. Les enregistrements sont conservés durant 29 jours sur support numérique.
- Le périmètre du bâtiment est cerclé de grillage surmonté de fil de fer barbelé.
- L'ensemble des moyens de sécurité est centralisé sur un système Excalibur.
- Le bâtiment est gardé en 24/7 par un organisme de sécurité (agents cynophiles).
- Gestion des clés des locaux techniques via deux armoires électroniques avec contrôle d'accès.

l. Télécom

Le Datacenter est connecté à Internet via 6 fibres optiques utilisant des points de pénétration différents dans le bâtiment.
Les fibres sont opérées et monitorées en 24/7 et sous contrat avec une GTR < 4 heures.
La capacité maximum actuelle est de 249 Gbps. Les équipements sont en redondance 2N actif/actif.

ASPSERVEUR est connecté aux Meet-me-room » suivantes :

- INTERXION Marseille
- TDF Aix en Provence
- SFR Courbevoie (Paris)
- INTERXION Zaventem (Bruxelles Belgique)
- NEXICA (Barcelone)

L'ensemble de ces POP opérateurs permet à nos clients l'interconnexion avec n'importe quel opérateur.

Opérateurs connectés actuellement :
SFR - ZAYO TELECOM - INTEROUTE - COGENT NETWORK – PACWAN – FRANCEIX-TDF-RENATER

m. Les baies APC NetShelter

Large baie avec options avancées de gestion des câbles, pour applications serveur et réseau haute densité.

Hauteur max : 1991 mm (42 U)
Largeur max : 750 mm
Profondeur max : 1200 mm
Capacité de poids : 1363.64 kg
Largeur du rack : 19 ‘’
Couleur : noir
Livrée avec les blank panel de confinement
Conformité : RoHS, REACH, PEP, EOLI

n. Respect de l'environnement

L'utilisation conjointe des technologies éco-efficientes à l'état de l'Art nous permet d'afficher un PUE (Power Usage Effectiveness) inférieur à 1.4.

EcoAisle est une solution de confinement thermique intelligente conçue pour améliorer l'efficacité du système de refroidissement tout en protégeant à la fois l'équipement informatique stratégique et le personnel. La fonction de contrôle de débit actif (AFC) du système EcoAisle fournit des informations au système de refroidissement afin d'obtenir le débit d'air de refroidissement adapté à la charge de l'équipement informatique. La consommation du ventilateur est ainsi réduite par rapport aux systèmes de refroidissement traditionnels.

Les onduleurs Symmetra PX s'appuie sur la technologie Double Conversion brevetée par APC. Ils atteignent ainsi un rendement de 95 %, le meilleur de tous les onduleurs on-line double conversion du marché. Ils réduisent les coûts en alimentation et en refroidissement et maintiennent ce rendement jusqu'à une charge de 35 %.

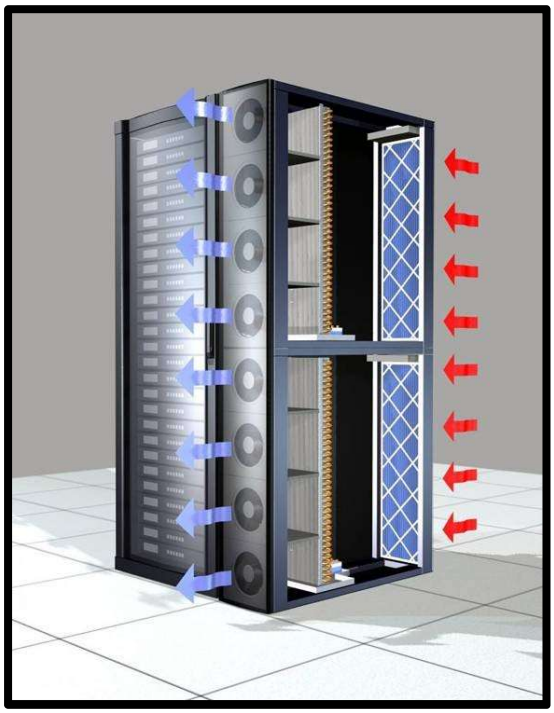
o. Dispositifs de redondance

Redondance énergie :
Deux voies actives (A et B) comprenant chacune leur propre transformateur, TGBT et groupe électrogène.

Redondance Onduleurs :
Deux voies actives chacune en N+1
Autonomie sur batteries : 20 minutes

Groupes électrogènes :
Groupes en préchauffe constante, démarrage automatique en moins de 2 minutes.
Autonomie gasoil 72 heures.

Redondance climatisation :
Groupes de production d'eau glacée en N+2.
Climatiseurs de précision APC InRow.



p. Disponibilité contractuelle

Disponibilité contractuelle conforme au standard TIER IV soit supérieure à 99.995%

Type de tier	Caractéristiques	Taux de disponibilité	Indisponibilité statistique annuelle	Maintenance à chaud possible	Tolérance aux pannes
Tier I	Non redondant	unité 99,671 %	28,8 h	✗ Non	✗ Non
Tier II	Redondance partielle	99,749 %	22 h	✗ Non	✗ Non
Tier III	Maintenabilité	99,982 %	1,6 h	✓ Oui	✗ Non
Tier IV	Tolérance aux pannes	99,995 %	0,4 h	✓ Oui	✓ Oui

IV. Sécurité (extrait du Plan Assurance Sécurité)

1. Organisation de la sécurité

a. Suivi

Nous disposons d'une politique de sécurité des systèmes d'information mise en place pour la première fois en 2009. Cette dernière est mise en ligne au niveau de notre intranet permettant ainsi la consultation en ligne de toutes les personnes concernées. L'utilisation du versionning des documents permet d'avertir via une liste de diffusion prédéfinie l'ensemble des destinataires de la mise en place ou retrait d'anciennes versions par mail.

b. Gestion de la confidentialité

L'ensemble du personnel est sensibilisé et, est conditionné par une clause de confidentialité contenu dans les contrats de travail signés lors de l'embauche.
Ci-dessous un extrait de nos contrats de travail :
Vous êtes tenu sans réserve à une obligation de secret professionnel pour tout ce qui concerne les affaires internes de notre Société.
Tout document, note et d'une façon générale tout support contenant des informations de nature secrète ou confidentielle sur la société qui vous auraient été communiqués ou que vous auriez vous-même établi, ne devront être remis qu'à des personnes dûment autorisées.
Ils devront dans tous les cas être restitués en cas de cessation de votre contrat de travail ou en cas de demande expresse de la société, sans être dupliqués ou copiés de quelque façon que ce soit.
Vous devrez porter à la connaissance de la direction tous les faits dont vous pourriez avoir connaissance et qui seraient susceptibles de mettre la société en difficulté.
De plus, notre règlement intérieur remis et signé par chacun des salariés lors leur embauche stipule également les règles de confidentialité ainsi que le bon usage des outils de communication tel que le mail.
De même qu'il existe un plan de sensibilisation en matière de confidentialité et de respect du secret professionnel mené par notre Directeur administratif et par notre RSSI.

c. Révision

La révision des documents se fait notamment en routine lors de son utilisation ou à l'occasion d'une revue formelle décidée par la Direction d'Aspserveur.
Des réunions techniques hebdomadaires dirigées par notre RSSI, permettent suite à un état des lieux d'identifier des menaces entrainant des mesures de sécurité et de traitement du risque.
Ces réunions hebdomadaires font l'objet d'un compte rendu diffusé par mail à l'ensemble des personnes concernées pouvant amener une révision de notre PSSI.

2. Sécurité physique

a. Gestion des accès physique

1 Contrôle d'accès

La gestion des accès physique par badges est formalisée par une procédure interne indiquant les conditions de création / destruction des badges.
Le contrôle d'accès est confié à un ensemble de lecteurs de badges connectés à un logiciel de gestion des accès (Excalibur) et à plusieurs centrales autonomes.
Les boitiers du contrôle d'accès fonctionnent en mode autonome sur batterie, une panne du logiciel ou du serveur n'impacte pas le contrôle d'accès.

Les badges d'accès sont sectorisés, nul ne peut accéder à un autre périmètre que celui qui lui est affecté.
Un registre des entrées/sorties des visiteurs est tenu et conservé sur 10 ans.

b. Dispositifs d'alertes

2 GTC

Le Datacenter est équipé d'un système de Gestion Technique Centralisée (GTC) qui permet aux équipes de maintenance et personnels techniques de connaître tous les dysfonctionnements de la production en temps réel depuis un point unique.
La GTC permet de recevoir en un seul endroit toutes les informations de fonctionnement (évènements) et alarmes (défauts) provenant des différentes installations techniques (électricité, climatisation, incendie). Une politique de notification en temps réel par SMS et mail est mise en place et contrôlée par le RSSI. Celle-ci concerne en outre la climatisation, les APC, onduleurs, distribution électrique sur plusieurs points de contrôle tel que les températures du fluide, air, état des disjoncteurs, puissance PDU….. Tous répertorié au niveau du logiciel de Gestion ISX.

3 PRTG

Outil de surveillance de la performance réseau avec remontée d'alertes par SMS au niveau du service en charge du réseau. Prenant également en charge la supervision de la bande passante et de la consommation du réseau.

4 IP Label

Notre réseau est audité en permanence par un tiers de confiance IP LABEL générant des rapports sur la disponibilité, les temps de réponses et les anomalies constatées pour une période donnée.
Plusieurs indicateurs opérationnels détaillés sont mis en place afin d'avoir une vue précise sur les dysfonctionnements et leurs causes.
Un système d'alerte codifié en fonction de la gravité de l'incident est mis en place en collaboration avec IP Label pouvant aller du simple mail d'information à une alerte téléphonique.

5 Sécurité incendie

Conformité code des assurances (APSAD), Code des Télécommunication et Code du Travail.
Détection incendie SIEMENS.
Une télésurveillance est opérée en 24/7 par l'organisme Activeille.

3. Gestion des documents

a. Gestion des documents électroniques

Est utilisé au sein de l'entreprise un intranet SharePoint gérant des bibliothèques de documents internes et clients. L'accès à SharePoint est limité via SSL, réseau privé ainsi qu'Active Directory pour la gestion des droits en interne. Les chefs de chaque service en fonction du niveau de confidentialité, compétence, et investissement gèrent plus finement la gestion des droits d'accès au niveau de Sharepoint.
La gestion documentaire dans SharePoint c'est :

- La gestion des versions
- La gestion des processus et du cycle de vie du document
- La gestion des droits d'accès
- La possibilité de travailler les documents en relation avec les projets et les clients
- La possibilité de travailler les documents par balises META

Aucun document client sur support de stockage dit nomade (CD, DVD, clé USB, bandes ou autres) n'est utilisé. N'est autorisé que sur demande expresse du client pour envoi par courrier ou transporteur.

-

b. Gestion des documents papiers

6 Dématérialisation

La totalité des documents papiers reçus tels que les factures fournisseurs, courrier entrant, courrier administratif sont dématérialisés à réception, via numérisation au format PDF afin de garantir l'intégrité des documents reçus. Afin d'assurer une meilleure traçabilité ces derniers sont numérotés et, enregistrés au niveau d'un registre fournisseur / client au niveau de SharePoint. Les documents scannés, classés et stockés au niveau de notre intranet sur une durée illimitée.

7 Stockage

Les documents papiers sont archivés et stockés dans une pièce sous clé réservée à cet effet.
L'accès est limité par badge magnétique et clé aux seuls personnes ayant les droits nécessaires.

8 Edition

L'édition des documents est effectuée au niveau d'un local accessible à tous.
L'ensemble du personnel ayant été sensibilisé sur le fait de n'y laisser aucun document et d'utiliser le broyeur de documents prévu à cet effet à proximité du lieu de reprographie aux moyen d'affiches sensibilisant le personnel.

c. Gestion des supports de stockage

Aucun document client sur support de stockage dit nomade (CD, DVD, clé USB, bandes ou autres) n'est utilisé. N'est autorisé que sur demande expresse du client pour envoi par courrier ou transporteur.
En interne les supports de stockage tels que les disques durs issus de d'une récupération suite à résiliation de services client sont dans un premier temps formatés en bas niveau au moyen d'un logiciel (Acronis). Puis, sont stockés dans des baies munies de serrures magnétiques dans une salle munie d'un contrôle d'accès en vue d'une future destruction par une société tiers en charge du recyclage ou réutilisation.

4. Sécurité de l'exploitation

a. Gestion des postes de travail

Chaque utilisateur est authentifié par une authentification par nom d'utilisateur et mot de passe fort.
La gestion des mots de passe est soumise à une politique de sécurité stricte :

- Taille minimum : 8 caractères.
- Complexité : lettre, chiffre et symbole.
- Fréquence de changement : tous les 180 jours
- Historisation : mots de passe à usage unique

La politique de sécurité des postes de travail et des utilisateurs est géré sur un annuaire de type LDAP ou Active Directory géré par l'administrateur système gérant ainsi la gestion des accès et des habilitations. Le contrôle de la stratégie sécurité des mots de passe est par la même automatisé pour l'ensemble des utilisateurs.

Une stratégie de groupe (GPO) est envisagée pour une application aux utilisateurs afin de limiter le périmètre d'action sur le poste de travail. Chaque poste de travail dispose d'un anti-virus et de l'installation automatiquement des mises à jour système.

b. Sécurité des serveurs

L'identification des serveurs est réalisée par un numéro d'inventaire sans signe distinctif.

Chaque serveur dispose d'une redondance des éléments critique :

- Double alimentation électrique
- Redondance des disques durs (miroir de disque type RAID1) minimum requis pour les serveurs dédiés en utilisation interne.
-

Les serveurs intègrent des applications de sécurité comme un anti-virus et pare-feu opérationnels et mis à jour. L'installation automatique des mises à jour système est recommandée à l'ensemble de nos clients

ayant à leur charge leur propre plan de lutte antivirale comprenant également la gestion des correctifs de sécurité.

En interne depuis la version Windows 2008 R2 nous avons préféré les mises à jour automatiques Microsoft ou autres éditeurs de logiciel. Les serveurs de correctifs en push présentaient des limitations telles que l'impossibilité de pouvoir faire du cas par cas pour nos clients; Désormais ils ont la possibilité de pouvoir procéder en leur propre réglage et mise à jour.

c. Gestion des sauvegardes

L'intégralité des données générées par les clients ou les applications ainsi que les systèmes d'exploitation sont sauvegardées uniquement sur demande. En aucun cas ASPSERVEUR n'aura à mettre en œuvre un processus d'enregistrement, quel qu'il soit, ce rôle étant clairement dévolu à nos clients. La politique de sauvegarde et de restauration est variable selon les choix technologiques des clients de même que la diversité de ces dernières ne permettent pas un système centralisé. Cependant, ci-dessous la description d'un type de sauvegarde réalisé en interne :

9 Typologie des données :

En interne, les plans de sauvegardes sont fonctions de la typologie des données (Système d'exploitation, Bases de données ou données utilisateurs). Les sauvegardes sont constituées d'archives complètes, différentielles et incrémentales. La génération de ces types d'archive est gérée par le logiciel de sauvegarde qui consolide et nettoie les archives en fonction du plan de maintenance.

10 La fréquence de sauvegarde:

Systèmes d'exploitation serveurs : 1 fois par jour
Bases de données : Principe de protection en temps réel CDP (continuous data protection) pour les bases supportant les mécanismes de sauvegarde à chaud ou 1 fois par jour.
Données utilisateurs : Principe de protection en temps réel CDP (continuous data protection).

11 Tests de restauration

La vérification de cohérence est exécutée par les applications de backup à la fin de chaque cycle de sauvegarde. Cette vérification émet une alerte en cas de corruption ou d'échec d'un jeu de sauvegarde. Des environnements de test physiques ou virtuels sont en place afin de permettre d'effectuer les tests de restauration.

12 Principe d'externalisation

L'externalisation des données a pour but la protection de l'intégrité physique des supports de données. Disposant de deux sites distants de 40 km, cette tâche est réalisée grâce à des liaisons réseaux fibre. Les données des systèmes de stockage basées dur des disques (NAS et SAN) sont répliquées en temps réels grâce à des contrôleurs RAID de technologie NETAPP.

13 Architecture de sauvegarde

La sauvegarde peut être effectuée de manière centralisée. Les différentes sources de données sont sauvegardées par des agents de backup qui communiquent avec les serveurs de sauvegarde.
Celle-ci est mise en œuvre par des serveurs pouvant être de technologie ACRONIS, Microsoft Data Protection Manager, etc… suivant la typologie des données
Les serveurs de sauvegarde communiquent avec les périphériques de stockage (SAN, NAS) par un réseau spécialisé disposant d'une bande passante dédiée.
Les baies de stockages sont de type ISCSI ou Fiber channel. Les grappes de disques sont configurées en groupe RAID de différents niveaux assurant la redondance matérielle. Elle dispose également de disque de spare d'une double alimentation. Les contrôleurs RAID sont redondés de la même manière. Les interfaces gigabit assurent une communication à débit élevé entre les nœuds de backups et les espaces de stockage.

14 Gestion du stockage

Les administrateurs du système de sauvegarde disposent d'un monitoring complet des espaces de stockages disponible et utilisés.
La capacité de stockage peut être étendue grâce aux ajouts de groupement RAID, au changement de capacité des disques.

15 Lancement des sauvegardes

Les agents de sauvegarde exécutent les plans de maintenance sur les systèmes. Ces derniers reçoivent l'ordre depuis les serveurs de sauvegarde de :

- L'heure de déclenchement de sauvegarde
- Le type de données à sauvegarder (répertoire, base de données, …)
- Les scripts de presnapshots

16 Archivage des données

L'archivage des données est fonction du type de la donnée sauvegardée. Il existe différents niveaux de sauvegarde pour lesquels des plans de maintenance différents sont mis en œuvres.
Les plans de sauvegardes sont de types « grand père, père, fils ».
Les sauvegardes sont donc exécutées de manière quotidienne, sur 7 jours, puis de manière hebdomadaire, et enfin mensuellement. Les archives mensuelles sont conservées sur plusieurs mois.

d. Gestion des traces

Il est enregistré les traces générées par :

- Les postes de travail.
- Les serveurs
- Les équipements réseaux (routeur, switch, firewall, IPS)

L'ensemble des équipements tracés font référence à une source temporelle commune via le protocole NTP.
Les traces sont envoyées via le protocole Syslog au serveur de journalisation. Ce serveur est sauvegardé et, les traces sont archivés mois par mois sur une durée d'un an. L'exploitation des traces est limitée au personnel technique et l'accès aux journaux uniquement sur demande et validation par le RSSI.

Les traces réseaux sont centralisées sur un serveur de gestion des logs (SSH et TSE) par compression des bases de données en un format fichier Txt permettant une rétention sur un an (passage à 3 ans récemment) par le logiciel Kiwi Sys Log. Le suivi ainsi que l'analyse des traces n'est faite que sur besoin ou demande.
Les logs IPS sont collectés au niveau du logiciel d'administration de cette dernière afin de ne pas surcharger le serveur de gestion des logs par défaut.

e. Sécurité réseau

17 Trafic du réseau interne

Le réseau interne est segmenté en plusieurs réseaux locaux (LAN) virtuels (VLANs). Chaque VLAN dispose d'une configuration spécifique afin d'assurer l'étanchéité réseau :

- Application d'une politique de routage en fonction du type de LAN.
- Application de privilèges d'accès spécifiques (filtrage des flux entrants et sortants autorisés/refusés).
-

f. Gestion des accès à distance

Les accès distants sont contrôlés par un cluster actif/actif de Firewalls. Une politique de filtrage est appliquée pour autoriser uniquement les flux nécessaires. L'utilisation des Firewalls ainsi que la politique de filtrage sont fonctions de nos offres commerciales en cours.
Nos firewalls répondent à la règle par défaut «deny any any» et, intègrent des cartes de détection des intrusions (IPS) qui assurent la sécurité du réseau ainsi que la protection contre les attaques réseaux et applicatives. Ces IPS comportent une base de données de signatures d'attaques pour détecter et bloquer toutes tentatives d'intrusions. Les attaquants sont automatiquement bannis de notre réseau.

L'administration distante des matériels réseaux est uniquement autorisée via un tunnel VPN chiffré. Chaque salarié ayant les qualifications nécessaires dispose d'un accès avec identification unique (nom d'utilisateur et mot de passe fort) lors de la connexion depuis leur poste de travail.

g. Accès à internet en interne

L'accès à internet en interne passe par un serveur proxy qui assure trois fonctions principales :

- Antivirus : les paquets échangés lors des communications sur Internet sont analysés par un système d'antivirus intégré au Proxy pour détecter et bloquer le téléchargement de tout fichier contenant des risques potentiels sur la sécurité.
- Filtrage d'URL : les sites web sont classés selon un grand nombre de catégories prédéfinies. Les accès à toute catégorie de sites à risque potentiel sont rejetés.
- Filtrage sur le contenu : le serveur contient une base de données de signatures d'applications à laquelle nous avons recours pour bloquer l'utilisation de certains types de programmes dans les bureaux d'Aspserveur, comme le P2P ou le MSN.

h. Continuité des services

Les deux sites de production d'Aspserveur sont dotés de groupes électrogènes permettant de faire face à des difficultés d'approvisionnement électrique via le réseau EDF.
Sur le site hébergeant actuellement les serveurs, le système pourra faire face à une coupure avec une autonomie garantie de 72 heures.
Le choix de la politique de disponibilité réseau, est établi sur le principe de multi opérateurs. Assurant ainsi, une connectivité permanente à Internet, et ce, même en cas de défaillance d'une liaison ou du réseau complet d'un opérateur. A cela, nos systèmes de surveillance analysent en permanence la qualité des réseaux de nos fournisseurs et réagissent instantanément à toute défaillance, panne ou ralentissement pour corriger et rediriger le trafic en toute transparence.
Le pool technique d'ASPSERVEUR est composé d'un nombre suffisant de techniciens et d'ingénieurs, possédant des compétences élargies dans des domaines transverses, pouvant se charger d'un problème de reboot ou d'administration de serveur, de réparation hardware ou logicielle, ainsi que la prise ne charge des demandes de support par le système de tickets.
L'intégralité du personnel de la société, y compris la direction, est en mesure de déposer des noms de domaines ou modifier une zone DNS.
De ce fait, même en présence d'un pic de 40% d'absentéisme prévue par le gouvernement au plus fort d'une crise de type pandémie, nos services seront toujours en mesure d'assurer la continuité de service de nos clients même si cela n'est pas formalisé sous la forme d'un plan de secours.
Des tests périodiques sont réalisés sur les différents équipements et sont consignés sur des cahiers de recette. Le délai de retour garanti est fonction de chaque type de contrat et de redondance choisi par le client au niveau contractuel.