GUIDE ADENIUM

PLAN DE CONTINUITE INFORMATIQUE (PCI)

2022

Mettre en œuvre un Plan de Continuité Informatique (PCI)

Adenium SAS
www.adenium.fr
+33 (0)1 40 33 76 88
adenium@adenium.fr

adenium-brg
be resilient group

adenium-brg
be resilient group

Sommaire

Copyright 2022 © ADENIUM

1. Introduction

Le plan de continuité informatique (PCI) est une sous partie du plan de continuité d'activité (PCA), destinée à permettre la reprise du système d'information (SI) lorsque celui-ci est impacté par une situation de crise, sinistre ou défaillance majeure.

Son objectif est de contribuer à redémarrer l'activité du SI le plus rapidement possible et de minimiser la perte de données, les seuils en matière de temps de reprise et de pertes de données étant fixés au moment de l'analyse réalisée dans le cadre de l'élaboration du PCI, en fonction des besoins de l'entreprise et du budget accordé pour la continuité du SI.

Les entreprises d'aujourd'hui étant de plus en plus dépendantes de leur SI, la sécurisation des moyens informatiques est une démarche importante.

Le plan de continuité informatique est l'un des éléments essentiels constituant la politique de sécurité du système d'information, abordé dans les normes ISO 22301, ISO 27001-27002, et détaillé dans la norme ISO 24762.

Ce guide est destiné à vous aider dans votre démarche d'élaboration et la mise en place de votre PCI afin de prévenir l'incapacité d'exploiter régulièrement les systèmes d'information face aux risques de :

- Catastrophes Naturelles (inondations, tempêtes…),
- Incendie,
- Actes de malveillances internes ou externes,
- Erreurs ou accidents,
- Risques technologiques et Industriels.

Ce guide, présente les solutions techniques existantes pour la mise en œuvre d'un PCI. Ces solutions prennent en compte chaque élément de la chaîne qui constitue un système d'information, du poste client aux serveurs.

Copyright 2022 © ADENIUM

2. La démarche de mise en œuvre du PCI

2.1. Le phasage du projet

Après une phase de cadrage avec la direction, l'élaboration du PCI de votre structure se déroule en **6** étapes :

1. Identifier **l'organisation** à mettre en place pour l'élaboration et la mise en œuvre du PCI,
2. Identifier les **scénarios** d'incidents à prendre en compte,
3. Recueillir le **besoin** métier de rétablissement des services fournis par le SI,
4. Identifier les **moyens*** du SI concernés par chaque scénario d'incident et les mesures de prévention déjà en place,
5. Élaborer les **mesures** préventives, les mesures palliatives et les mesures de secours,
6. Préparer les moyens nécessaires et **tester** les solutions.

2.2. Une démarche au service des utilisateurs

En complément de la démarche PRA (Plan de Reprise d'Activités) habituelle, centrée sur les solutions techniques, la démarche PCI repose avant tout sur l'analyse des besoins utilisateurs en matière de disponibilité du SI. La méthodologie d'analyse et de réduction des risques peut s'appuyer sur une méthode telle que MEHARI. Cette analyse doit permettre :

- D'identifier les activités critiques pour l'entreprise
- D'analyser les impacts qui résulteraient d'un arrêt de ces activités
- D'estimer les besoins en matière de ressources humaines, de bureaux, de postes de travail, et de reprise du SI pour fonctionner en mode dégradé

Cette approche permet d'identifier les mesures nécessaires pour réduire les risques, et dans certains cas, les annuler.

Copyright 2022 © ADENIUM

2.3. Une architecture du SI qui s'adapte aux besoins de l'organisation

Pour chaque élément du SI, deux indicateurs de temps sont définis, permettant ensuite de choisir la solution technique la plus adaptée aux besoins de l'entreprise.

- **Le RTO, Recovery Time Objective**, représente le temps d'arrêt de service que l'on peut tolérer.

- **Le RPO, Recovery Point Objective**, correspond à la quantité de données que l'on juge acceptable de perdre lors de la reprise.

D'une manière générale, plus une solution permet de redémarrer rapidement une activité du SI, tout en minimisant la perte de données, plus elle est coûteuse.

L'analyse des besoins utilisateurs permet de qualifier le niveau de disponibilité requis pour les différentes applications, et d'élaborer les solutions de continuité dont le coût est en adéquation avec les résultats attendus.

Haute Disponibilité	Moyenne Disponibilité	Faible Disponibilité
Reprise immédiate ou quasi-immédiate (quelques minutes). Perte de données très limitée	Secours en quelques heures (moins de 12 heures). Perte de données limitée (quelques minutes à quelques heures).	Secours en 48 heures ou plus. Perte de données en général inférieure à 24 heures.

Dans une démarche PRA centrée sur les solutions techniques, le risque est de mettre en place une architecture inutilement trop coûteuse, ou au contraire, une solution insuffisante pour répondre aux besoins en matière de disponibilité nécessaire à la survie de l'entreprise face à d'une crise majeure.

Copyright 2022 © ADENIUM

3. Elaboration du PCI

L'élaboration du PCI nécessite les actions suivantes :

Prise en compte de l'existant
- PCA pour **identifier** les besoins métier et cerner la situation de crise
- En cas d'absence de PCA les informations doivent être **collectées** auprès du métier avec arbitrage de la direction.

Ebauche du PCI
- Identifier **l'organisation** à mettre en place
- Identifier les **scénarios** à prendre en compte
- Identifier les **moyens** concernés

Tester le PCI
- Procédure
- Processus
- Moyens

- Nommer un Responsable PCI & Identifier les différents acteurs pour faire le diagnostic en cas d'incident.

4. Définition – Continuité SI

Définitions liées à la continuité de fonctionnement SI :

L'incident, qui provoque l'interruption du SI, par rapport auquel on identifie :

Les pertes de données créées avant l'incident et après la **dernière sauvegarde des données**.

La durée maximale avant un incident pendant laquelle les acteurs métiers acceptent de perdre des données est spécifiée, pour chaque type de données, par la **Perte de Données Maximale Admise** (**PDMA**, notion également liée à celle « d'**intégrité** des données » utilisée dans le cadre de la Politique de Sécurité du SI.

La **Durée Maximale d'Interruption Admise** (**DMIA)** après survenance de l'incident. La DMIA est fixée pour chaque service fourni par le SI. Cette notion est également liée à celle de « **disponibilité** des services » décrite dans le cadre de la Politique de Sécurité du SI. Elle est définie en fonction des contraintes métiers des utilisateurs de ce service et de la possibilité de s'appuyer ou non sur des solutions alternatives temporaires en l'absence du service.

Après le **délai de réaction** nécessaire à la détection de l'incident et à la mobilisation des acteurs, puis après le **délai de décision** nécessaire à la sélection des actions à mener dans le cadre de la gestion de crise, la cellule de gestion de crise déclenche la **mise en application du volet** « **Reprise du fonctionnement du SI »** du PCI : la **reprise progressive du SI** se fait en mettant en œuvre une **reprise des systèmes** suivie d'une **restauration des données**, ou encore des **mesures de fonctionnement palliatives** ou de secours. Cette reprise donne la priorité aux systèmes les plus critiques.

Copyright 2022 © ADENIUM

Pendant cette période, le **SI** peut fonctionner **en mode dégradé**, mode dans lequel il ne fournit que partiellement les services attendus. Des **procédures métier dégradées** adaptées à cette réduction du niveau de service fourni par le SI peuvent alors être nécessaires.

Le SI doit redevenir complètement opérationnel dans le délai fixé par **l'Objectif de reprise de fonctionnement du SI**. Les activités métier peuvent de nouveau s'appuyer sur les procédures fonctionnelles normales.

Les **opérations de récupération / reprise des données** doivent être menées. Elles portent sur les données éventuellement produites dans le cadre des procédures dégradées et de l'utilisation de moyens palliatifs d'une part et d'autre part sur la reconstitution ou la ressaisie des données perdues suite à l'incident.

Ces activités visant à réintégrer ces données dans le SI opérationnel sont menées aussi bien au niveau technique du SI qu'au niveau fonctionnel métier.
La **fin de crise** peut être décrétée quand il est validé que l'ensemble des systèmes et des données sont restaurés dans un état normal.

5. Définition PCA – PCI

Les différents termes utilisés dans le domaine de la continuité de fonctionnement informatique sont :

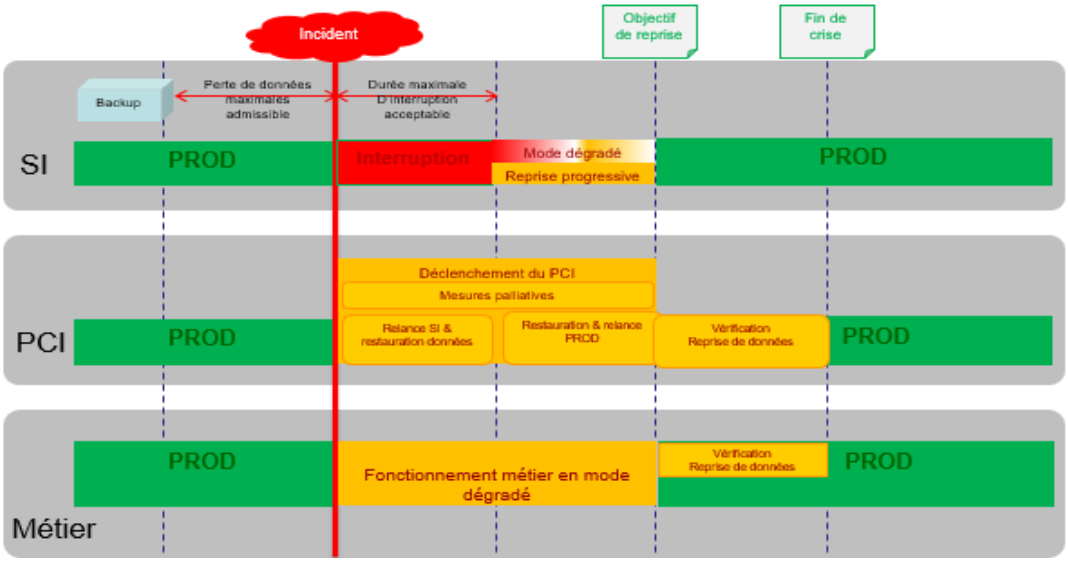
Incident : « Situation qui peut être, ou conduire à, une perturbation, une perte, une urgence ou une crise » (source ISO 22300)
Plan de Reprise d'Activité (PRA) : Ensemble des mesures prévues pour rétablir l'activité de la structure après qu'elle ait été interrompue suite à un incident. Le PRA fait partie du PCA.

Plan de Reprise Informatique (PRI), également « Plan de Reprise d'Activité du SI (PRA du SI) » : Ensemble des mesures prévues pour rétablir l'activité du SI après qu'elle ait été interrompue suite à un incident. Volet du PRA consacré au SI.

Le **PRI** constitue une partie du PCI. La suite de ce guide traite du PCI dans sa globalité sans dissocier les mesures particulières de reprises (PRI).

Copyright 2022 © ADENIUM

Exemple de schéma d'incident impactant la continuité de fonctionnement du SI :



6. Explication du schéma

Site de secours

Salle blanche (site froid) : salle vide prête à recevoir le matériel informatique.
Salle orange (site tiède) : serveurs dédiés aux applications présents & prêts à fonctionner
Salle rouge (site chaud) : tous les équipements présents, les données peuvent être disponible plus ou moins rapidement.
Salle miroir : identique à salle rouge avec disponibilité des données immédiate

Le choix technologique, entre ces différents moyens, doit être fait, en fonction de la durée d'indisponibilité tolérée par le SI. Bien entendu, cela peut varier d'une application à une autre et des choix différents peuvent cohabiter au sein d'un même PCI.

Sauvegarde Backup

Plan de Sauvegarde : indispensable pour avoir une vision d'ensemble des éléments à sauvegarder et formaliser les modalités de récupération.
Sauvegardes physiques : volume par volume. Cas de matériel identique (serveur, baie de stockage)
Sauvegardes logiques : complètes, différentielles, incrémentales
Sauvegardes applicatives : concerne les éléments, informations nécessaires au bon fonctionnement des applications.

Certains modes de sauvegardes sont plus ou moins adaptés au PCI. Par exemple la sauvegarde physique n'est pas toujours possible si le matériel sur le site secours n'est pas identique à celui de production. On remarque également que la restauration d'une sauvegarde incrémentale peut nécessiter un grand nombre de supports (la dernière sauvegarde complète et toutes les incrémentales qui ont suivi) ce qui n'est pas idéal dans le cadre d'un PCI. Inversement, les sauvegardes complètes ou applicatives, sont plus longues à effectuer, mais parfaitement adaptées à la mise en œuvre d'un PCI

Copyright 2022 © ADENIUM

LAN – WAN Internet

LAN de secours : pour permettre la communication serveurs et clients serveurs.
liens **WAN** de secours : pour permettre la communication entre serveurs, applis distantes ou interconnexion avec site distant. Dans le cas d'accès à site distant prévoir ouverture auprès des firewalls distants.
Internet : besoins bureautique, mails, web, télétravail, accès VPN, mise à jour DNS

Postes clients

Relogement des utilisateurs
Location de bureau
Télétravail

Dans tous les cas de figure, il est important de sensibiliser les utilisateurs, avant même la mise en place du plan, pour éviter qu'ils ne travaillent en local, mais sur des serveurs de fichiers sauvegardés.

Téléphonie

Reroutage des lignes avec les numéros sur le site de secours
Reroutage vers un numéro unique
Mise en place d'un **message** personnalisé
Utilisation des **mobiles**

L'utilisation du GSM n'est pas une solution fiable dans tous les cas. En effet lors d'un sinistre de grande envergure, il est possible que le réseau soit saturé, ou que les antennes soient détruites.

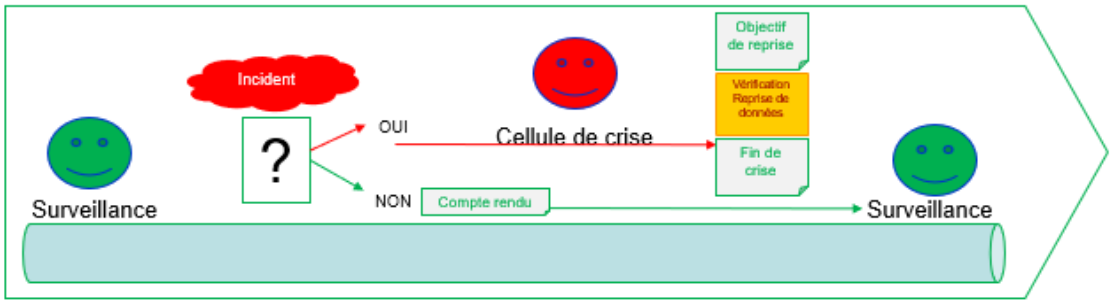
7. Vie du PCI - Incidents

Pour que les incidents puissent être traités efficacement, la structure doit organiser la **surveillance** des évènements qui interviennent au sein du SI, leur **analyse** et leur **qualification** éventuelle en **incident**.

Les différentes étapes de traitement d'un incident qui impacte la continuité du SI doivent être **pilotées** par une structure dédiée avec, quand nécessaire, une mobilisation de la **cellule de crise** qui est l'organe central et indispensable de la gestion de la crise.
L'organisation de continuité de fonctionnement du SI s'appuie en premier lieu sur les circuits existants au sein de la structure en termes de continuité d'activité globale et de gestion de crise. Ces circuits rassemblent la direction et les responsables métiers,

Copyright 2022 © ADENIUM

administratifs et techniques du bon niveau pour prendre les **décisions** en situation de crise.



8. Vie du PCI – Test et évolution

L'efficacité opérationnelle d'un **PCI** doit être validée par des tests **réguliers**, au cours d'exercices à plus ou moins grande échelle, du test unitaire au niveau d'un serveur, aux tests en conditions réelles.

Il est conseillé de réaliser des tests unitaires chaque **trimestre**, et après chaque **évolution** du SI.

Un test **global** devrait être réalisé une à deux fois par **an**.
Pour minimiser les risques d'un test global, il est possible de réaliser un test « **à blanc** », c'est-à-dire sans arrêter la production.

- Un tel test ne permet pas de tester tous les éléments du PCI, comme un reroutage sur Internet. Par contre, cela valide la capacité de reproduire l'environnement de production sur le site de secours.

Le **bilan** établi suite aux tests du PCI permet de **valider** son efficacité.

Il permet également de prendre en compte les **changements** au sein du SI pour faire **évoluer** le PCI.

Copyright 2022 © ADENIUM

9. Le Cloud computing

Le cloud computing, (l'informatique en nuage) consiste à exploiter la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet. Les serveurs sont loués à la demande, le plus souvent par tranche d'utilisation, selon des critères techniques (puissance, bande passante, etc.), mais, également, au forfait. Le cloud computing se caractérise par sa grande souplesse : selon le niveau de compétence de l'utilisateur client, il est possible de gérer soi-même son serveur ou de se contenter d'utiliser des applicatifs distants en mode SaaS.

Les principaux services proposés en cloud computing sont le SaaS (Software as a Service), le PaaS (Platform as a Service) et le IaaS (Infrastructure as a Service). En fonction du service, les systèmes d'exploitation, les logiciels d'infrastructure et les logiciels applicatifs seront de la responsabilité soit du fournisseur soit du client.

Dans le cadre de la sécurité du SI la mise en œuvre de cloud computing nous oblige à nous poser certaines questions afin d'assurer un service efficace et efficient.

Le Cloud est un secteur très dynamique. Quelles que soient leur taille et leur activité, de plus en plus d'entreprises migrent une partie de leur Système d'information (SI) dans le Cloud. C'est surtout le cas pour les services d'application à la demande (SaaS).

Si ces solutions présentent d'indéniables atouts, il convient d'avoir une vision globale et détachée. Il est nécessaire d'appréhender l'ensemble des problématiques liées aux services et hébergements accessibles à distance. Il est devenu indispensable d'intégrer le Cloud dans la gestion des risques numériques.

Copyright 2022 © ADENIUM

Certes, les données hébergées dans un data center bénéficient d'un niveau de protection plus fort qu'en local. Contrôles stricts des accès utilisateurs et administrateurs, redondance des sauvegardes, vidéosurveillance (en plus des badges) des accès physiques… Mais comme tout système et infrastructure, le risque zéro n'existe pas. Vulnérabilités logicielles, défaillance technique, tentatives d'attaques externes ou internes, pertes de données intentionnelles ou non…, les risques sont variés.

Ce constat a été rappelé par le CESIN (Club des experts de la sécurité informatique et du numérique) à l'occasion d'une récente étude.

Accord de la direction & information sur ce qu'est le Cloud Mes fournisseurs CLOUD ont-ils signés un contrat avec mon entreprise ? Validation par un juriste ?	Identifier les risques associés au CLOUD : - Sécurité - Juridique (CNIL) - Valeur des données externalisées - …….	Type de cloud : Privé Publique Hybride

10. Cloud – modalités PCI

<u>Les questions à se poser :</u>

1. Type de Cloud utilisé : Public, Privé, Communautaire, Hybride
2. Quel est le niveau de criticité des applications en Cloud
3. Quels sont les SLA associées à ces applications
4. Est-ce conforme avec la réglementation (concernant mon entreprise)
5. Les modes d'utilisation en fonction des charges de travail
6. Comment sont-elles intégrées au reste du SI

<u>La politique de sécurité</u> :

Elle doit tenir compte des deux aspects hors Cloud et en Cloud.
Les modalités de stockage des données et de leur protection doivent être inscrites dans votre politique SI.

- L'adoption du cloud computing peut être une occasion d'améliorer vos politiques de sécurité et votre position globale de sécurité.

Copyright 2022 © ADENIUM

Les fournisseurs de services Cloud :

S'informer sur les technologies utilisées, Vérifier la transportabilité des données ou de nouvelles fonctions, processus.	Modalités de protections des données et des sites, Respect des normes SAS La formation / certification Pays d'hébergement.	Les accès aux machines Data center : accès maintenance L'architecture du cloud (les nœuds réseau & de stockage)

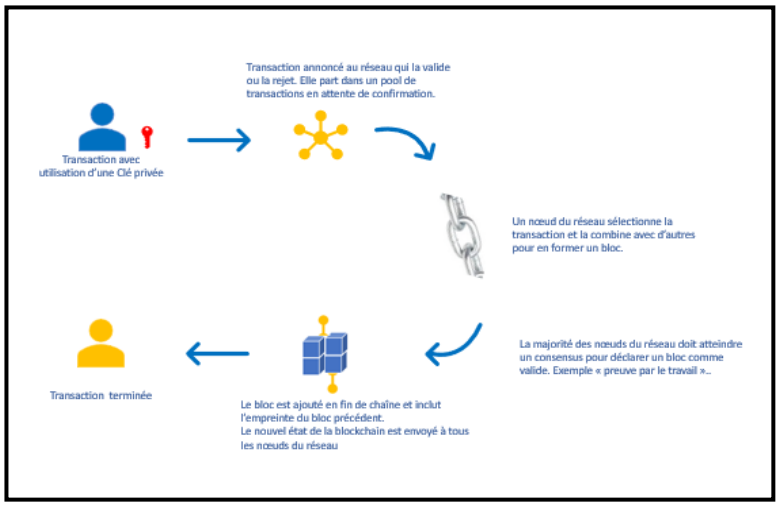
11. Blockchain et PCI

Une blockchain, ou *chaîne de blocs*, est une manière de stocker des informations de façon distribuée, sans organe de contrôle centralisé. Toutes les personnes ayant accès à cette blockchain peuvent y rajouter des informations qui, si elles sont validées par une majorité des nœuds du réseau, seront rajoutées et intégrées à la chaîne. Chaque action effectuée depuis la création de la blockchain y est répertoriée.

Il s'agit donc d'une base de données, décentralisée, et impossible à altérer (du moins très difficile au sens cryptographique). L'utilisation la plus connue et répandue aujourd'hui est en tant que technologie sous-jacente aux différentes cryptomonnaies telles que le Bitcoin, l'Ether, ou encore le Monero.

Copyright 2022 © ADENIUM

Schéma d'une transaction :



Il existe plusieurs centaines de cryptomonnaies, et donc autant de blockchains publiques servant de support pour enregistrer les transactions entre deux acteurs souhaitant s'échanger la monnaie associée. Les chaines de blocs des cryptomonnaies agissent comme des livres de comptes (ou registre) d'une banque, à la différence près qu'il n'y a pas d'organisme centralisé chargé de valider chaque ligne de transaction inscrite dans ces livres.

La blockchain permet donc de stocker des transactions passées de manière inaltérable. Mais la technologie permet des applications bien plus larges que le domaine monétaire.

On peut définir deux grandes méthodes de classification des blockchains le caractère et son usage.

A l'étude la blockchain au service des serveurs DNS, Dans ce type de blockchain, les transactions ne représentent pas un transfert d'argent mais un enregistrement ou une modification de domaine.

Le marché évoluant très rapidement, il sera intéressant de voir l'évolution de la technologie blockchain dans les prochains mois, en particulier les futurs usages en sécurité de l'information.

12. Infos utiles

Les différents guides :

- Guide d'hygiène informatique de l'ANSSI
- Guide ANSSI – CPME des bonnes pratiques de l'informatique
- Guide ENISA sur le Cloud pour les PME (Cloud Security Guide for SMEs)
- ENISA
- Guide du SGDSN sur les plans de continuité d'activité
- Norme ISO 22301 sur la continuité d'activité
- Norme ISO 27000 sur le management du risque

Copyright 2022 © ADENIUM

13. Présentation Adenium

13.1. Qui sommes-nous ?

Adenium est le spécialiste français indépendant des Plans de Continuité d'Activité (PCA) selon ISO 22301.

Depuis sa création en 2002, Adenium intervient régulièrement auprès des organisations (opérateurs vitaux, grands comptes publics ou privés, PME/ETI) pour déployer leur démarche en Plan de Continuité d'Activité (PCA), secours informatiques (PCI, PCIT, PRA/DRP), et continuité de la Supply Chain (Supply Chain Continuity Management - SCCM).

Partisan dès l'origine de la gestion globale des risques et fort d'un historique de spécialiste en gestion de crise, nous avons été pionniers des PCA et de la discipline Business Continuity en France. A ce titre, Adenium a mis en œuvre le premier Système de Management de la Continuité d'Activités (SMCA) certifié ISO 22301* en France. Par la suite, Adenium a accompagné avec succès de nombreuses organisations jusqu'à la certification, ce qui a contribué à la reconnaissance des organisations professionnelles (AFNOR, HCFDC, CLUSIF, EuroCloud, INHESJ, AMRAE, CDSE, …) comme étant l'acteur de référence dans le domaine des PCA.

Par ailleurs, Adenium a cofondé le Club 22301 afin de fédérer les utilisateurs de PCA et de favoriser l'adoption de tels dispositifs par les organisations en France. Engagé activement à l'AFNOR, Adenium anime le groupe de travail « Continuité d'Activité et Résilience Organisationnelle » au sein de la commission de normalisation.

Soucieux de partager ses connaissances avec le plus grand nombre, Adenium est également le cofondateur du Master 2 RPCA et Gestion de Crise de l'Université Paris 13 sous le haut patronage du SGDSN.

Aujourd'hui nos équipes de consultants dédiées à 100% à la continuité d'activité, tous certifiés Lead Implementer ISO 22301, vous accompagnent dans la mise en oeuvre de votre Système de Management de la Continuité d'Activité (SMCA).

Les atouts d'Adenium sont ses compétences, son professionnalisme et le sens de l'engagement de ses équipes.

Adenium est une Société par Actions Simplifiée (SAS) au Capital de 150 000 Euros dont le siège social est basé à Paris. Adenium est également implanté à Lyon.

Copyright 2022 © ADENIUM

13.2. Notre valeur ajoutée

Respectueux des cadres normatifs, notre longue expérience en gestion des risques permet de garantir une approche opérationnelle et d'obtenir des résultats.

De taille humaine, la structure d'Adenium regroupe des spécialistes qui vous apporteront des services et conseils personnalisés en adéquation avec votre culture d'entreprise et votre appétence au risque.

Notre flexibilité et notre sens de l'écoute assurent un service de proximité et une véritable relation de confiance entre notre cabinet et nos clients.

13.3. Contacts utiles

Notre équipe se tient à votre disposition pour vous renseigner :

ADENIUM

Paris :
Siège social : 10, rue Emile Landrin - 75020 Paris
Téléphone : 01 40 33 76 88
Télécopie : 01 40 33 76 67
Email : adenium@adenium.fr
Web : www.adenium.fr

Lyon :
Adresse : 33, rue Saint-Maximin – 69003 Lyon
Téléphone : +33 (0)9 82 58 85 22

Copyright 2022 © ADENIUM