Pū Ti´aauraae Faaineineraa Tōro´a

République française
Polynésie française

EXAMEN PROFESSIONNEL
DE LA FONCTION PUBLIQUE COMMUNALE
AU TITRE DE L'ANNÉE 2025

RÉSOLUTION D'UN CAS CONCRET

CORRIGÉ

SPÉCIALITÉ : TECHNIQUE
CADRE D'EMPLOIS : MAÎTRISE (CATEGORIE B)
GRADE : TECHNICIEN PRINCIPAL

Durée : 3 h 00 Coefficient : 1

⚠ A lire attentivement avant de traiter le sujet ⚠

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom, ni votre prénom, ni signature, paraphe ou nom de collectivité, même fictifs, et aucune initiale, numéro, ou autre indication étrangère au traitement du sujet.
- Seul l'usage d'un stylo à bille ou à encre de couleur noir est autorisé. L'utilisation d'une autre couleur, d'un surligneur, d'un crayon à papier ou porte-mine peut être considérée comme un signe distinctif.
- Ne pas utiliser de stylo bille effaçable par friction (dit « friXion »), ni les encres claires
- Les feuilles de brouillons ne seront pas prises en compte.
- Les copies supplémentaires seront insérées à l'intérieur de la première copie. Aucun trombone ou agrafe ne doit être fixé aux copies.
- Tous les candidats doivent remettre une copie, même blanche. Dans cette hypothèse, ils signent leur copie en indiquant « copie blanche ».

Ce document comprend un sujet de 4 pages et un dossier de 20 pages.
S'il est incomplet, en avertir un surveillant.

EXAMENS PROFESSIONNELS POUR L'ACCÈS AU GRADE DE TECHNICIEN PRINCIPAL
(catégorie B)

Spécialité « ***Technique*** »

Domaine ***« Systèmes d'informations »***

SESSION 2025

Résolution d'un cas concret,

A partir d'un dossier à caractère administratif, assorti de plusieurs questions destinées à mettre le candidat en situation professionnelle.

Durée : 3 h 00
Coefficient : 1

SUJET :

Vous êtes technicien des systèmes d'information dans une commune de taille moyenne. Un matin, vous arrivez au travail et découvrez que le système informatique central de la commune a été victime d'une attaque par ransomware. Les données sensibles sont chiffrées, et les services essentiels sont perturbés.

Après avoir appliqué les mesures d'urgence, votre DGS vous demande, en vous aidant des éléments de contexte, du corpus joint et de votre expérience professionnelle, de rédiger à son attention une note devant lui permettre d'être éclairé sur les aspects suivants :

1. **Analyse de la situation** :
    - Quels sont les principaux impacts de l'attaque sur les services de la commune ?
    - Quelles ont été les premières mesures prises pour limiter les dégâts ?
2. **Gestion de crise** :
    - Comment mettre en œuvre le plan de continuité des activités pour assurer la poursuite des services essentiels ?
    - Quels sont les rôles et responsabilités des différents acteurs impliqués (techniciens, direction, prestataires externes) ?
3. **Sécurité et confidentialité** :
    - Quelles mesures de sécurité doivent être immédiatement renforcées pour éviter de nouvelles attaques ?

- Comment gérer la communication avec les parties prenantes (personnel, public, médias) concernant la sécurité des données ?

4. **Plan d'action** :
    - Proposez un plan d'action détaillé pour la résolution à court terme de la crise.
    - Comment évaluer l'efficacité des mesures prises et ajuster le plan en conséquence ?
5. **Collaboration et communication** :
    - Comment coordonner les efforts entre les équipes internes et les prestataires externes ?
    - Quelles sont les clés pour une communication efficace avec la direction et les autres services de la commune ?

Instructions pour le candidat :

- Utilisez les documents fournis pour étayer vos réponses.
- Organisez vos réponses de manière logique et structurée.
- Proposez des solutions pratiques et opérationnelles.

DOCUMENTS JOINTS

Document 1 : Rapport d'incident **(1 page)** ;

Document 2 : Préfecture du Nord, « *Guide à l'usage des maires pour la réalisation d'un plan de continuité des activités* », extraits, décembre 2013 **(2 pages)** ;

Document 3 : Sauvegardes et stockage **(2 pages)** ;

Document 4 : Organigramme de la commune **(2 pages)** ;

Document 5 : Contrats avec les fournisseurs **(2 pages)** ;

Document 6 : Agence nationale de sécurité des systèmes d'information, « *Crise d'origine Cyber, les clés d'une gestion opérationnelle et stratégique* », Fiche n°4, décembre 2021 **(4 pages)** ;

Document 7 : Cartographie du système d'information **(3 pages)** ;

Document 8 : Plan de communication de crise **(4 pages).**

Éléments de correction

Question 1 : Analyse de la situation

Impacts de l'attaque sur les services de la commune :

L'attaque par ransomware a gravement perturbé les services de la commune, avec des conséquences importantes sur le fonctionnement des systèmes critiques. Tout d'abord, le système de gestion des dossiers administratifs est devenu inaccessible, ce qui empêche le traitement des demandes des citoyens, telles que les actes d'état civil ou les autorisations administratives. Ensuite, la base de données des contribuables a été chiffrée, ce qui compromet la gestion fiscale, notamment la collecte des taxes et impôts locaux. Par ailleurs, le système de gestion des ressources humaines (RH) est indisponible, ce qui perturbe la gestion du personnel, incluant le traitement de la paye et des congés. Enfin, les postes de travail connectés au réseau local sont inutilisables, ce qui paralyse les activités quotidiennes des agents municipaux.

Sur le plan organisationnel, cette attaque entraîne une interruption des services essentiels pour les citoyens, ce qui risque d'affecter leur vie quotidienne. De plus, il existe un risque d'atteinte à la confidentialité des données sensibles, telles que celles des contribuables et des employés. Cette situation pourrait également entraîner une perte de confiance durable des usagers envers la commune.

Premières mesures à prendre :

Face à cette crise, plusieurs mesures doivent être prises immédiatement pour limiter l'impact de l'attaque. Tout d'abord, il est impératif d'isoler les systèmes infectés en déconnectant les postes et serveurs compromis afin d'empêcher la propagation du ransomware dans le réseau communal. Ensuite, il convient d'activer une cellule de crise composée du Maire, du Directeur Général des Services (DGS) et du Responsable informatique pour coordonner efficacement les actions à mener. Par ailleurs, il est nécessaire de contacter les prestataires externes responsables de la sécurité informatique et du stockage afin qu'ils interviennent rapidement pour diagnostiquer et résoudre le problème. Enfin, une communication interne doit être mise en place pour informer tous les agents municipaux des consignes à suivre, notamment l'interdiction d'allumer ou d'utiliser les postes infectés.

Question 2 : Gestion de crise

Mise en œuvre du Plan de Continuité des Activités (PCA) :

Dans une situation de crise telle qu'une attaque par ransomware, il est essentiel d'activer le Plan de Continuité des Activités (PCA) afin de garantir un fonctionnement minimal des services prioritaires. La première étape consiste à identifier ces services prioritaires. Par exemple, les services sociaux doivent continuer à fonctionner pour venir en aide aux personnes vulnérables. De même, la police municipale doit assurer la sécurité publique malgré l'incident. Ensuite, il est indispensable d'utiliser les sauvegardes disponibles pour restaurer les données critiques nécessaires au fonctionnement des systèmes essentiels. Si certaines activités ne peuvent pas être automatisées immédiatement, il faudra recourir à des

solutions temporaires comme le traitement manuel ou papier pour répondre aux besoins urgents.

Rôles et responsabilités dans la gestion de crise :

Dans cette situation exceptionnelle, chaque acteur joue un rôle précis. Le Maire doit prendre les décisions stratégiques et assurer une communication transparente avec le public pour maintenir leur confiance. Le Directeur Général des Services (DGS) est chargé de coordonner l'ensemble des services impactés par l'attaque et superviser la mise en œuvre du PCA. Le Responsable informatique doit effectuer un diagnostic technique approfondi pour identifier l'origine du problème et mettre en œuvre les solutions nécessaires à sa résolution. Enfin, les prestataires externes spécialisés en cybersécurité doivent intervenir rapidement pour fournir leur expertise dans la restauration et la sécurisation du système.

Question 3 : Sécurité et confidentialité

Mesures immédiates à renforcer après l'incident :

Après une attaque par ransomware, plusieurs actions doivent être prises rapidement pour renforcer la sécurité et préserver la confidentialité des données. Tout d'abord, il est impératif de modifier tous les mots de passe utilisateurs afin d'empêcher tout accès non autorisé aux systèmes restaurés. Ensuite, il convient de vérifier l'intégrité et la fiabilité des sauvegardes avant toute tentative de restauration afin d'éviter toute réinfection ou corruption supplémentaire. Enfin, il est nécessaire de déployer ou mettre à jour les outils antivirus et anti-malware sur tous les postes encore fonctionnels ainsi que sur ceux qui seront restaurés.

Gestion de la communication avec les parties prenantes :

La communication joue un rôle crucial dans la gestion d'une telle crise. En interne, il est important d'informer régulièrement le personnel communal sur l'état d'avancement du processus de résolution et sur leurs responsabilités spécifiques dans cette situation. Il peut également être utile de diffuser un guide simplifié sur les bonnes pratiques en cybersécurité pour éviter toute erreur humaine future. En externe, un communiqué officiel doit être préparé afin d'expliquer clairement l'incident tout en rassurant le public sur les mesures prises pour rétablir rapidement les services publics essentiels. Le site internet et les réseaux sociaux peuvent être utilisés comme canaux principaux pour fournir ces mises à jour régulières.

Question 4 : Plan d'action

Plan détaillé pour résoudre la crise à court terme :

Pour résoudre cette crise rapidement et efficacement, plusieurs étapes doivent être suivies dans un ordre précis. La première étape consiste à effectuer un diagnostic complet afin d'identifier l'origine du ransomware grâce aux analyses techniques réalisées par le Responsable informatique et son équipe ainsi que par les prestataires externes spécialisés en cybersécurité. Une fois l'origine identifiée et maîtrisée, il sera possible de passer à la restauration des données critiques en utilisant uniquement les sauvegardes validées comme étant non compromises.

Avant toute remise en service des systèmes affectés, il est impératif de sécuriser ces derniers en réinstallant leurs environnements dans un cadre isolé et protégé contre toute nouvelle tentative d'intrusion.

Évaluation post-crise et ajustements nécessaires :

Une fois que tous les systèmes ont été restaurés et remis en service sécurisé, une surveillance active doit être mise en place pendant plusieurs semaines afin de détecter toute anomalie persistante ou nouvelle tentative malveillante. Par ailleurs, un audit complet du système d'information devra être réalisé pour identifier toutes les failles exploitées lors de l'attaque et mettre en œuvre des corrections durables.

Question 5 : Collaboration et communication

Coordination entre équipes internes et externes :

La coordination entre toutes les parties prenantes est essentielle pour gérer efficacement cette crise. Il est recommandé d'organiser régulièrement des réunions avec la cellule de crise afin de suivre l'avancement du plan d'action et ajuster celui-ci si nécessaire. Les prestataires externes identifiés dans les contrats avec la commune doivent également être impliqués activement dans leurs domaines respectifs (cybersécurité ou sauvegarde).

Communication efficace avec la hiérarchie et le collectif de travail :

Pour garantir une gestion fluide entre tous les acteurs concernés par cette crise, il faut fournir régulièrement au Maire et au DGS des rapports détaillés sur l'état actuel ainsi que sur les prochaines étapes prévues dans le plan d'action global. En parallèle, une collaboration interservices doit être encouragée afin que chaque service apporte ses compétences spécifiques pour minimiser l'impact global sur le fonctionnement communal.

Document 1 : Rapport d'incident

Date et heure de l'incident : 4 mars 2025, 08h00

Type d'incident : Attaque par ransomware

Description de l'incident :

Ce matin, à l'ouverture des bureaux, plusieurs employés ont signalé des difficultés pour accéder aux systèmes informatiques de la commune. Les premières investigations ont révélé que le système central de fichiers et plusieurs applications critiques ont été chiffrés par un logiciel malveillant de type ransomware. Les attaquants exigent une rançon en échange de la clé de déchiffrement.

Systèmes et données affectés :

- **Système de gestion des dossiers administratifs** : Tous les documents administratifs récents sont inaccessibles.
- **Base de données des contribuables** : Les informations personnelles et financières des contribuables sont chiffrées.
- **Système de gestion des ressources humaines** : Les données relatives au personnel sont indisponibles.
- **Réseau local** : Plusieurs postes de travail ne peuvent pas se connecter au réseau.

Premières mesures prises :

1. **Isolation du réseau** : Le réseau a été isolé pour empêcher la propagation du malware.
2. **Alerte aux équipes** : Tous les employés ont été informés de ne pas tenter d'accéder aux systèmes affectés.
3. **Notification des autorités** : Les autorités compétentes ont été prévenues.

Prochaines étapes :

1. **Analyse approfondie** : Une analyse détaillée du système pour identifier les points d'entrée et les mesures de sécurité à renforcer.
2. **Mise en œuvre du plan de continuité** : Activation des procédures pour assurer la poursuite des services essentiels.

Responsable de l'Incident : [Nom du responsable], Responsable du Service Informatique.

Contact : [Téléphone] [Courriel]

Document 2 : Préfecture du Nord, « *Guide à l'usage des maires pour la réalisation d'un plan de continuité des activités* »

https://www.nord.gouv.fr/content/download/16351/100429/file/PCA%20-%20Guide%20

QU'EST CE QU'UN PLAN DE CONTINUITE D'ACTIVITE ?

La survenance d'une crise majeure (catastrophe naturelle, accident industriel, pandémie...) est susceptible de perturber très fortement le fonctionnement d'une organisation, qu'elle soit publique ou privée, avec des conséquences allant jusqu'à la cessation définitive d'activité. Or le responsable d'une organisation se doit de concevoir et mettre en œuvre des stratégies de protection permettant de limiter les effets directs d'un tel événement sur les objectifs de l'organisation, et d'assurer la continuité d'activité malgré la perte de ressources.

Dans cette perspective, un plan de continuité d'activité (PCA) a pour objet de décliner la stratégie et l'ensemble des dispositions qui sont prévues pour garantir à une organisation la reprise et la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal.

METHODOLOGIE D'ELABORATION DU PCA

L'élaboration d'un PCA impose au préalable une action spécifique de communication interne visant à sensibiliser l'organisation - ici les services municipaux - à la gestion du risque et à la continuité d'activité. Le maire et la direction doivent par conséquent être fortement impliqués et commencer par désigner un chef de projet.

Idéalement le chef de projet est rattaché au directeur des risques. Il doit connaître le métier et disposer d'une autorité reconnue. Il devra disposer de correspondants dans les différents services dont les responsables auront eux-même été sensibilisés à l'objectif du PCA.

La démarche méthodologique, présentée par étapes, consiste à :

- définir les objectifs de l'organisation
- identifier et formaliser les besoins de continuité
- identifier et gérer les risques prioritaires
- formaliser les moyens et procédures et définir la stratégie de continuité
- assurer la capacité de mise en œuvre du plan

MISSIONS DU MAIRE ET ACTIVITES ESSENTIELLES A LA VIE COLLECTIVE

Pour élaborer son plan de continuité d'activité, le maire doit avant tout se poser la question de ses missions et des activités essentielles qui doivent être maintenues, fut-ce en mode dégradé, pour les mener à bien lors d'une situation de crise impliquant des ressources humaines ou matérielles limitées.

De manière générale, les missions du maire en période de crise sont :

- le soutien de la population de la commune
- le maintien de la vie collective

La définition des activités à maintenir en priorité dans la commune en période de crise découle de ces deux missions prioritaires. A l'inverse, certaines activités plus secondaires (manifestations sportives ou culturelles, événementiel, grands rassemblements...) peuvent être interrompues pendant toute la durée de la crise. Les activités essentielles peuvent être assurées par les services municipaux ou des prestataires extérieurs. **Cela suppose donc d'impliquer étroitement ces prestataires dans l'élaboration du PCA, en leur demandant à eux aussi des garanties en terme de continuité d'activité**. Ces garanties doivent être intégrées aux contrats qui lient la communes à ses partenaires.

Les activités essentielles à la vie collective dans une commune sont principalement :

- la protection et la sécurité des personnes
- l'état civil
- le maintien des bonnes conditions d'hygiène (traitement des ordures ménagères, nettoyage des bâtiments collectifs...)
- l'alimentation en eau potable ainsi que l'assainissement et le traitement des eaux usées
- le maintien et le fonctionnement des chauffages collectifs
- le maintien de la paye pour les agents impliqués dans la continuité de service
- les services funéraires

Document 3 : Sauvegardes et stockage

Les sauvegardes et le stockage des données jouent un rôle crucial dans la résilience du système d'information de la commune. En cas d'incident informatique, ces solutions permettent de restaurer les données critiques et de minimiser l'impact sur les services publics.

1. Infrastructure de sauvegarde

1. **Serveur de sauvegarde local :**
    - Localisation : Service informatique de la mairie.
    - Fréquence des sauvegardes : Quotidiennes (chaque nuit à 2h00).
    - Données sauvegardées : Bases de données administratives, dossiers RH, fichiers partagés.
2. **Sauvegarde hors site :**
    - Localisation : Data center sécurisé situé à Papenoo.
    - Fréquence des sauvegardes : Hebdomadaires (chaque dimanche à 3h00).
    - Données sauvegardées : Réplication complète des serveurs centraux.
3. **Stockage cloud :**
    - Fournisseur : Microsoft.
    - Utilisation : Stockage des documents non sensibles (ex. rapports publics, archives non critiques).
    - Sécurité : Chiffrement des données en transit et au repos.

2. Procédures en cas de restauration

1. **Étape 1 : Évaluation des données nécessaires**
    - Identifier les systèmes critiques à restaurer en priorité (voir annexe "Cartographie du SI").
    - Vérifier l'intégrité des sauvegardes pour éviter toute restauration de fichiers compromis.
2. **Étape 2 : Restauration depuis le serveur local**
    - Utiliser les sauvegardes locales si les serveurs centraux sont encore fonctionnels.
    - Temps estimé pour la restauration complète : 4 à 6 heures.
3. **Étape 3 : Restauration depuis le site hors site**
    - Activer la réplication depuis le data center externe en cas d'indisponibilité totale des serveurs locaux.

- Temps estimé pour la restauration complète : 12 à 24 heures.

4. **Étape 4 : Validation post-restauration**
    - Tester les systèmes restaurés pour s'assurer qu'ils fonctionnent correctement.
    - Informer les utilisateurs concernés une fois les services rétablis.

3. Points Critiques Identifiés

1. **Risque de perte de données entre deux cycles de sauvegarde** :
    - Les modifications effectuées après la dernière sauvegarde quotidienne ou hebdomadaire pourraient être perdues.
2. **Dépendance aux prestataires externes** :
    - La restauration depuis le site hors site ou le cloud dépend des délais d'intervention du fournisseur.
3. **Sécurisation des sauvegardes** :
    - Les sauvegardes doivent être protégées contre tout accès non autorisé ou corruption par ransomware.

4. Recommandations

1. Mettre en place une solution de sauvegarde continue pour réduire le risque de perte entre deux cycles.
2. Effectuer régulièrement des tests de restauration pour garantir l'intégrité et la disponibilité des données.
3. Renforcer la sécurité des sauvegardes (chiffrement, authentification multi-facteurs pour l'accès).

Document 4 : Organigramme de la commune

L'organigramme de la commune présente la structure hiérarchique et les responsabilités des différents services. Il est essentiel pour comprendre le fonctionnement interne et la coordination des efforts en cas de crise.

Structure hiérarchique :

1. **Maire** : Chef de l'exécutif communal.
    - Responsabilités : Stratégie globale, relations extérieures.
2. **Adjoint au Maire** : Chargé des affaires générales et des ressources humaines.
    - Responsabilités : Gestion du personnel, coordination des services.
3. **Directeur Général des Services** : Supervise l'ensemble des services techniques et administratifs.
    - Responsabilités : Coordination des services, gestion budgétaire.

Services communaux :

1. **Service technique** :
    - Responsable : [Nom]
    - Responsabilités : Entretien des bâtiments, gestion des infrastructures.
2. **Service administratif** :
    - Responsable : [Nom]
    - Responsabilités : Gestion des dossiers administratifs, archives.
3. **Service informatique** :
    - Responsable : [Nom]
    - Responsabilités : Gestion des systèmes informatiques, sécurité numérique.
4. **Service social** :
    - Responsable : [Nom]
    - Responsabilités : Aide aux personnes vulnérables, services sociaux.

5. **Police municipale** :
    - Responsable : [Nom]
    - Responsabilités : Sécurité publique, gestion des urgences.

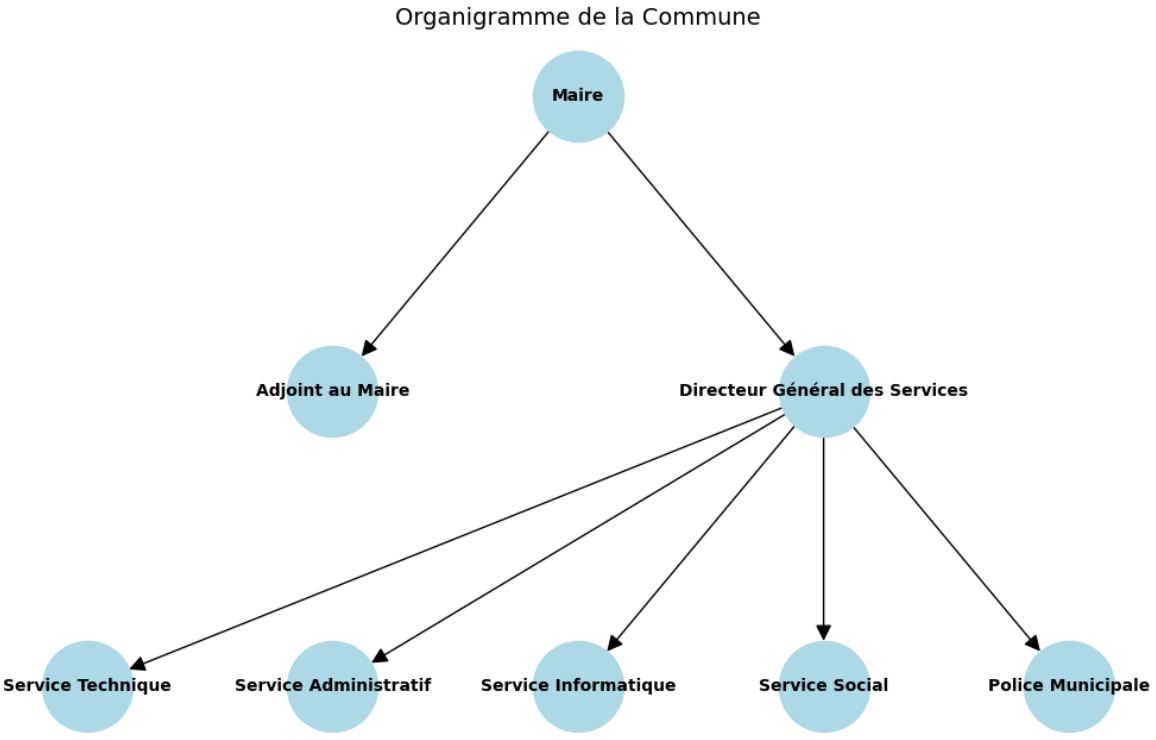
Cellule de crise :

En cas de crise, une cellule de crise est mise en place sous la direction du Maire. Elle comprend :

- Le Directeur Général des Services
- Le Responsable du Service Informatique
- Le Responsable de la Communication

Coordination et communication :

La coordination entre les services est assurée par des réunions régulières et une communication fluide. En cas de crise, des protocoles spécifiques sont activés pour informer le personnel et les usagers.



Document 5 : Contrats fournisseurs

Les contrats avec les fournisseurs de services informatiques et technologiques jouent un rôle clé dans la gestion des systèmes d'information de la commune. En cas de crise, ces contrats définissent les responsabilités, les délais d'intervention, et les services fournis par les prestataires externes.

1. Liste des Fournisseurs et Prestations

Fournisseur	Service fourni	Contrat en cours	Contact	Délai d'intervention garanti
Fournisseur A	Maintenance des serveurs et stockage cloud	Contrat de 3 ans (2023-2026)	[Nom/Email/Téléphone]	4 heures (urgence)
Fournisseur B	Sécurité informatique et antivirus	Contrat annuel (renouvelable)	[Nom/Email/Téléphone]	2 heures
Fournisseur C	Logiciel de gestion des dossiers administratifs	Contrat de 5 ans (2021-2026)	[Nom/Email/Téléphone]	1 jour ouvré
Fournisseur D	Réseau et télécommunications	Contrat de 3 ans (2022-2025)	[Nom/Email/Téléphone]	6 heures

2. Clauses importantes des contrats

1. **Clause de support technique :**
    - Les fournisseurs doivent fournir une assistance technique 24h/24 pour les incidents critiques.
    - Les délais d'intervention sont définis dans le tableau ci-dessus.
2. **Clause de confidentialité :**
    - Les fournisseurs s'engagent à protéger les données sensibles de la commune.

- Toute fuite ou utilisation non autorisée des données est passible de sanctions contractuelles.

3. **Clause de sauvegarde :**

   - Les fournisseurs responsables des systèmes critiques doivent garantir la disponibilité de sauvegardes régulières (quotidiennes ou hebdomadaires).

4. **Clause de pénalités :**

   - En cas de non-respect des délais d'intervention, des pénalités financières sont appliquées.

3. Procédure en Cas d'Incident

1. **Signalement :**

   - L'équipe informatique interne doit contacter immédiatement le fournisseur concerné via le numéro d'urgence indiqué dans le contrat.

2. **Diagnostic :**

   - Le fournisseur doit effectuer un diagnostic initial dans un délai maximum de 2 heures après la notification.

3. **Intervention :**

   - Selon la gravité du problème, le fournisseur doit intervenir sur site ou à distance dans les délais contractuels.

4. **Rapport post-intervention :**

   - Un rapport détaillant l'origine du problème, les actions menées, et les recommandations est fourni par le prestataire après résolution.

4. Contact en Cas d'Urgence

- Fournisseur A (Maintenance serveurs) : [Téléphone] / [Email]
- Fournisseur B (Sécurité informatique) : [Téléphone] / [Email]
- Fournisseur C (Logiciel administratif) : [Téléphone] / [Email]
- Fournisseur D (Réseau et télécoms) : [Téléphone] / [Email]

Document 6 : Agence nationale de sécurité des systèmes d'information, « *Crise d'origine Cyber, les clés d'une gestion opérationnelle et stratégique* », Fiche n°4, décembre 2021

https://cyber.gouv.fr/anticiper-et-gerer-une-crise-cyber

FICHE 4

ADAPTER SON ORGANISATION DE CRISE AU SCÉNARIO CYBER

La particularité du scénario de crise cyber implique de mobiliser à la fois des profils métiers, cyber et IT, ainsi que d'assurer la bonne coordination entre les différents niveaux. Il convient donc de planifier une organisation de crise en amont de tout événement et de s'accorder sur le rôle de chaque partie, afin de faciliter la mobilisation.

Le dispositif de crise à établir se compose d'un volet stratégique, porté au minimum par une cellule de crise dite « stratégique » ou « décisionnelle ». Elle regroupe les représentants des fonctions décisionnelles de l'entité, qui s'approprient les fonctions usuelles d'une cellule de crise : directeur de crise, personnes en charge du management de l'information, appui à la conduite de crise, communicants, etc.

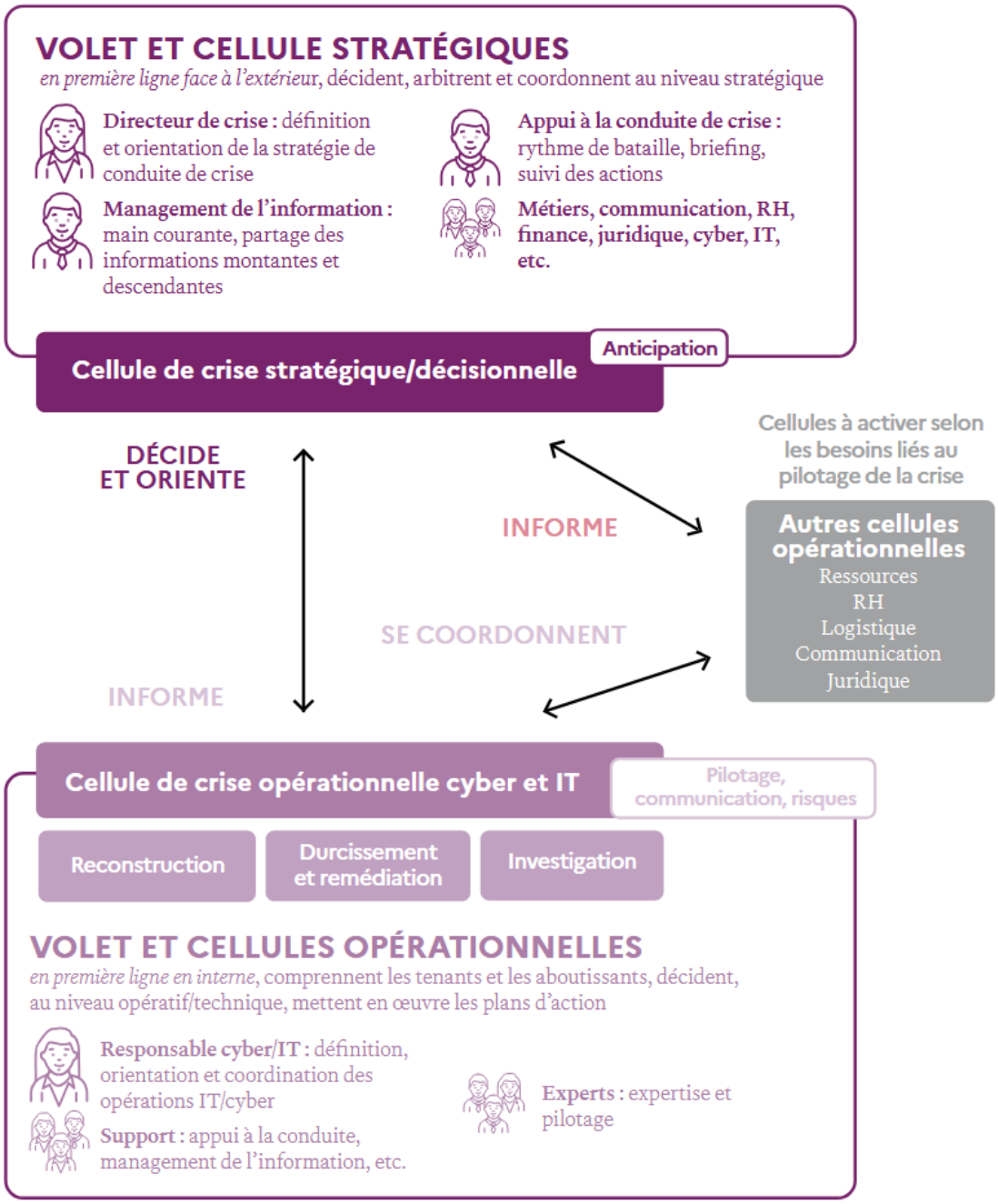
Un volet opérationnel est également mis en place. Au sein de l'organisation, les fonctions cyber et IT sont en charge du pilotage d'une ou de plusieurs cellules et s'assurent d'échanger avec la cellule stratégique.

En fonction des impacts de la crise à gérer, d'autres cellules peuvent également être mises en place : cellules métiers, cellule communication, cellule RH, cellule logistique, cellule juridique, cellule de crise opérationnelle cyber et IT, etc.

« Nous avons mis en place une organisation agile autour du duo formé par notre DGA et le DSI et de "task forces", qui nous a permis d'être réactif en fonction des urgences. Une "cellule ressource" était chargée de rassembler des prestataires et des renforts et d'aider nos équipes à se focaliser sur leur cœur de métier. »

Bouygues Construction

PROPOSITION D'ORGANISATION DE GESTION DE CRISE CYBER[12]



12. À noter que cette organisation est particulièrement adaptée aux grands groupes. Toutefois, elle peut également s'appliquer aux plus petites entités.

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Mettre en place des critères et des procédures d'activation des cellules de crise**	
RECOMMANDATIONS	Les critères d'activation et de désactivation sont établis en fonction des scénarios de référence cyber définis et permettent d'objectiver la mobilisation et la démobilisation d'une cellule stratégique. Ils sont connus des membres du dispositif. Une chaîne d'alerte est formalisée. Plusieurs modes sont prévus dont un mode « alerte » et un mode « crise ». Un référentiel de management des crises cyber intégrant une description de l'ensemble du dispositif de crise (organisation, gouvernance, ressources, outils, annuaire) est formalisé, promu et maintenu à jour. Les fonctions décisionnelles de l'organisation sont sensibilisées aux enjeux cyber. Les fonctions cyber et IT sont systématiquement représentées dans la gouvernance de crise (cyber et hors cyber).	Un processus d'alerte, de gestion et de réponse aux incidents intégrant un volet « sécurité du numérique » est formalisé et testé. Il s'appuie notamment sur des outils de détection et de gestion d'incident[13]. Les critères d'activation et de désactivation du dispositif opérationnel sont définis en fonction des scénarios cyber de référence. Ils prévoient en particulier l'activation par effet de seuil (par le bas) et l'activation sur décision du dispositif stratégique (par le haut). Ils sont connus des membres du dispositif de crise et des équipes de gestion d'incident. Une chaîne d'alerte est formalisée. Plusieurs modes sont prévus dont un mode « alerte » et un mode « crise ».

13. Les outils de détection et de gestion d'incident qualifiés par l'ANSSI attestent d'une conformité à des exigences règlementaires, techniques et de sécurité : www.ssi.gouv.fr/entreprise/qualifications/produits-recommandes-par-lanssi/les-produits/

OBJECTIF 2	Organiser ses cellules de crise cyber	
RECOMMANDATIONS	Une fois les membres de la cellule de crise identifiés, ils sont informés de leur nomination au dispositif, de leur rôle et de leurs missions et y sont formés. Le périmètre d'action de chaque membre (rôles et responsabilités) est défini en amont. Une interface unique (type tableau de bord) est mise en place pour uniformiser la circulation de l'information. Des objectifs et des critères de sortie de crise atteignables sont pré-identifiés. Selon le niveau de maturité de l'organisation, un volet d'anticipation peut être mis en place pour identifier les scénarios de dégradation ou d'amélioration de la situation. Selon le périmètre géographique de l'entité, les problématiques internationales sont prises en compte (différences liées aux fuseaux horaires, aux systèmes pénaux, aux cultures, etc.) et des relais sont identifiés.	Une organisation de crise similaire à la cellule de crise stratégique est définie. Elle intègre des experts clés capables de fournir des orientations ainsi qu'un relais pour la communication de crise. L'organisation de crise en place doit être la plus efficace possible et ne s'appuie pas forcément sur l'organisation usuelle interne. Les équipes techniques cyber et IT sont organisées de manière à réaliser les actions d'investigation/ endiguement, de durcissement/ remédiation et de reconstruction. Un registre est mis en place pour suivre les risques, les dérogations, et les communications internes et externes.

Document 7 : Cartographie du système d'information

La cartographie du système d'information (SI) permet de visualiser les composants technologiques utilisés par la commune, leurs interconnexions, et leur rôle dans les services municipaux. Elle est essentielle pour identifier les points critiques et les priorités en cas de crise informatique.

1. Structure générale du système d'information

Le système d'information de la commune est organisé autour des éléments suivants :

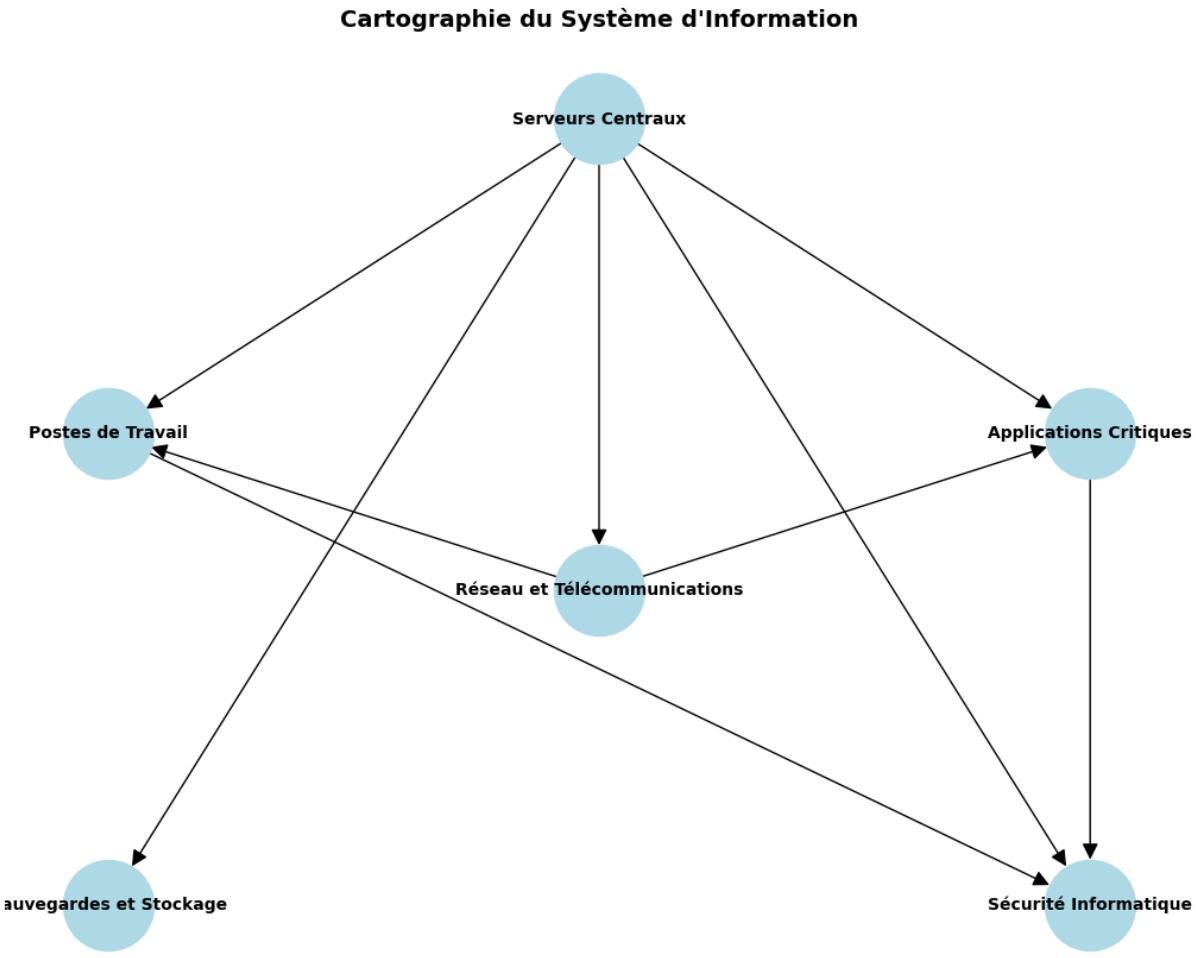
1. **Serveurs centraux** :
    - Hébergent les bases de données administratives, financières, et RH.
    - Localisés dans le centre informatique de la mairie.
2. **Postes de travail** :
    - Environ 150 postes répartis entre les différents services (technique, administratif, social, etc.).
    - Connectés au réseau local via des commutateurs.
3. **Applications critiques** :
    - Logiciel de gestion des dossiers administratifs.
    - Système de gestion des ressources humaines.
    - Outil de gestion des finances publiques.
4. **Réseau et télécommunications** :
    - Réseau local (LAN) pour la communication interne.
    - Connexion Internet sécurisée avec pare-feu et VPN pour les accès externes.
5. **Sauvegardes et stockage** :
    - Sauvegardes automatiques quotidiennes sur un serveur dédié hors site.
    - Stockage cloud pour certains documents non sensibles.
6. **Sécurité informatique** :
    - Antivirus déployés sur tous les postes.

- Solution de détection des intrusions (IDS) active sur le réseau.

2. Cartographie Visuelle

La cartographie visuelle du système d'information inclut les interconnexions entre :

- Les serveurs centraux.
- Les postes de travail des différents services.
- Les applications critiques utilisées par chaque service.
- Les systèmes de sauvegarde et stockage.



3. Points Critiques Identifiés

1. **Serveurs centraux** : Toute panne ou attaque sur ces serveurs affecte directement les services essentiels.
2. **Logiciels critiques** : Les applications administratives et financières sont indispensables à la gestion quotidienne.

3. **Connexion internet** : Une interruption limite l'accès aux outils cloud et aux communications externes.

4. **Sauvegardes** : La perte des sauvegardes compromet la récupération des données en cas d'incident.

4. Recommandations

1. Renforcer la sécurité des serveurs centraux (firewalls, audits réguliers).

2. Mettre en place une solution de sauvegarde redondante pour garantir une récupération rapide.

3. Former le personnel à identifier les cybermenaces courantes (phishing, malwares).

4. Réaliser une mise à jour régulière des logiciels critiques pour éviter les vulnérabilités.

Document 8 : Plan de communication de crise

Le plan de communication de crise vise à garantir une information claire et cohérente auprès des différentes parties prenantes (internes et externes) lors d'un incident critique, tel qu'une attaque informatique. Une communication efficace est essentielle pour maintenir la confiance du public, éviter les malentendus et coordonner les actions.

1. Objectifs du Plan de communication

1. **Informer rapidement** sur l'incident et ses impacts.
2. **Rassurer les parties prenantes** en expliquant les mesures prises pour résoudre la crise.
3. **Maintenir la transparence** tout en protégeant les informations sensibles.
4. **Coordonner les messages** entre les différents acteurs pour éviter toute confusion.

2. Parties prenantes identifiées

1. **Interne :**
    - Personnel communal.
    - Élus locaux (Maire, adjoints, conseillers municipaux).
    - Cellule de crise.
2. **Externe :**
    - Citoyens et usagers des services publics.
    - Médias.
    - Prestataires et partenaires externes.
    - Autorités compétentes (préfecture, CNIL en cas d'atteinte aux données personnelles).

3. Canaux de Communication

Canal	Public cible	Usage en situation de crise
Email interne	Personnel communal	Diffusion des consignes et mises à jour régulières.
Réunions d'urgence	Cellule de crise	Coordination des actions et décisions stratégiques.
Communiqués officiels	Citoyens, médias	Annonces publiques sur l'état des services municipaux.
Site internet de la commune	Citoyens	Publication des informations officielles et FAQ.
Réseaux sociaux (Facebook, Twitter)	Citoyens, médias	Communication rapide sur l'évolution de la situation.
Ligne téléphonique dédiée	Usagers	Réponse aux questions spécifiques des citoyens.

4. Messages clés à communiquer

1. **Au début de la crise :**
    - Nature de l'incident (exemple : "La commune fait face à une attaque informatique").
    - Services impactés (exemple : "Certains services administratifs sont temporairement indisponibles").
    - Engagement à résoudre le problème rapidement.
2. **Pendant la gestion de la crise :**
    - État d'avancement des actions correctives.

- Mesures prises pour protéger les données sensibles.
- Conseils pratiques pour les citoyens (exemple : "Utilisez nos services physiques ou téléphoniques en attendant").

3. **Après résolution :**
   - Rétablissement complet des services.
   - Mesures préventives mises en place pour éviter une récidive.
   - Remerciements aux citoyens pour leur patience.

5. Rôles et Responsabilités

Acteur	Responsabilité dans la communication
Maire	Porte-parole principal auprès des citoyens et médias.
Directeur Général des Services	Supervision globale du message diffusé.
Responsable Communication	Rédaction des messages, gestion des réseaux sociaux et site web.
Responsable Informatique	Fourniture des informations techniques nécessaires aux messages.

6. Étapes clés du plan

1. Activation immédiate du plan dès détection de la crise.
2. Désignation d'un porte-parole officiel (généralement le Maire).
3. Diffusion d'un premier communiqué dans les 2 heures suivant l'incident.
4. Mise à jour régulière des informations via les canaux identifiés.
5. Organisation d'une conférence de presse si nécessaire.

7. Recommandations post-crise

1. Réaliser une analyse post-crise pour évaluer l'efficacité de la communication.

2. Mettre à jour le plan en fonction des enseignements tirés.

3. Former régulièrement le personnel à la gestion de communication en situation critique.