PROJET SECURITE CIVILE

Propriétés	Description
Intitulé	Proposition, choix et mise en place d'une solution technique assurant le fonctionnement permanent et optimum des Centres Opérationnels Départementaux et la mise en œuvre d'une connexion distante permettant l'accès aux ressources et outils métiers par les agents de terrain.
Présentation Rapide	Le projet consiste à mettre en œuvre les missions suivantes : **Missions :** Optimiser la résilience informatique des Centres Opérationnels Départementaux en proposant une solution technique autonome et redondé ; notamment en redondant l'accès Internet. - Mettre en œuvre d'une Messagerie Électronique - Superviser les serveurs et équipements critique - Réaliser une connexion OpenVPN Road Warrior et diffuser des applications à distance - Mettre en œuvre le logiciel open source eBrigade
Durée estimée	8 semaines
Savoir-faire SI mobilisés en priorité	Les savoir-faire de la phase d'étude du projet, auxquels s'ajoutent : D1.2 - Choix d'une solution D1.3 - Mise en production d'un service D2.1 - Exploitation des services *A2.1.2 Évaluation et maintien de la qualité de service* D3.1 - Conception d'une solution d'infrastructure (P1) Mise en production d'un service *SI1 – Installer, configurer et administrer le système d'exploitation d'une solution technique d'accès* *SI1- Spécifier les procédures d'alerte associées au service* *SI1 – Valider et documenter une solution technique d'accès* (P3) Administration et supervision d'une infrastructure *S3- Installer un système de gestion des éléments d'infrastructure,* *S3- Installer un outil de supervision, métrologie avec dispositif d'alerte* *S3- Installer et configurer des éléments de sécurité permettant d'assurer la protection du système informatique*
Notions EDM	EM4.5 – Le système d'information et les risques organisationnels
Documents joints	Expressions de besoins, ANNEXES 1, 2, 3, 4, 5, 6
Modalités de réception	Présentation d'un système opérationnel – recettage solution mouazi@ccicampus.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

AP4

SECURITE CIVILE

SÉCURITÉ CIVILE

Date limite de réponse : Lundi 15 Avril 2024

SOMMAIRE

1) CONTEXTE

1.1) Introduction

La sécurité civile désigne l'ensemble des moyens mis en œuvre par un État pour protéger ses citoyens, en temps de guerre comme en temps de paix.

En France, La Sécurité civile en tant qu'administration a été créée le 17 novembre 1951.

L'article 1 de la loi n°2004-811 du 13 août 2004 de modernisation de la sécurité civile définit que :

« La sécurité civile a pour objet la prévention des risques de toute nature, l'information et l'alerte des populations ainsi que la protection des personnes, des biens et de l'environnement par la préparation et la mise en œuvre de mesures et de moyens appropriés relevant de l'État, des collectivités territoriales et les personnes publiques ou privées. »

L'organisation de la sécurité civile, et, plus largement, de gestion de crise, repose en France sur des principes à la fois simples et clairs.

La garantie de la sécurité, de la salubrité et de la tranquillité publiques – regroupées sous l'appellation d' « ordre public » – sont l'objet d'une compétence obligatoire des autorités qui en sont investis. Cette compétence de police administrative générale les amène à prendre les mesures nécessaires pour prévenir et faire cesser les atteintes à l'ordre public.

Trois autorités sont traditionnellement responsables de la police administrative générale en France et exercent cette compétence en fonction de l'ampleur des problèmes à traiter :

- Le maire dans sa commune ;
- Le préfet de département ;
- Le Premier ministre.

En qualité de chef du gouvernement, le Premier ministre prépare et coordonne l'action des pouvoirs publics en cas de crise majeure (article L.111-3 du Code de la défense).

En ce qui concerne plus précisément la préparation et l'exécution des politiques de sécurité intérieure et de sécurité civile qui concourent à la défense et à la sécurité nationale, celles-ci relèvent du ministre de l'Intérieur, sous l'autorité du Premier ministre.

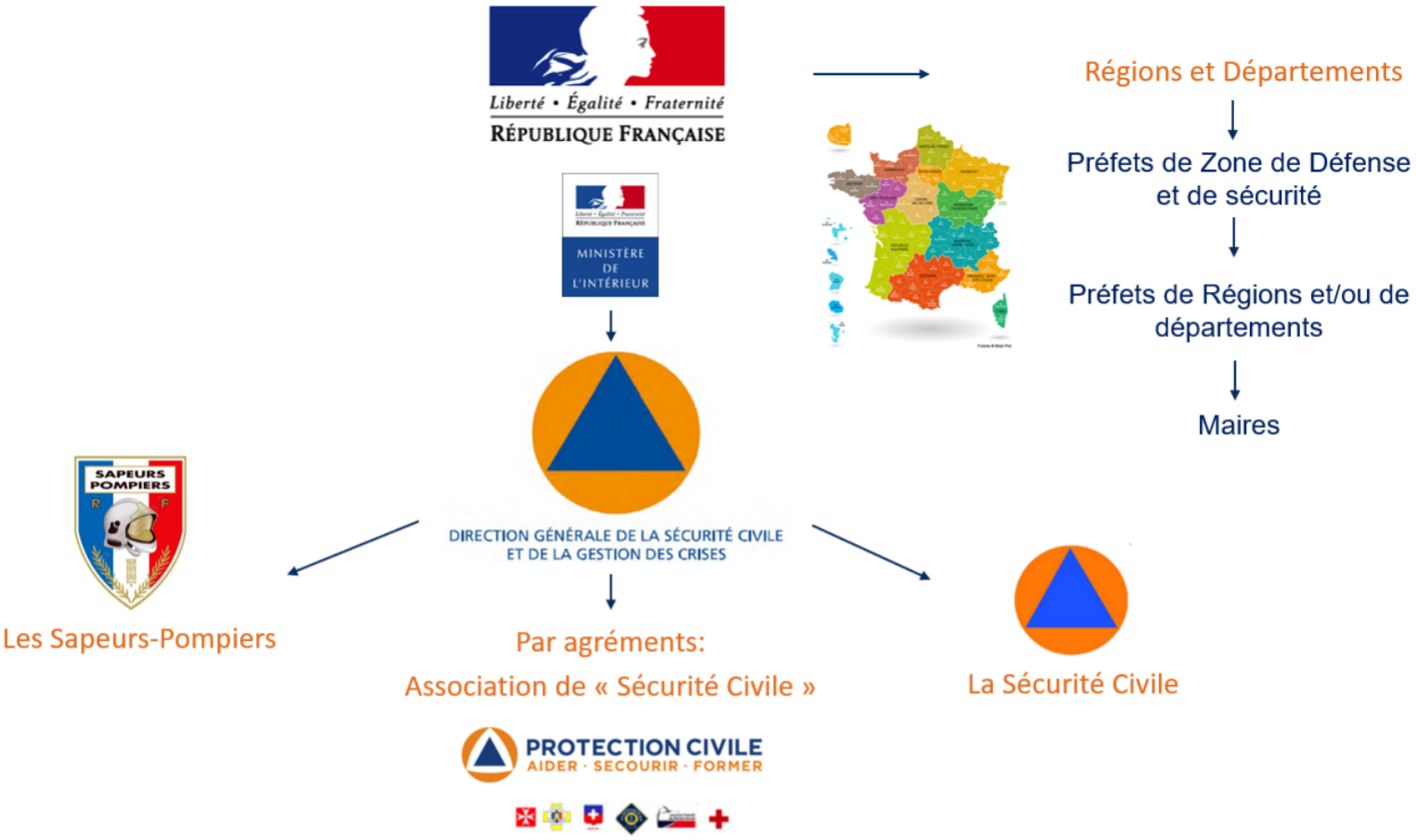
A ce titre, il est, sur le territoire de la République, responsable de l'ordre public, de la protection des personnes et des biens ainsi que de la sauvegarde des installations et ressources d'intérêt général.

En complément des échelons communal, départemental, et national, la zone de défense et de sécurité s'intercale dans des missions d'appui, de planification, de gestion de moyens, de synthèse.

Ce dispositif constitue le fondement de l'organisation de la sécurité civile et plus largement de la gestion de crise en France.

Il est complété par la loi de modernisation de la sécurité civile du 13 Août 2004 qui a refondé la doctrine et l'organisation de la sécurité civile en s'appuyant sur les retours d'expérience des évènements tels que la canicule (2003), les inondations du Gard (2002), l'explosion de l'usine AZF (2001) ou les tempêtes (1999).

1.2) Organisation de la Sécurité Civile en France



DIRECTION GÉNÉRALE DE LA SÉCURITÉ CIVILE ET DE LA GESTION DES CRISES

La Direction Générale de la Sécurité Civile et de la Gestion des Crises (DGSCGC) anime et coordonne, les forces civiles composées des Sapeurs-Pompiers, des personnels de la Sécurité Civile et des bénévoles membres des associations agréées.

La DGSCGC placée sous l'autorité du directeur général assisté d'un adjoint, chef de service, comprend :

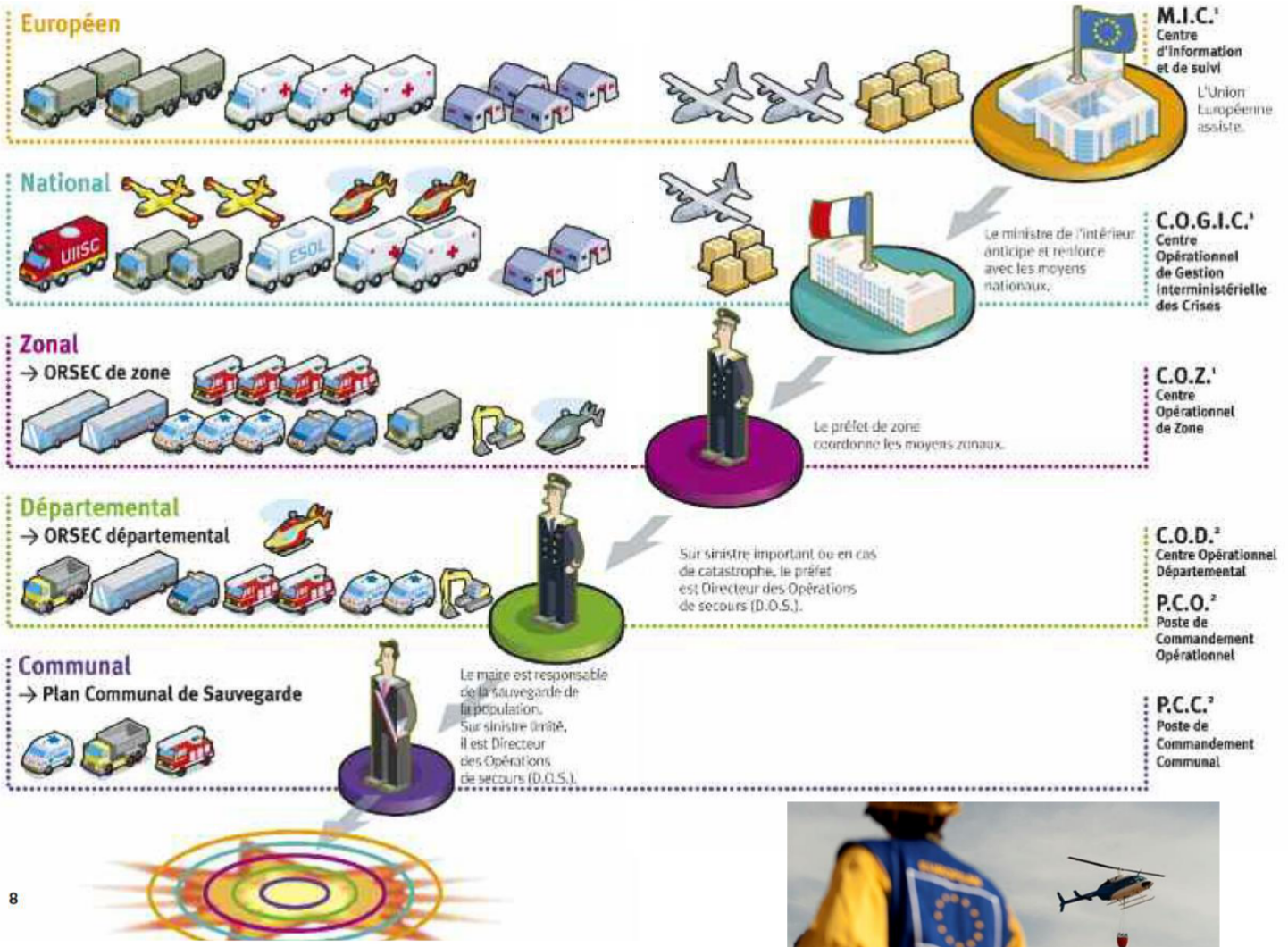
- L'Inspection de la Défense et de la Sécurité civiles ;
- La Direction des sapeurs-pompiers ;
- La sous-direction de la planification et de la gestion des crises qui anime le centre opérationnel de gestion interministérielle des crises (COGIC) ;
- La sous-direction des moyens nationaux ;
- Le Cabinet.

Parmi les acteurs de la sécurité civile en France, figurent les sapeurs-pompiers, les militaires des unités d'instruction et d'intervention, les pilotes d'avions et d'hélicoptères ainsi que les démineurs, les bénévoles des associations agrées. Tous ensemble, ils luttent au quotidien pour porter secours et assistance, en France comme à l'étranger, et assurer la sauvegarde des personnes et des biens ; pour faire face au quotidien comme à l'exceptionnel.

Organisation de la Réponse de SEcurité Civile (ORSEC), anciennement appelé ORganisation des SECours

Élaboré en Préfecture, le plan est conçu pour mobiliser et coordonner, sous l'autorité unique du préfet, les acteurs de la sécurité civile au-delà du niveau de réponse courant ou quotidien des services.

L'ORSEC est une organisation opérationnelle permanente, permettant d'anticiper et de gérer les événements en apportant une réponse graduée selon les circonstances. Elle impose, d'une part, à chaque acteur mentionné dans le plan, l'obligation de mettre en œuvre une organisation interne de réponse opérationnelle. Elle fédère, d'autre part, l'ensemble des acteurs de la sécurité civile, services permanents de secours et de sécurité, acteurs publics ou privés (opérateurs de réseaux, associations ou entreprises), autour du service préfectoral chargé de la protection civile.



Mécanisme européen de protection civile (MEPC)

Créé en 2001 d'abord pour aider à la coopération entre autorités nationales de protection civile de pays européens, ce mécanisme permet - quand cela est nécessaire et décidé - une réponse européenne mieux coordonnée, et optimisant l'efficacité de la réponse à une crise, notamment si elle est transfrontalière, de pollution marine (alors en lien avec l'Agence européenne de sécurité maritime ou EMSA), ou pour répondre à une demande d'aide d'une région touchée par une catastrophe. Une aide organisationnelle, en nature (dont apport de données satellites fraiches pour évaluer une situation et son évolution), le déploiement d'équipes ou d'experts. Le mécanisme doit aussi améliorer la qualité, la pertinence et l'accessibilité des informations mise à disposition en cas de catastrophe. Il favoriser les recherches concernant la résilience aux catastrophes. Il développe des outils d'alerte précoce1. De 2001 à 2018, son plus grand déploiement a concerné la crise des feux de forêts en Suède en 2018 (sur 3 semaines : 7 avions, 6 hélicoptères, 67 véhicules et plus de 360 pompiers et personnels d'appui pour lutter contre « des incendies forestiers sans précédent (...) 815 heures de vols et 8822 largages d'eau »).

1.3) Présentation du Service interministériel de défense et de protection civile

Au sein de chaque Préfecture, existe le Service interministériel de défense et de protection civile (SIDPC) ou Le Service Interministériel Régional des Affaires Civiles et Économiques de Défense et de Protection Civile (SIRACEDPC) dépendant du Directeur de Cabinet du Préfet, est chargé de la coordination de l'ensemble des acteurs concourant à la sécurité civile du département.

Ses missions sont de trois ordres :

► La prévention en amont de la crise

En matière de prévention, la connaissance du risque, naturel, technologique ou liée à la vie courante est essentielle. La sensibilisation, l'information des populations et des élus en amont sont primordiales. Son action en matière de défense civile et de prévention des actes malveillants s'est largement accrue (VIGIPIRATE, secteurs d'activité d'importance vitale, …). Il est également chargé d'une mission de prévention (établissements recevant du public, études de sécurité publique, secourisme, information préventive,).

Dans ce cadre, sur la base des études de risques, le SIDPC : - élabore et met à jour en lien avec les services compétents les plans de secours (dispositif ORSEC), le document départemental des risques majeurs (DDRM) et les dispositifs d'alerte, - organise des exercices qui associent la population et les acteurs locaux, - gère les travaux des commissions de sécurité des établissements recevant du public, - effectue le suivi des formations des secouristes et veille à la structuration du réseau des partenaires associatifs de la sécurité civile, - gère les demandes de déminage ainsi que les dossiers de spectacles pyrotechniques.

► Au cœur de la crise

Le SIDPC assiste le corps préfectoral. Il assure l'activation et l'animation de la salle opérationnelle de la Préfecture. Il constitue l'interface entre le Préfet, directeur des opérations de secours, et tous les acteurs publics et privés identifiés dans les plans de secours (services de l'État, collectivités, opérateurs, associations, experts, entreprises…) pour assurer la protection des populations (alerte, information et secours), des biens et de l'environnement et garantir, voire rétablir, si la crise les affecte, des fonctions essentielles (ravitaillement, transport, production d'énergie, télécommunications).

►L' après-crise

Le Préfet coordonne le suivi de l'après-crise. Après les opérations de secours, l'aide à la population change de nature. Toutefois elle demeure centrée sur la mise à disposition de moyens matériels ou humains pour faire face aux situations générées par l'événement (relogement, restauration du cadre de vie, redémarrage de l'activité, information et orientation des sinistrés…). Le SIDPC instruit les demandes de reconnaissance de l'état de catastrophes naturelles présentées par les communes, rassemble les rapports adéquats puis les transmet à la cellule catastrophe naturelle du ministère de l'Intérieur où les dossiers seront examinés en commission avant prise d'un arrêté interministériel de reconnaissance si la demande est éligible. Après chaque crise et chaque exercice, un retour d'expérience est établi pour identifier les enseignements et veiller à améliorer en continu des procédures. Le SIDPC assure également le suivi et l'élaboration des Plans Particuliers de Protection (PPP) et des Plans Particuliers Externes (PPE) au titre des points d'importance vitale du département ainsi que l'habilitation des personnels des directions départementales (à l'exception des militaires de la gendarmerie) dans le cadre de la défense civile.

1.4) Présentation des moyens d'alertes

Est toujours activé et assure une veille permanente

Au niveau national

- Un Centre Opérationnel de Zone (COZ), sous l'autorité du Préfet de Zone
- Le Centre Opérationnel de Gestion Interministérielle des Crises (C.O.G.I.C), sous l'autorité du Ministre de l'Intérieur.

Au niveau local

- Le Centre de Traitement de l'Alerte et le Centre Opérationnel Départemental d'Incendie et de Secours (CTA-CODIS) - Réceptionne les appels « 18 »
- Le Centre de Réception et de Régulation des Appels (CRRA) du SAMU (ou centre 15) → « 15 et 112 »
- Le Centre d'Information et de Commandement (CIC) → « 17 »

En cas de crise, peut-être activé :

- Le Poste de Commandement Communal (PCC), sous l'autorité du Maire
- Un Poste de Commandement Opérationnel (PCO) sous l'autorité du Chef des Opérations de secours
- Un Centre Opérationnel Départemental (COD), sous l'autorité du Préfet

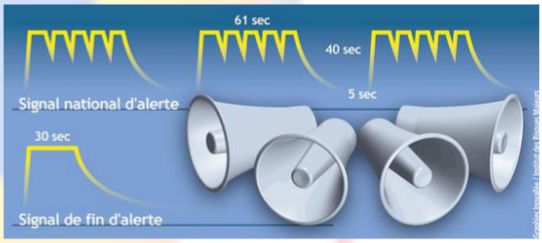
L'alerte aux populations

L'automate d'alerte de la préfecture

En cas d'indisponibilité de l'automate d'alerte, la préfecture assure l'appel des maires du département avec, le cas échéant, le concours des forces de l'ordre.

Le Signal National d'Alerte est la diffusion d'un signal sonore par une sirène pour avertir la population d'un danger imminent. Un essai des sirènes est effectué tous les 1ers mercredis du mois à 12h00.

Limiter à 3 répétitions du cycle d'1 minute et 41 secondes permet donc de le percevoir efficacement tout en évitant de générer un stress supplémentaire à une population déjà soumise à une crise.



En 2013, on estime que 78 % des personnes ne savent pas quoi faire lorsque les sirènes retentissent hors essai.

Ce qu'il faut faire

Lorsque le signal d'alerte retentit, les personnes sont invitées

- À se confiner dans l'endroit clos le plus proche (domicile, lieu public, entreprise, école...) en colmatant les ouvertures, en coupant les ventilations, climatiseurs et chauffages, et en restant loin des fenêtres ;
- À s'abstenir de faire des flammes, de fumer, d'ouvrir les fenêtres ;
- À s'abstenir de téléphoner (ni téléphone fixe, ni téléphone mobile) sauf détresse vitale, afin de laisser les lignes libres pour les secours ;
- S'informer par les médias : télévision et Internet sont les sources les plus courantes, mais en cas de défaillance de tout le réseau, suite à une attaque informatique par exemple, les radios locales continueront d'émettre sur ondes courtes. France Info et France Inter constituent les principaux canaux pour les communications des autorités. Par ailleurs, en cas de défaillance du réseau d'électricité, il est toujours possible d'écouter la radio avec un poste à piles, à batterie, solaire ou bien à alternateur (« dynamo », manivelle permettant de charger la batterie). On peut toutefois noter qu'il est possible aujourd'hui de capter la radio avec la plupart des téléphones mobiles. La station répétera en boucle la situation et les consignes à suivre.
- Les enfants scolarisés sont pris en charge par l'école, c'est le lieu où ils sont le plus en sécurité. Il est donc dangereux et inutile d'aller les chercher.

1.5) Présentation du Service Interministériel départemental des systèmes d'informations et de communication (SIDSIC)

Le service interministériel départemental des systèmes d'information et de communication (SIDSIC) est placé sous l'autorité du secrétaire général de la préfecture, est chargé de missions opérationnelles de supervision et de maintenance de réseaux informatiques et télécoms gouvernementaux

Ces principales missions sont :

- D'assurer la continuité des liaisons gouvernementales et du support en situation de crise
- De veiller au maintien en condition des systèmes informatiques
- La conduite et l'intégration de projets concernant les réseaux informatiques et télécoms (téléphonie et radio numérique)
- La gestion des équipements, les applications informatiques et les sites intra, extra et internet.
- D'assurer une continuité de service au sein de la préfecture et des directions départementale interministérielle (DDI)
- D'assurer l'assistance aux utilisateurs de la préfecture et des sous-préfectures
- De mettre en œuvre une politique de sécurité des systèmes d'information
- La gestion du standard de la préfecture
- La gestion de l'automate d'alerte de la préfecture
- La gestion informatique et infrastructure du centre opérationnel départemental

Il veille à la qualité de service et à la convergence des technologies et des pratiques. Il lui appartient de garantir un service homogène sur son périmètre d'action.

2) LES ENJEUX

L'action fictive du projet prends place au sein du Service Interministériel départemental des systèmes d'informations et de communication (SIDSIC).

2.1) Les enjeux Informatique du Centre Opérationnel Départemental

Assurer un fonctionnement nominal et optimum des systèmes d'informations et de communication (SIC) en toutes circonstances sur place et à distance.

Le Centre Opérationnel Départemental est composé de :

- 1 salle de situation
- 1 salle de décision
- Des cellules de liaison : les services peuvent y joindre leur centre opérationnel respectif
- Des cellules spécifiques : médias, maires etc.

Infrastructures et matériels :

- Tableaux blancs, marqueurs, papiers et stylos en cas de défaillance du système informatique.
- Les postes de travail
- Les serveurs
- L'accès aux réseaux et les équipements permettant l'accès aux réseaux
  - Locaux
  - Internet
  - Radios
  - Satellites
- Téléphones (et téléphones de secours)
- Ordinateur avec plusieurs écrans :
  - 1 écran le suivi de l'opération
  - 1 écran avec le synoptique des moyens et la cartographie du département
  - 1 écran pour la gestion administrative
  - 1 écran pour la gestion des appels radio

Logiciels :

- Réception et gestion des appels
- Gestion et suivi des interventions et des intervenants
- Cartographie
- Annuaire France Télécom inversé

Objectifs :

Coordonner les actions et les acteurs.

- Visualiser en temps réel le **images de vidéo protection** / **Médias etc.** pour faire des points de situation
- Consulter les **cartographies opérationnelles** et informatives à partir du système d'information géographique (SIG) sur les différents risques répertoriés et les enjeux associés
- Communiquer avec les principales autorités publiques (**visioconférence, téléphone satellitaire** en cas de rupture du réseau de communication terrestre) en période de crise
- Utiliser une **main courante** informatisée de manière à suivre en temps réel l'événement et de disposer d'une chronologie des actions engagées.

Ces outils sont indispensables à l'efficacité et la réactivité des cellules de crise mises en place : Cellules Evaluation, Logistiques technique et sociale, Communication, Transmissions, Juridiques et Finances, services extérieurs.

2.2) Les enjeux SIC à distance

Si le Centre Opérationnel Départemental (COD) est situé dans les locaux de la Préfecture, il faut bien des acteurs sur les lieux de l'événement afin de porter assistance et secours et informer en temps réel de la situation et des besoins.

Pour cela, il faut assurer des liaisons entre le terrain et le COD, en fonction de l'ampleur et de l'envergure des événements, les besoins seront différents.

Ainsi ; le Service des Systèmes d'Information doit pouvoir mettre en œuvre tous les moyens de communication dont il dispose pour assurer la mise en œuvre de :

- Liaisons radio téléphoniques
- Accès Internet
- Liaisons téléphoniques, fax et transmissions de données
- Liaisons téléphoniques sur réseaux de téléphonie mobile
- Liaisons téléphoniques et/ou fax sur réseau téléphonique commuté fixe si une ou plusieurs lignes sont disponibles immédiatement.
- Groupes électrogènes portatifs

L'agent d'astreinte du Service Informatique est le premier agent de son service à être mobilisé. Il alerte les renforts adaptés à la mise en œuvre des moyens nécessaires à la cellule "Informatique / transmissions" du COD.

3) LE PROJET

Le projet doit permette aux Préfectures d'améliorer leur résilience informatique en cas de crise, optimiser son système d'information ainsi que l'accessibilité sécurisée de son système d'information à l'extérieur.

3.1) Objectifs

Réaliser une proposition technique et commerciale du projet avec un devis de votre projet incluant tous les éléments nécessaires à la réalisation du projet.

Afin de se donner une idée avant la mise en œuvre réelle du projet, il est demandé une mise en œuvre d'un maquettage sous environnement virtuel de l'ensemble des besoins exprimés au point 3.2 dans les délais fixés.

Les écarts liés aux contraintes de l'environnement virtuel seront à notifier par écrit.

3.2) Expressions des besoins

Lors de différents retours d'expériences (REX), il est apparu plusieurs difficultés et besoins dont voici quelques extraits communiqués par le Directeur du service SIDSIC de la Préfecture du Bas-Rhin.

« A plusieurs reprises en salle de crise, nous n'avions pas ou plus accès à Internet, nous devions utiliser le réseau mobile, qui était parfois saturé ou non fonctionnel. Sur le terrain il faudrait pouvoir accéder à nos outils et services habituels, de façon sécurisée, si possible, interconnecté, comme cela les échanges se réaliseront en temps réels et tout le monde aura le même niveau d'informations en temps réel ».

« On nous a recommandé le logiciel open source **eBrigade**, il permettrait de gérer du personnel, des interventions et de créer des mains courantes informatisés ainsi que la génération des rapports, cela permettrait aux différents acteurs d'accéder aux informations en direct et d'en exporter rapidement le contenu, nous souhaiterions le mettre en œuvre afin de le tester lors d'un prochain exercice afin d'en tirer des conclusions ».

« Nous avons le devoir d'être autonome et de garantir la sécurité des accès et des données. Nous devons avoir la maîtrise de notre infrastructure, des équipements et des outils que nous utilisons, c'est pourquoi nous voulons que tous les serveurs et services soient installés localement, la messagerie, eBrigade… »

« Par ailleurs, il faut un outil permettant de superviser les serveurs et équipements critiques, les administrateurs devront être averti par courrier électronique immédiatement en cas de dysfonctionnements. Cet outil servira également de tableau de bord (monitoring) pour connaître l'état du système d'informations en temps réel. »

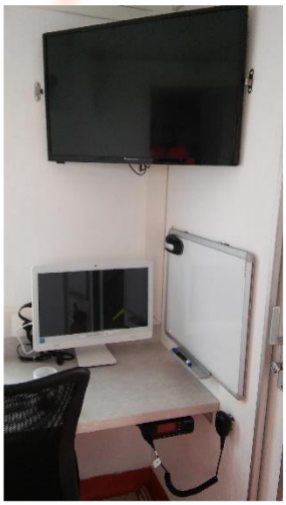
« Nous voulons également évaluer l'impact de la téléphonie sur le réseau et garantir son bon fonctionnement »

En Préfecture :

- Réseau électrique ondulé
- Redondance des routeurs et liens WAN *(2 routeurs, 2 accès Internet, pour la simulation 1 seul accès Internet est autorisé)*
- Accès aux ressources du serveur eBrigade en LAN et DMZ
- Messagerie électronique fonctionnelle uniquement en LAN/VPN RW
- L'ensemble des postes de travail sont sur Windows 10 Pro x64
- Couplage avec l'annuaire Active Directory de l'établissement (à créer).
- La cible est de 10 utilisateurs en simultanés

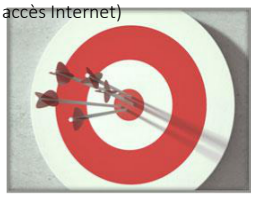
Connexion à distance :

- Connexion à distance au réseau informatique de la Préfecture en mode « OpenVPN Road Warrior »
- Une fois la connexion VPN RW initialisée, il sera possible de :
    - Envoi/Réception de courriers électroniques
    - Appels sur téléphone IP via softphone
    - L'accès et l'utilisation du logiciel eBrigade + accès en mode dégradé via DMZ



3.3) Objectifs attendues

Chaque groupe devra mettre en œuvre une solution technique répondant aux objectifs suivants :



1. Mise en œuvre d'une haute disponibilité de routeurs et liaison Internet redondée (2 routeurs / 2 accès Internet)
2. Mise en œuvre de 2 serveurs Active Directory (Principal et Secondaire)
3. Mise en œuvre d'1 serveur de messagerie et déploiement d'un client de messagerie -> Utilisation des comptes de l'Active Directory
4. Mise en œuvre d'1 serveur de supervision et de monitoring
   - Supervision de la disponibilité des routeurs et serveurs
   - Monitoring et historique des indisponibilités des routeurs et serveurs
   - Alerte par mail aux administrateurs en cas de panne
5. Mise en œuvre d'une solution de VPN RW (Road Warrior) -> Utilisation des comptes de l'Active Directory
   - Lorsque la connexion VPN est établie, l'accès aux ressources et outils est possible sinon non (Téléphonie, Messagerie…)
6. Mise en œuvre d'une DMZ pour accéder au Serveur WEB E-Brigade (Avec règles de pare-feu adaptés)
7. Respecter et appliquer les contraintes en 3.4

3.4) Contraintes

En compléments des objectifs fixés, voici les contraintes à respecter

A) Projet

- Respecter la date de début (08 Février 2024) et de fin de projet (15 Avril 2024)
- La solution doit être à moindre coût,
- Proposer un devis complet qui tiendra compte de tous les éléments indispensables au projet (matériels, licences, main d'œuvre…)
- Rendre les livrables aux dates prévues

B) Accessibilité aux données

- Une authentification à l'AD préalable sera nécessaire pour l'accès au contenu des données

4) EVALUATIONS

4.1) Groupes et Notations

- Le projet est à réaliser par groupes de 3
- La composition des groupes non libre – Note individuelle alignée sauf exception
- Chaque groupe désignera 1 Chef de Projet

A l'examen, l'épreuve E5 est individuelle, chaque partie de cet AP peut constituer un sujet d'examen

La notation est individuelle.

Il y aura plusieurs coefficients :

- Coeff. 1 pour chaque Oral, QCM et bonus ou défis individuels.
- Coeff. 2 pour chaque production écrite
- Coeff. 3 pour la démonstration technique (maquette)

4.2.2) Planning de préparation des examens E4-E5

Respecter la forme des dossiers et la nomenclature du dossier zip qui sera remis

4.3) Livrables et Oraux

- Chaque Chef de Projet déposera sur le dossier partagé avec les formateurs les différents livrables, dans les délais.
- Chaque membre du groupe aura accès au dossier partagé et devra suppléer le Chef de Projet en cas de défaillance.
- Rendre compte de problèmes par courriel aux formateurs ou conversation Teams (avec les deux formateurs invités dans la conversation).

LIVRABLE 1 : PROPOSTION TECHNIQUE ET COMMERCIALE

A ENVOYER LE

- Chaque groupe rédigera une proposition technique et commerciale selon le modèle proposé « LIVRABLE_1_GROUPE_X_YYYYMMJJ_HHMM » à rendre sous format électronique .DOCX et .PDF.

Votre proposition technique et commerciale répondra entièrement à l'expression des besoins du projet et indiquera précisément tous les éléments nécessaires à la réalisation du projet.

- La composition et présentation de votre groupe
- Le rappel des besoins et objectifs du projet
- Votre solution argumentée, avec un comparatif (tableau comparatif entre deux solutions pour chaque objectif)
- La liste des tâches prévisionnelle de votre projet

Lister les tâches dans l'ordre chronologique ; pour vous aider, identifier les tâches que vous pouvez réaliser sans attendre qu'une autre soit terminée

- Budget / Coût du projet

Nous n'attendons pas un devis, simplement un tableau reprenant les différentes ressources (humaines, financières, matérielles) nécessaires à la réalisation de votre projet et le coût global s'approchant du réel).

- Diagramme de Gantt prévisionnel de votre projet

Spécifiant les tâches, durées et ressources nécessaires apparaîtront clairement.

- Schéma réseau complet

Contenant : les pares-feux, serveurs, rôles/fonctionnalités, noms, adresses IP, équipements réseaux et connexions / liens et toutes informations utiles.

- Une fiche reprendra tous les éléments de configuration sans rédaction sous la forme d'un tableau *Site, Paramétrages des services selon les sites, Adressage IP/masque/passerelle, Dns selon les sites*
- Un tableau des flux de votre pare-feu

Règles du pare-feu principal indiquant précisément les flux autorisés ou bloqués en précisant la source, la destination, le port et la description

ORAL 1 :

PRESENTATION ORALE : 15 minutes

10 minutes de présentation puis 5 minutes de questions / réponses

Les éléments de réponses envoyés au Livrable 1 seront à commenter et justifier.
Le groupe sera évalué sur ses compétences relationnelles et sa capacité à :

- Analyser et interpréter l'expression des besoins
- Proposer des spécifications techniques et le choix des outils les plus adaptés pour la réalisation attendue
- Présenter une formalisation de la démarche envisagée pour répondre aux besoins exprimés

LIVRABLE 2 : RAPPORT DE CLÔTURE DE PROJET ET DOCUMENTATION TECHNIQUE A ENVOYER LE

- Chaque groupe livrera un rapport de clôture de projet selon le modèle proposé « LIVRABLE_2_GROUPE_X_Rapport_de_cloture_du_projet_et_documentation_YYYYMMJJ_HHMM » à rendre sous format électronique .DOCX et .PDF.

- Le rapport de clôture du projet est un document de synthèse qui permettra de :
    - Garder la trace des caractéristiques du projet à son démarrage
    - Formaliser les écarts finaux entre les résultats obtenus et les résultats attendus (Objectifs)
    - Cristalliser les bonnes pratiques à pérenniser et garder trace des erreurs à ne plus commettre ○ Faciliter le transfert de connaissances

- Documentation technique complète du projet à la façon d'un mode d'emploi, rédigée et mise en forme à rendre sous format électronique .DOCX **et** .PDF, obligatoire.

La documentation est autorisée à l'examen E5 et peut-être demandée à l'examen E4

ORAL 2 :

PHASE 1 - PRESENTATION ORALE : 10 minutes

Chaque groupe présentera son rapport de clôture de projet.

Le groupe présente sa solution et tous les éléments nécessaires pour justifier de la conformité de sa production aux exigences de la demande.

PHASE 2 - DEMONSTRATION TECHNIQUE : 20 minutes

Chaque groupe présentera techniquement la solution attendue.

La commission questionne ensuite le groupe et vérifie avec lui l'opérationnalité de la solution, la pertinence des outils utilisés et de la démarche suivie.

4.4) Pénalités et Bonus

Les productions à livrer (déposer) sur le dossier partagé avec les formateurs ont des dates de remise à respecter.

Chaque jour de retard entraîne le retrait d'1 point sur 20 par jour à l'exception du livrable 2, sanctionné d'un 0/20 (Date de fin du projet).

La remise aux formateurs des attestations de réussite des MOOC suivants seront comptabilisés (note sur 20 coeff. 1).

https://secnumacademie.gouv.fr/

https://atelier-rgpd.cnil.fr/

https://pix.fr

https://www.netacad.com/fr/courses/cybersecurity/introduction

https://www.netacad.com/fr/courses/cybersecurity/cybersecurity-essentials

ANNEXES

ANNEXE 1 : Organigramme de la Direction Générale de la Sécurité Civile et de la Gestion des Crises

ANNEXE 2 : Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu

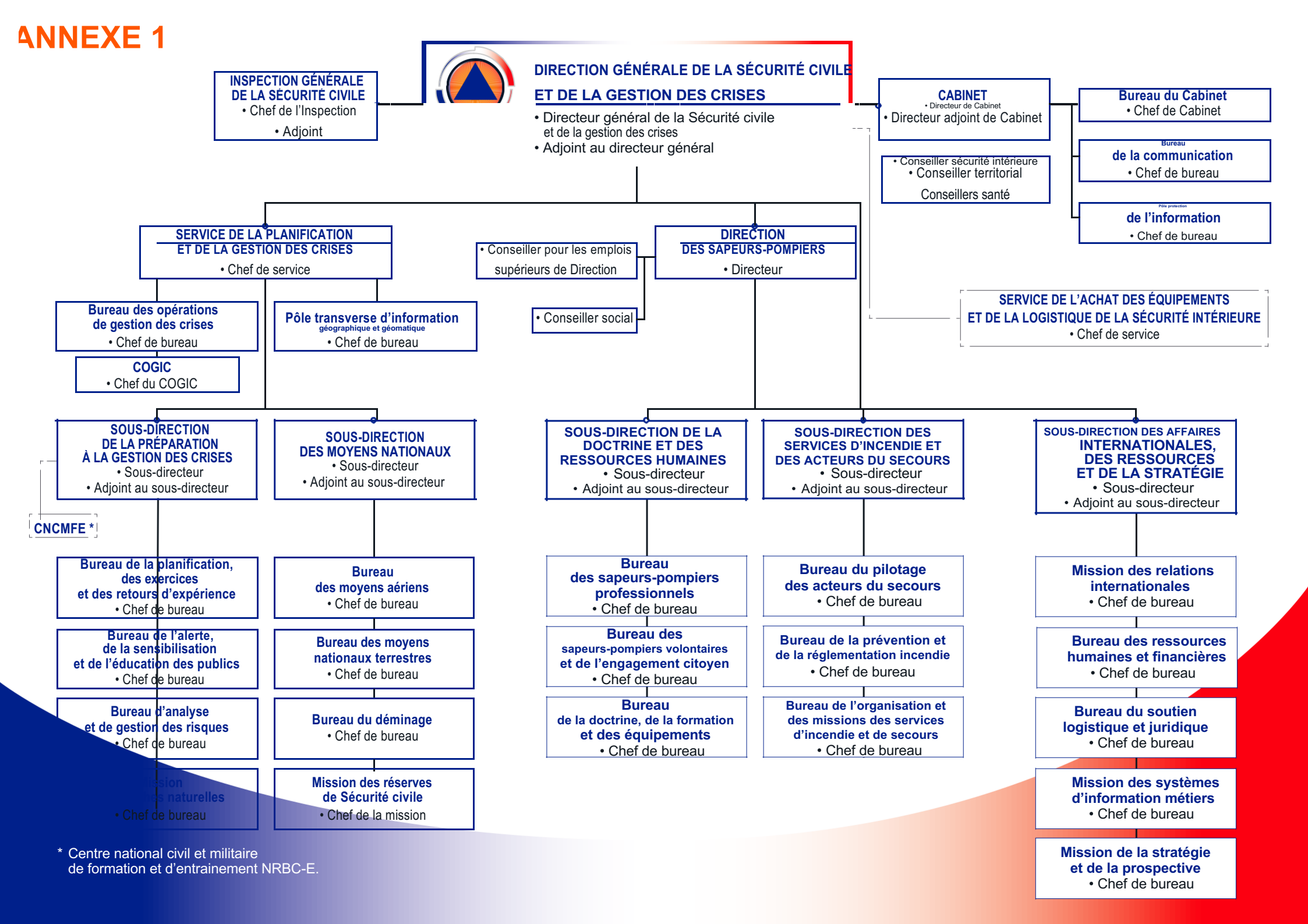
ANNEXE 3 : Plaquette de présentation du plan d'Organisation de la Réponse de Sécurité Civile

ANNEXE 4 : Plaquette de présentation de la Préfecture de la Zone de Défense et de Sécurité Est

ANNEXE 5 : Plaquette de présentation de la formation PSC-1-Prévention-Secours-Civique-1

ANNEXE 6 : Extrait des Métiers des Systèmes d'Informations et de Communication au sein du Ministère de l'Intérieur et de la Défense.

ANNEXE 1



* Centre national civil et militaire de formation et d'entrainement NRBC-E.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité
des systèmes d'information

Paris, le 30 mars 2013

N° DAT-NT-006/ANSSI/SDE/NP

Nombre de pages du document : 1+15

Note technique

Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu

Public visé:

Développeur	
Administrateur	X
RSSI	X
DSI	X
Utilisateur	X

Informations

Avertissement

Personnes ayant contribué à la rédaction de ce document:

Contributeurs	Rédigé par	Approuvé par	Date
BSS, BAI, BAS, LAM	BSS	SDE	30 mars 2013

Évolutions du document :

Version	Date	Nature des modifications
1.0	30 mars 2013	Version initiale

Pour toute remarque:

Contact	Adresse	@mél	Téléphone
Bureau Communication de l'ANSSI	51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP	communication@ssi.gouv.fr	01 71 75 84 04

Table des matières

1 Préambule

L'objectif de ce document est de fournir les éléments organisationnels permettant de structurer la base de règles constituant la politique de filtrage réseau appliquée sur un pare-feu d'interconnexion. Cette note est indépendante de la fonction du pare-feu (accès internet, cloisement de datacenter, isolation d'un partenaire) ; elle fait l'abstraction des solutions techniques qui peuvent être employées [1] (logiciel, équipement dédié) et ne tient pas compte de son mode d'administration (ligne de commande, interface web, client lourd). Certaines des préconisations mentionnées dans ce document ne seront donc applicables que si la technologie utilisée le permet ; il appartient au lecteur d'apprécier et de détermi-ner si les différentes recommandations sont adaptées à son cas d'usage. Ceci dépend notamment de la famille [2] à laquelle appartient le pare-feu.

Cette note technique s'adresse à l'ensemble des personnes qui ont la charge de définir, de mettre en œuvre ou d'administrer des architectures d'interconnexion sécurisées et qui souhaitent inscrire dans leur démarche la volonté d'assurer la pérénnité des politiques de filtrage réseau appliquées sur les pare-feux.

Dans la suite de ce document les termes « pare-feu » et « passerelle » seront utilisés indifférement, ils désignent tous les deux un équipement d'interconnexion capable de réaliser un filtrage réseau en tenant compte de l'état des connexions préalablement établies (stateful).

Les bonnes pratiques relatives au positionnement d'un pare-feu dans une architecture ne sont pas pré-sentées dans ce guide, celles-ci sont détaillées dans un document complémentaire publié par l'ANSSI intitulé « Définition d'une architecture de passerelle d'interconnexion sécurisée ». Ce guide est dispo-nible dans la section « Bonnes pratiques ! Recommandations et guides ! Sécurité des réseaux » sur www.ssi.gouv.fr.

1. Pour rappel, la liste des pare-feux qualifiés par l'ANSSI est disponible dans la section « Certification/ Qualification » sur www.ssi.gouv.fr.

2. En effet, il existe deux catégories de pare-feux, la première concerne ceux dont les règles de filtrage sont définies par paire d'interfaces réseaux (une entrante, une sortante), la seconde ceux dont les règles sont définies globalement. Dans ce deuxième cas, ce n'est pas l'administrateur qui détermine les interfaces d'entrée/sortie auxquelles s'appliquent chacune des règles mais le pare-feu lui même.

2 Pourquoi cette note ?

La rédaction de cette note technique a été motivée par les raisons suivantes :

Les architectures d'interconnexion se complexifient de plus en plus pour pouvoir faire face aux nouvelles menaces, différentes briques techniques y sont régulièrement ajoutées (exemple : IDS, Firewall Web Applicatif). Le pare-feu reste cependant l'un des éléments majeurs d'une défense en profondeur [3] efficace, il est le premier rempart pour stopper les attaques ou ralentir leur pro-gression.

L'ajout permanent de nouvelles fonctionnalités aux pare-feux (ou à leurs outils de management) complexifie leur administration et peut rendre la lisibilité des politiques de filtrage réseau plus difficile.

L'historique parfois lourd des passerelles dégrade naturellement l'état des politiques de pare-feux (méconnaissance de l'utilité des certaines règles, non suppression de règles liées à des équipements retirés de la production).

La rotation des équipes en charge de l'administration des passerelles peut conduire à une dérive des configurations (réutilisation d'adresses, règles surchargées).

3. Le concept de défense en profondeur est détaillé dans un mémento disponible dans la section « Bonnes pratiques ! Outils méthodologiques » sur www.ssi.gouv.fr

3 Organisation d'une politique de filtrage réseau

3.1 Présentation du modèle

La politique de filtrage d'une passerelle peut être construite en suivant un modèle d'organisation de règles applicable dans la majorité des cas d'usage.

L'organisation proposée dans ce document a pour objectifs :

de renforcer la protection du pare-feu et des réseaux de confiance qu'il

isole ; de faciliter la lisibilité de la politique de filtrage ;

de minimiser les sources d'erreurs et les dérives.

Cette organisation est construite selon un modèle de sécurité positif (tout ce qui n'est pas explicitement autorisé est interdit), il est possible de la décomposer en 6 sections rigoureusement ordonnées de la façon suivante :

Ordre	Contenu
Section n°1	Règles d'autorisation des flux à destination du pare-feu
Section n°2	Règles d'autorisation des flux émis par le pare-feu
Section n°3	Règle de protection du pare-feu
Section n°4	Règles d'autorisation des flux métiers
Section n°5	Règles "antiparasites"
Section n°6	Règle d'interdiction finale

3.2 Conditions d'application du modèle

Les conditions d'application du modèle présenté sont les suivantes :

les règles de filtrage sont évaluées séquentiellement par le pare-feu (de haut en bas) ;

une règle de filtrage unique est appliquée à un flux (la première qui autorise ou interdit ce flux) ; il est possible de définir précisement les flux ayant pour origine ou destination le pare-feu [4]. Si cela n'est pas possible les sections n°1 et n°2 ne seront pas présentes dans la politique de filtrage.

4. Certaines solutions ne permettent pas de gérer finement les flux émis ou reçus par le pare-feu. Dans ces cas précis, des règles sont automatiquement ajoutées à la politique de filtrage, elles sont directement liées à l'activation de certains paramètres d'administration de la solution, et il n'est pas toujours possible de les désactiver (se référer au paragraphe 5.1).

3.3 Détail du modèle

3.3.1 Section n°1 : règles d'autorisation des flux à destination du pare-feu

Cette première section contient un nombre minimal de règles car un pare-feu n'offre qu'un nombre restreint de services, sa surface d'attaque doit être la plus réduite possible. Un pare-feu doit idéalement être administré et supervisé via une interface réseau physique dédiée connectée à un réseau d'adminis-tration.

Deux types de règles constituent cette section :

les règles autorisant les services d'administration de la

passerelle ; les règles autorisant les services de supervision de la

passerelle. Voici une illustration simple :

Source	Destination	Service	Action	Journalisation
Serveurs d'administration	Interface d'administration de la passerelle	ssh, https	Autoriser	Oui
Serveurs de supervision	Interface d'administration de la passerelle	get-snmp	Autoriser	Oui

R1	Les règles de sécurité qui autorisent l'accès aux services proposés par un pare-feu doivent être regroupées dans la politique de filtrage. Ces règles sont peu nombreuses et doivent être définies précisément, en particulier au niveau de leurs adresses sources et de leurs services.

3.3.2 Section n°2 : règles d'autorisation des flux émis par le pare-feu

Cette seconde section contient également un nombre limité de règles, elle ne décrit que les flux ayant pour origine la passerelle elle-même.

Trois types de règles constituent cette section :

les règles autorisant les services d'envoi de journaux de la passerelle

; les règles autorisant les services d'alerte de la passerelle ;

les règles autorisant les services qui permettent le maintien en condition opérationelle de la passerelle (par exemple les flux de sauvegarde).

Voici une illustration simple :

Source	Destination	Service	Action	Journalisation
Interface d'administration de la passerelle	Serveur de journaux	syslog	Autoriser	Oui
Interface d'administration de la passerelle	Serveur de supervision	trap-snmp	Autoriser	Oui
Interface d'administration de la passerelle	Serveur de sauvegarde	ssh	Autoriser	Oui

R2	Les règles de sécurité qui autorisent les flux ayant pour origine le pare-feu doivent être regroupées dans la politique de filtrage. Ces règles sont peu nombreuses et doivent être définies précisément, en particulier au niveau de leurs adresses de destinations et de leurs services.

3.3.3 Section n°3 : règle de protection du pare-feu

Cette section ne comporte qu'une seule règle dite de protection de la passerelle ; elle est toujours la même et peut être décrite de la façon suivante :

Source	Destination	Service	Action	Journalisation
Toutes	Toutes les interfaces de la passerelle	Tous	Interdire	Oui

L'action « Interdire » correspond à une suppression du trafic sans réponse du pare-feu (action drop en anglais), cela permet d'éviter un signalement trop explicite de la passerelle aux éventuels attaquants.

Cette protection permet de « verrouiller » l'accès à la passerelle, si dans la suite de la politique est ajoutée une règle qui va à l'encontre (autorisation de flux à destination du pare-feu), celle-ci ne sera pas prise en compte. Elle pourra même être signalée comme incohérente si la solution technique est en mesure d'effectuer cette vérification. La journalisation est obligatoirement activée pour cette règle afin de conserver la trace de l'ensemble des flux non légitimes à destination de la passerelle.

R3	La mise en place d'une règle de protection du pare-feu est impérative pour prévenir l'ouverture de flux non légitimes à destination de la passerelle ; la journalisation de cette règle permet de conserver la trace de ces flux illégitimes.

3.3.4 Section n°4 : règles d'autorisation des flux métiers

Cette section contient les règles d'autorisation qui décrivent les flux métiers, celles-ci sont ordonnées selon une logique établie ; plusieurs orientations sont possibles, en voici deux exemples :

Organisation des règles en fonction des entités métier : les règles sont regroupées en fonction des entités métiers auxquelles elles ouvrent des services (comptabilité, ressources humaines).

Organisation des règles en fonction des services offerts : les règles sont regroupées en fonction des services autorisés (navigation internet, accès aux proxy, accès aux bases de données).

Le choix de l'organisation des règles est dépendant de plusieurs éléments du contexte comme le nombre de règles de la politique ou encore le rôle de la passerelle (accès internet, cloisement de datacenter, accès partenaire).

R4	Les règles qui autorisent les flux métiers doivent être regroupées et organisées selon une logique établie et adaptée au contexte. Ces règles constituent l'essentiel de la politique de filtrage, elles doivent être définies précisement au niveau de leurs adresses sources, de leurs adresses de destination et de leur services.

3.3.5 Section n°5 : règles "antiparasites"

Cette section est facultative, elle s'inscrit dans le cadre d'une politique globale de journalisation. Elle contient la liste des règles décrivant les flux non autorisés dont la trace n'est volontaire-ment pas conservée (certains flux de broadcast par exemple) afin de maintenir les journaux de la passerelle exploitables. Cela suppose qu'une trace de ces flux est conservée par une autre brique de l'architecture (cela doit être documenté dans la politique globale de journalisation).

La règle suivante illustre cette section :

Source	Destination	Service	Action	Journalisation
Réseau de test	255.255.255.255	udp-137,udp-138 (netbios)	Interdire	Non

R5	Les règles "antiparasites" peuvent être utilisées pour alléger les journaux de la passerelle, mais doivent être établies en accord avec la politique globale de journalisation de l'archi-tecture.

3.3.6 Section n°6 : règle d'interdiction finale

Cette section ne comporte qu'une seule règle d'interdiction ; celle-ci est dite finale car celle se trouve toujours en dernière position dans la politique. Cette règle a pour objectifs d'une part d'interdire le trafic qui n'a pas été explicitement autorisé par les règles précédentes, d'autre part de conserver une trace des flux non légitimes. La règle de protection est toujours la même et peut être décrite de la façon suivante :

Source	Destination	Service	Action	Journalisation
Toutes	Toutes	Tous	Interdire	Oui

Certaines solutions techniques appliquent automatiquement une règle d'interdiction à la fin de la po-litique de filtrage, mais celle-ci n'est généralement pas journalisée ou n'apparaît pas explicitement à la fin de la politique ; c'est la raison pour laquelle une règle finale explicite est ajoutée dans tous les cas.

R6	L'ajout d'une règle explicite d'interdiction finale journalisée garantit l'application du mo-dèle de sécurité positif (tout ce qui n'a pas été autorisé précédemment est interdit) et permet de conserver la trace des flux non légitimes.

4 Mise en forme d'une politique de filtrage réseau

La lisibilité et la maintenabilité d'une politique de filtrage dépend avant tout de sa forme ; c'est la raison pour laquelle il est primordial de définir et de documenter les conventions à respecter lors de son élaboration et de sa mise à jour.

Une politique de filtrage se traduit par une liste de règles, elles même composées d'objets de différentes natures :

des machines (Une adresse IP) ;

des réseaux (Une adresse de réseau combinée à un masque) ;

des plages réseau (Une suite d'adresses IP consécutives) ;

des services (tcp, udp, autres)

; des groupes d'objets.

R7	La gestion rigoureuse d'une politique de sécurité commence par la définition précise de la représentation des objets et des règles qui la composent.

4.1 Mise en forme des objets

4.1.1 Convention de nommage

La définition d'une convention de nommage rigoureuse pour chacun des types d'objets utilisés dans la politique de sécurité facilite les opérations suivantes :

la recherche (dans une liste de taille conséquente)

; la manipulation (tri, mise à jour, suppression) ;

l'audit.

Plusieurs orientations sont possibles pour définir une convention de nommage, voici deux exemples :

Convention de nommage fonctionnelle : les objets sont nommés en fonction de leur rôle, par exemple : srv_dns-interne, tcp_appli1.

Convention de nommage technique : les objets sont nommés en fonction d'une caractéristique technique qui leur est propre (adresse IP, nom d'hote, port), par exemple : srv_appollo, tcp_21000.

Le choix de l'orientation d'une convention dépend d'éléments liés au contexte, en particulier de la connaissance précise du métier. Il est possible de combiner différentes conventions, mais il faut garder à l'esprit de ne pas trop alourdir la lecture. La solution technique utilisée pourra également être un facteur limitant à prendre en considération (existence d'une taille maximale des noms d'objets ou

encore présence de termes réservés). La casse fait également partie des paramètres à définir dans la convention.

R8	Une convention de nommage doit être définie pour l'ensemble des types d'objets qui com-posent les règles de la politique de filtrage.

4.1.2 Convention de mise en forme

Certaines solutions offrent la possibilité de colorer une partie des objets (machine, réseau, plage réseau), c'est un moyen supplémentaire utilisé pour augmenter la lisibilité de la politique de sécurité. Des incohérences grossières peuvent ainsi être détectées visuellement plus rapidement.
La logique consiste à utiliser une couleur pour l'ensemble des objets appartenant à une même zone, le code couleur est établi en fonction d'un critère ; par exemple :

Le niveau de confiance de la zone : un jeu de dégradé est choisi afin d'associer une couleur à cha-cun des niveaux de confiance existant dans l'architecture. Le tableau 1 est un exemple illustrant ce type de code couleur :

Couleur	Type de zone
	Réseau externe
	DMZ publique
	DMZ privée
	Réseau interne

Table 1 – Coloration selon le niveau de confiance

Le rôle de la zone : une couleur est associée selon un critère fonctionnel des différents types de zone existant dans l'architecture. Le tableau 2 est un exemple illustrant ce type de code couleur :

Couleur	Type de zone
	DMZ hébergeant les serveurs d'authentification
	DMZ hébergeant les serveurs de base de données
	DMZ hébergeant les proxys
	DMZ hébergeant les reverse proxys

Table 2 – Coloration selon un critère fonctionnel

R9	La définition d'une convention de coloration des objets qui composent les règles de sécurité est une aide supplémentaire à la compréhension de la politique.

4.2 Mise en forme des règles de sécurité

4.2.1 Convention de nommage

4.2.1.1 Nommage des règles

Certaines solutions permettent d'attribuer un nom aux règles de sécurité, ce champ est utilisé pour aider à la compréhension de la politique, des flêches peuvent être employées pour indiquer le sens de communication que chacune des règles doit transcrire.

Exemple : Relais DNS -> DNS publiques

4.2.1.2 Commentaires des règles

Certaines solutions autorisent l'ajout de commentaires aux règles de sécurité, ce champ est utilisé pour décrire plus précisement la signification de chacune des règles composant la politique de filtrage. Voici une liste non exhaustive d'éléments qui peuvent apparaître dans un commentaire :

le descriptif fonctionnel de la règle ;

la date d'implémentation ou de mise à jour de la règle dans un format court ;

la référence de la demande dans l'outil de gestion de tickets (s'il existe) qui a conduit à la création ou à la modification de la règle ;

l'identifiant de l'intervenant qui a implémenté ou mis à jour la règle dans un format court.

Les éléments choisis doivent être réfléchis et adaptés au contexte, la solution technique utilisée pourra également être un facteur limitant à prendre en considération lors du choix des éléments à inclure dans les commentaires (taille maximale du champ commentaire par exemple).

R10	Si des champs textuels éditables spécifiques à chacune des règles de sécurité sont dispo-nibles, il est important de les utiliser pour expliciter le contenu de la politique de filtrage. Les élements constitutifs de ces champs doivent respecter une structure préalablement définie et adaptée au contexte.

4.3 Séparateurs de règles

Certaines solutions sont capables de scinder la politique de filtrage à l'aide de séparateurs de règles, cette fonctionnalité est utilisée pour augmenter la lisibilité de la politique et faciliter son exploitation. Ces séparateurs sont employés pour faire apparaître les sections présentées précédemment et mettre en évidence les regroupements opérés pour les flux métiers (contenu de la section n°4). Si les séparateurs disposent d'un champ texte éditable, une convention de nommage doit également être définie pour celui-ci.

Voici une illustration simple reprenant les 6 sections et quelques exemples de flux métiers :

Section	Intitulé du séparateur
1	Flux à destination de la passerelle
2	Flux émis par la passerelle
3	Règle de protection de la passerelle
4	Flux métiers
	–|Flux d'accès aux bases de données
	——|Flux concernant la ferme 1 de bases de données
	——|Flux concernant la ferme 2 de bases de données
	–|Flux d'accès aux proxys
	——|Flux concernant le proxy x
	——|Flux concernant le proxy y
5	Règles "antiparasites"
6	Règle d'interdiction finale

5 Bonnes pratiques d'ordre général

5.1 Désactivation des flux implicites

Certaines solutions permettent l'ouverture de flux implicites dans le but de faciliter l'administration de la passerelle ou de simplifier l'ouverture de services considérés parfois à tort comme non risqués. Malheureusement cela conduit souvent à l'ouverture de règles trop permissives ou méconnues des ad-ministrateurs.

Voici le type de flux implicites que l'on peut rencontrer :

flux nécessaires à l'administration de la passerelle (https, ssh) ;

flux nécessaires au fonctionnement de la passerelle (snmp, ntp,

syslog) ; flux permettant l'établissement des VPN (IKE, IPsec) ;

flux DNS ;

flux ICMP.

R11	Une gestion rigoureuse de la politique de filtrage conduit à désactiver les flux implicites s'ils existent et si la désactivation est possible ; les flux légitimes quels qu'ils soient doivent être définis manuellement et précisément par les administrateurs.

L'objectif de cette démarche est double :

porter à la connaissance des administrateurs l'ensemble des règles de sécurité appliquées par le pare-feu ;

réduire la surface d'attaque de la passerelle et des réseaux qu'elle protège on n'autorisant que les flux stritement nécessaires au besoin.

5.2 Vérification de la séquence de démarrage

Un pare-feu peut être vulnérable lors de sa séquence de démarrage. En effet, durant le laps de temps qui sépare l'allumage électrique de l'équipement et l'application effective de la politique de filtrage réseau, le pare-feu peut se retrouver dans un état ne lui permettant pas d'assurer la sécurité des réseaux qu'il protège ainsi que sa propre protection. Dans le pire des cas, le pare-feu ne filtrera pas les paquets et les routera en effectuant aucun contrôle. Il convient donc de vérifier à quelle étape de la séquence de démarrage le routage s'active sur l'équipement.

R12	Afin d'éviter toute exposition inutile des réseaux et du pare-feu, il est recommandé de se documenter sur le fonctionnement précis de la solution employée, de réaliser des tests et de prendre en considération leurs résultats lors des opérations nécessitant un redémarrage de l'équipement (maintenance par exemple).

6 Documentation, validation et maintenance

6.1 Documentation

Les choix réalisés en application des bonnes pratiques décrites dans ce guide doivent être formalisés dans un document transmis à l'ensemble des intervenants opérant sur les pare-feux concernés. L'effort de rédaction est nécessaire pour assurer le respect des consignes au delà des personnes qui les ont établies.

R13	Les consignes permettant la gestion des politiques de filtrage réseau doivent être documentées et diffusées aux personnes en charge de la mise en œuvre et la gestion des pare-feux.

6.2 Validation

Les politiques de filtrage mises en place doivent être validées en pratique pour s'assurer que la solution technique adoptée se comporte correctement (utilisation d'outil d'analyse réseau par exemple). Le respect du modèle présenté dans ce document contribue au maintien des politiques de filtrage, mais il ne permet pas de se prémunir contre certaines erreurs humaines ou certains fonctionnements spécifiques ; charge à l'administrateur de rester vigilant quant à la compréhension des opérations qu'il exécute.

R14	Une politique de filtrage réseau doit être testée une fois implémentée.

6.3 Maintenance

Pour conserver son efficacité et sa fonction de sécurisation, une politique de filtrage doit être passée en revue régulièrement.

Ces vérifications ont pour objectifs :

de supprimer les règles temporaires obsolètes créées depuis la dernière revue

; de corriger les éventuels écarts par rapport aux conventions en vigueur ;

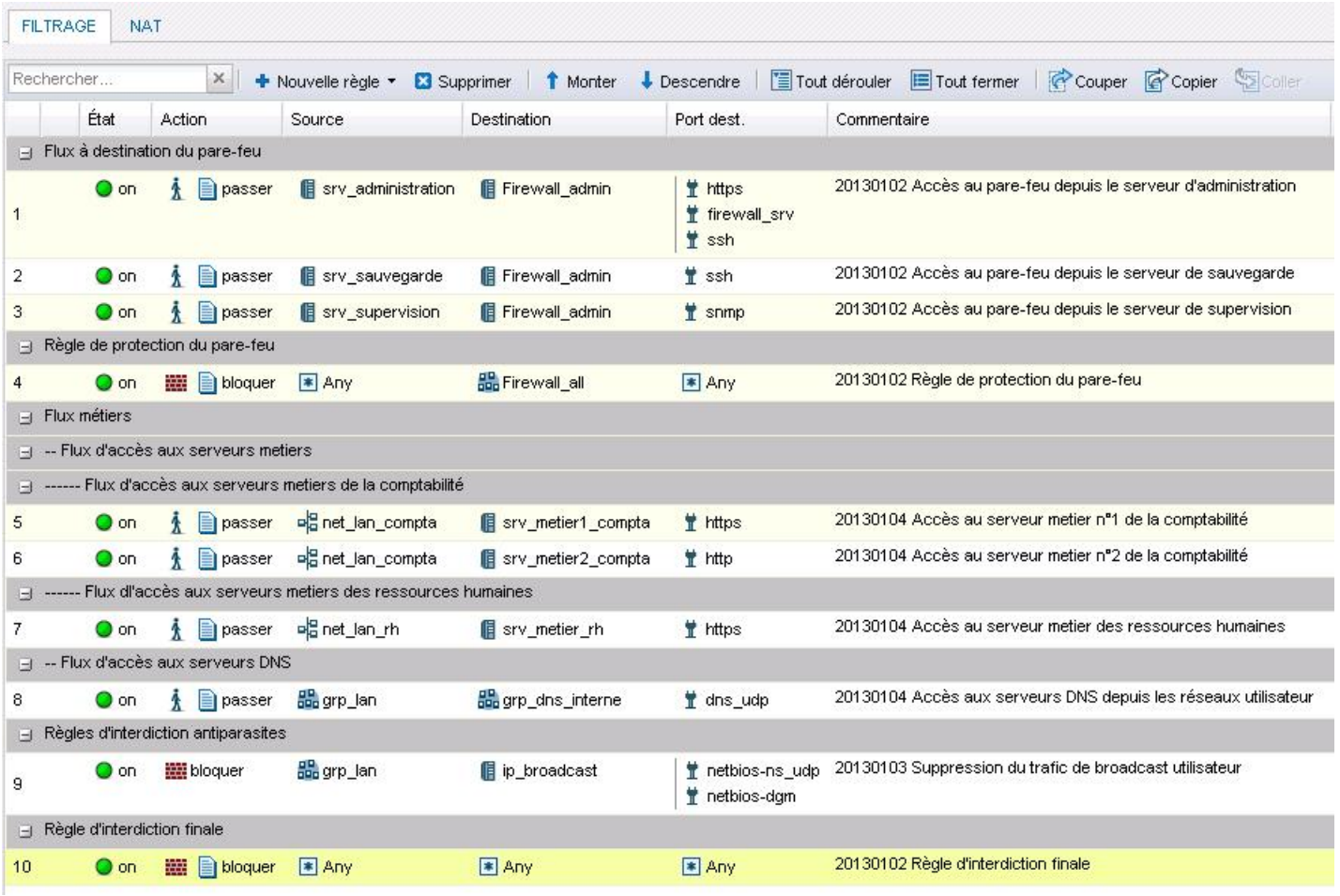
de vérifier la cohérence des règles ajoutées depuis la dernière revue : origine, utilité, précision, etc.

La présence de mécanismes techniques ou organisationnels visant à conserver sous contrôle la politique de filtrage ne dispense pas de la réalisation de ces revues régulières.

R15	Une politique de filtrage réseau doit être passée en revue à une fréquence bi-annuelle ou annuelle à minima.

7 Illustration

Une partie des recommandations présentées dans ce document sont illustrées à l'aide d'un jeu de règles simple défini sur un pare-feu NetAsq (solution qualifiée par l'ANSSI).



FILTRAGE | NAT

Rechercher... | Nouvelle règle | Supprimer | Monter | Descendre | Tout dérouler | Tout fermer | Couper | Copier | Coller

	État	Action	Source	Destination	Port dest.	Commentaire
Flux à destination du pare-feu						
1	on	passer	srv_administration	Firewall_admin	https firewall_srv ssh	20130102 Accès au pare-feu depuis le serveur d'administration
2	on	passer	srv_sauvegarde	Firewall_admin	ssh	20130102 Accès au pare-feu depuis le serveur de sauvegarde
3	on	passer	srv_supervision	Firewall_admin	snmp	20130102 Accès au pare-feu depuis le serveur de supervision
Règle de protection du pare-feu						
4	on	bloquer	Any	Firewall_all	Any	20130102 Règle de protection du pare-feu
Flux métiers						
-- Flux d'accès aux serveurs metiers						
------ Flux d'accès aux serveurs metiers de la comptabilité						
5	on	passer	net_lan_compta	srv_metier1_compta	https	20130104 Accès au serveur metier n°1 de la comptabilité
6	on	passer	net_lan_compta	srv_metier2_compta	http	20130104 Accès au serveur metier n°2 de la comptabilité
------ Flux dl'accès aux serveurs metiers des ressources humaines						
7	on	passer	net_lan_rh	srv_metier_rh	https	20130104 Accès au serveur metier des ressources humaines
-- Flux d'accès aux serveurs DNS						
8	on	passer	grp_lan	grp_dns_interne	dns_udp	20130104 Accès aux serveurs DNS depuis les réseaux utilisateur
Règles d'interdiction antiparasites						
9	on	bloquer	grp_lan	ip_broadcast	netbios-ns_udp netbios-dgm	20130103 Suppression du trafic de broadcast utilisateur
Règle d'interdiction finale						
10	on	bloquer	Any	Any	Any	20130102 Règle d'interdiction finale

Figure 1 – Politique de filtrage réseau sur NetAsq

Les flux émis par le pare-feu (section n°2) n'apparaissent pas dans l'exemple ci-dessous car ils sont définis implicitement (par exemple ntp et syslog) par la solution technique employée.

ANNEXE 3

O.R.SE.C.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR
DE L'OUTRE-MER
ET DES COLLECTIVITÉS
TERRITORIALES

Organisation de la Réponse de Sécurité Civile

pour la protection générale des populations

Le risque zéro n'existe pas

Tempête de 1999	Feux de forêt caniculaire de 2003	Accident industriel AZF 2001	Inondations 2001,2002, 2003




L'actualité se fait régulièrement l'écho d'événements soudains et dramatiques, qui touchent de nombreuses personnes.

Malgré les progrès technologiques, nous sommes toujours exposés à de nombreux aléas d'origine naturelle, technologique, ou sanitaire.

Leurs effets sont parfois amplifiés par le mode de fonctionnement de notre société très dépendante aujourd'hui :

- de l'énergie électrique,
- des réseaux de communications : téléphone, internet …,
- des moyens de communication: route, rail, aérien …,
- des approvisionnements en flux tendus.

Pour que notre société soit moins fragile, il faut :

- **réduire nos vulnérabilités** par des mesures de prévention,
- **préparer** à l'avance **une organisation solide et rôdée** pour répondre **dans l'urgence** à ces événements.

Soyons prêts à faire face ensemble

Pour faire face à ces événements, les pouvoirs publics s'appuient sur un dispositif de planification qui a évolué :

> **1952** création du **plan OR.SEC** (ORganisation des SECours) départemental placé sous l'autorité du préfet.

> **1987** en complément, création :

- **des plans OR.SEC. zonaux** au niveau des zones de défense,
- **des plans d'urgence** dans chaque département comprenant :

* les Plans Particuliers d'Intervention -P.P.I.-pour les installations dangereuses fixes,

* les Plans de Secours Spécialisés -P.S.S.- pour les autres risques technologiques et ceux d'origine naturelle

* les « plans rouges » destinés à porter secours à de nombreuses victimes.

> **2004**

Organisation de la Réponse de SEcurité Civile

Le plan O.R.SE.C. devient l'organisation unique chargée de gérer toutes les situations d'urgence :

La sécurité civile est l'affaire de tous

Le changement d'appellation implique d'élargir, au-delà du cercle des professionnels de l'urgence (sapeurs-pompiers, S.A.M.U., forces de l'ordre), **la préparation et la mobilisation** à **l'ensemble des acteurs publics et privés susceptibles d'être impliqués.**

Diverses réglementations imposent déjà à certains acteurs de développer des plans,par exemple :

- **les Plans d'Opération Interne (P.O.I.)** pour les installations classées « Seveso »,
- **les Plans Communaux de Sauvegarde (P.C.S.)** pour certaines communes,
- **les Plans d'Intervention et de Sécurité (P.I.S.)** pour les exploitants de certains réseaux routiers ou ferroviaires,
- **les Plans Blancs** pour les établissements de santé,
- …

Ces plans forment également la base de l'O.R.SE.C.

En effet, chaque acteur de l'O.R.SE.C., doit se préparer à intervenir en intégrant ses missions O.R.SE.C. dans sa propre organisation.

O.R.SE.C. est l'élément "chapeau"et coordonnateur de ces organisations.

Créer et entretenir le réseau des acteurs susceptibles d'être sollicités dans les situations d'urgence, développer les habitudes de travail en commun constituent un des objectifs du plan O.R.SE.C.

Que dit la loi de modernisation de la sécurité civile ?

Pour tous les acteurs

- Article 1er du décret n° 2005-1157 du 13 septembre 2005 relatif au plan O.R.SE.C.

« Chaque personne publique ou privée recensée dans le plan O.R.SE.C. : **a)** est en mesure d'assurer en permanence les missions qui lui sont dévolues dans ce cadre par le préfet de département, le préfet de zone ou par le préfet maritime ;
b) prépare sa propre organisation de gestion de l'événement …

Pour les exploitants de réseaux

- Extrait de l'article 6 de loi et de son décret d'application n° 2007-1400 du 28 septembre 2007.

« Les exploitants d'un service public destiné au public d'assainissement, de production ou de distribution d'eau pour la consommation humaine, d'électricité ou de gaz, ainsi que les opérateurs des réseaux de communications électroniques ouverts au publics prévoient les mesures nécessaires au maintien de la satisfaction des besoins prioritaires de la population lors de situations de crise.»
«les exploitants […] prennent toutes les mesures pour […] élaborer un plan interne de crise … »

Pour les communes

- Extrait de l'article 13 de la loi sur le plan communal de sauvegarde - P.C.S.

« Le plan communal de sauvegarde […] détermine, en fonction des risques connus, les mesures immédiates de sauvegarde et de protection des personnes[…]. Il est obligatoire dans les communes dotées d'un plan de prévention des risques naturels prévisibles approuvé ou comprises dans le champ d'application d'un plan particulier d'intervention. »

Pour tous les citoyens

- Extrait de l' article 4 de la loi.

« Toute personne concourt par son comportement à la sécurité civile.…»

La préparationet l'intervention des acteurs sont coordonnées par une autorité unique

La réponse aux situations d'urgence exige la mobilisation rapide de tous les moyens publics et privés et leur coordination efficace par une **direction unique**. Elle est assurée par **les maires ou les préfets, autorités de police générale,** investis de pouvoirs étendus dans de tels cas.

En cas d'événement

La **direction des opérations de secours** repose :

- dans le cas général, au quotidien, le plus couramment, sur **le maire**;
- le cas échéant, si la gravité de l'événement dépasse les capacités locales d'intervention ou lorsque le problème concerne plusieurs communes, sur le **préfet de département** qui **commande le dispositif O.R.SE.C.** Le maire reste alors chargé des mesures de soutien à sa population.

Cas particulier : pour Paris et les départements de la petite couronne, la direction des opérations de secours est assurée en permanence par le préfet de police, qui peut la déléguer aux préfets des départements concernés.

En mer, c'est le **préfet maritime** qui assure la direction des opérations de secours et commande le dispositif O.R.SE.C. maritime.

Rôle du Directeur des Opérations de Secours (D.O.S.)

- **Diriger et coordonner les actions de tous les intervenants.**
- **Assurer et coordonner la communication.**
- **Informer les niveaux administratifs supérieurs.**
- **Anticiper les conséquences.**
- **Mobiliser les moyens publics et privés sur son territoire de compétence.**

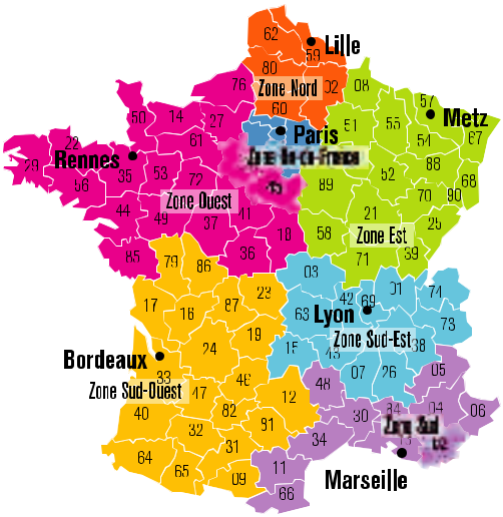
Si les conséquences risquent de dépasser les limites ou les capacités d'un département, le préfet de zone de défense, voire le gouvernement, interviennent dans la conduite des opérations lorsque c'est nécessaire.

Dans le cadre de la préparation

L'organisation des opérations se prépare dans le cadre du plan O.R.SE.C. qui est élaboré au niveau :

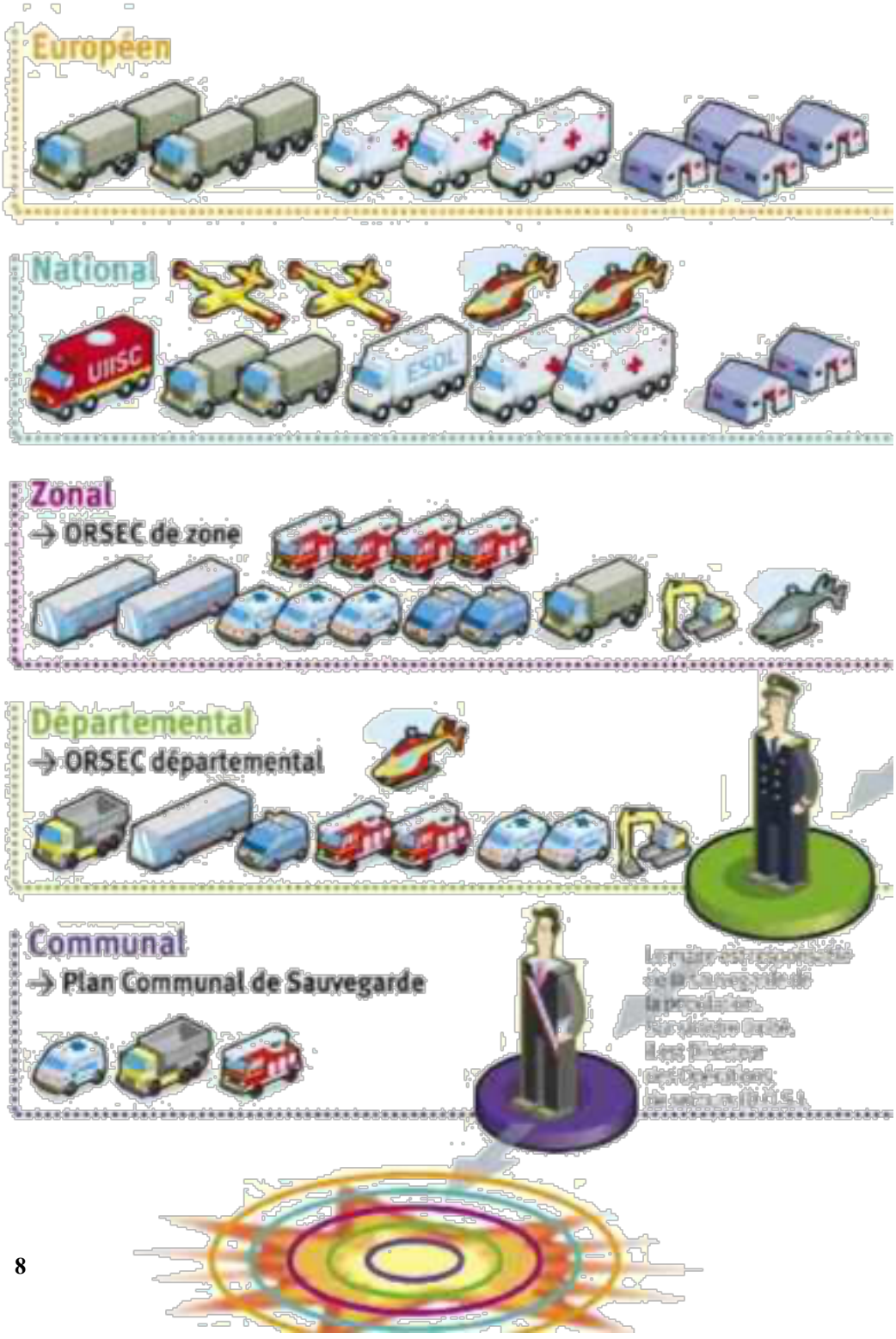
- départemental par les préfets de département,
- zonal par les préfets de zone,
- maritime par les préfets maritimes.

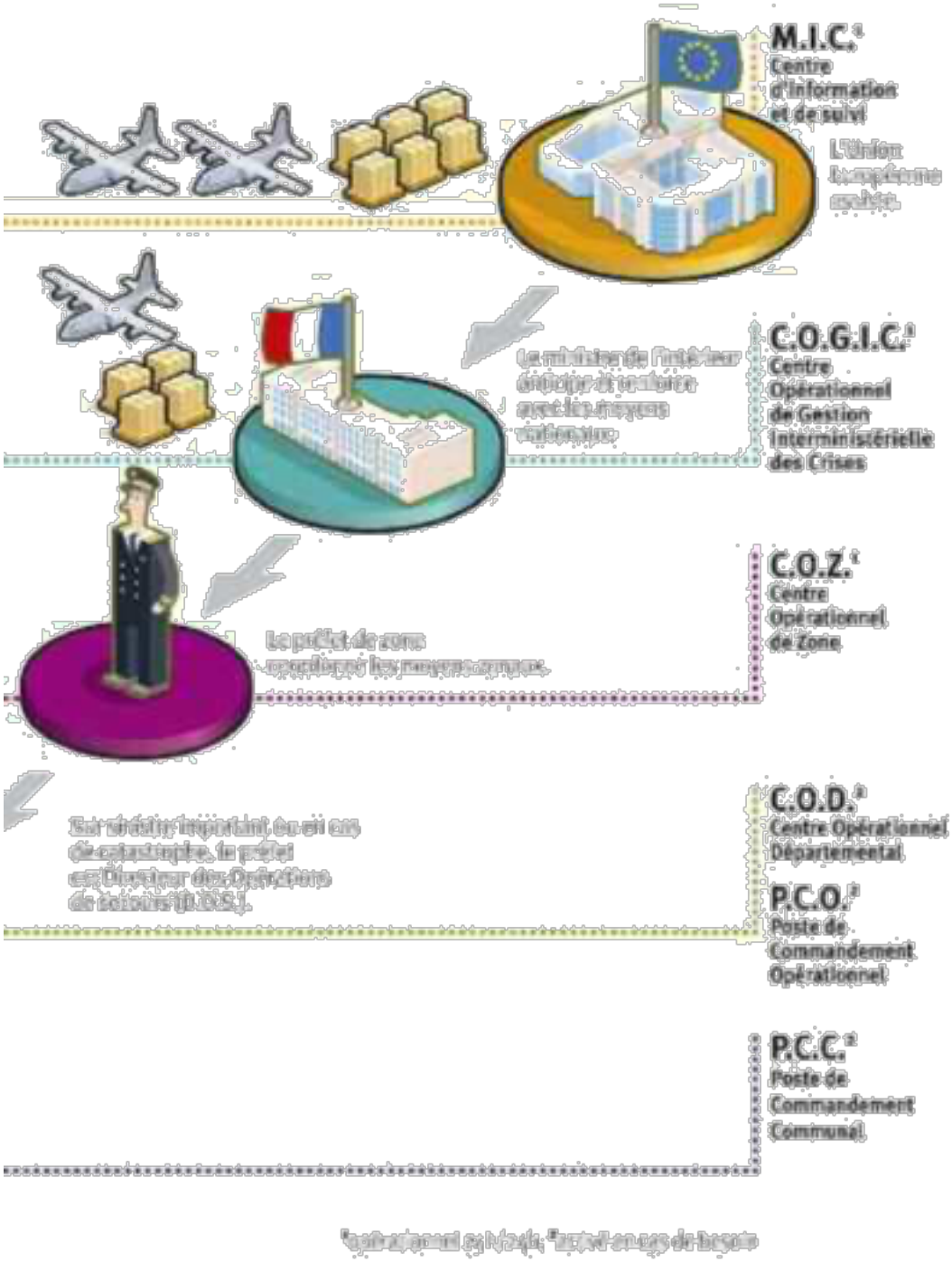
Carte des zones de défense



Certaines communes soumises à des risques majeurs localisés ont l'obligation de décliner le plan O.R.SE.C. en élaborant un **Plan Communal de Sauvegarde (P.C.S.).**
La réalisation de ce plan est cependant **fortement conseillée pour toutes les communes**

- pour prendre en compte les missions qui relèvent de leur compétence dans le cadre O.R.SE.C. :
  - l'alerte et l'information des populations,
  - l'appui aux services de secours,
  - le soutiendes populations (hébergement,ravitaillement…),
  - l'information des autorités…
- pour faire face à des situations d'urgence plus courantes nécessitant la mobilisation de moyens communaux et impliquant le maire comme Directeur des Opérations de Secours.


Européen
National
UIISC
ESOL
Zonal
→ ORSEC de zone
Départemental
→ ORSEC départemental
Communal
→ Plan Communal de Sauvegarde


M.I.C.[5]
Centre d'information et de suivi
L'Union la supérieure exclue.
C.O.G.I.C.[3]
Centre Opérationnel de Gestion Interministérielle des Crises
C.O.Z.[4]
Centre Opérationnel de Zone
C.O.D.[2]
Centre Opérationnel Départemental
P.C.O.[1]
Poste de Commandement Opérationnel
P.C.C.[1]
Poste de Commandement Communal

Principes et organisation du dispositif opérationnel

Le plan O.R.SE.C. n'est plus un « document figé », c'est une organisation

- **basée sur une analyse des risques** donc adaptée aux risques prévisibles recensés ;
- **permanente**, elle ne se « déclenche plus », elle s'appuie sur les procéduresde **vigilance**, veille permanente de certains risques (intempéries, inondations, risques sanitaires…) ;
- **progressive**, déployée selon l'**ampleur** des événements,elle **monte en puissance** dans la continuité de la réponse courante des premiers intervenants de sécurité civile en mobilisant d'autres acteurs ;
- **adaptable**, le schéma général de réaction est suffisamment **souple** pour s'adapter à toutes les situations même celles non prévues ;
- **rôdée par des entraînements et des exercices réguliers ;**
- **en évolution permanente,** chaque mise en œuvre ou exercice doit faire l'objet **d'un retour d'expérience**.

Le dispositif O.R.SE.C. se compose

- **de dispositions générales** définissant l'organisation de base capable de s'adapter à tout type de situation
- **de dispositions spécifiques** propres à certains risques particuliers préalablement identifiés.

Les dispositions générales

Véritable colonnevertébrale du dispositif, elles organisent :

au niveau départemental

- **le fonctionnement de la chaîne de commandement,**
- **la veille,** notamment la prise en compte des procédures de vigilance (météo, crue…)
- **l'alerte en toutes circonstances des acteurs** O.R.SE.C.,
- **l'alerte et l'information des populations,**
- **la communication,**
- **les missions pré-identifiées,** traitant de situations types telles que :
  - le secours à de nombreuses victimes,
  - l'hébergement, le ravitaillement, le soutien des populations sinistrées,
  - la prise en charge des graves perturbations des réseaux de téléphonie, d'électricité, d'eau…
  - …

au niveau zonal

- **le fonctionnementde la chaîne** de suivi et de coordinationdes opérations,
- **la synthèse des dispositifs** de vigilance et de surveillance,
- **l'organisation des renforts** au profit d'un ou de plusieurs départements,
- **le recensement des moyens rares,**
- **les modalités de coordination** de l'information lorsque l'événement présente des incidences communes en mer et à terre.

au niveau maritime

- **le fonctionnement** de la chaîne de direction des opérations,
- **les modalités de coordination et d'échange** d'informations avec les préfets des départements et des zones de défense des littoraux,
- **les missions pré-identifiées,** traitant de situations types telles que :
  - le secours à de nombreuses victimes,
  - la protection des biens et de l'environnement,
- **les modalités de mise en œuvre** des accords internationaux de coopération opérationnelle.

Pour faire face à des risques particuliers

Les dispositions spécifiques

Elles complétent les dispositions générales, en préparant les réponses adaptées à certainsrisques.

Les risques pouvant faire l'objet de dispositions spécifiques sont notamment :

- les **risques naturels** : inondations, avalanches, cyclones, séismes…
- les **risques technologiques localisés :** voir tableau ci-après
- les autres **risques technologiques**: transport de matières dangereuses, de matières radioactives, accident de transport collectif …
- **les risques sanitaires :** pandémies, canicules, épizooties…

Ces risques sont identifiés dans le cadre de recensements des risques effectués au niveau départemental, zonal ou maritime.

L'appellation Plan Particulier d'Intervention (P.P.I.) issue de la loi de 1987 est conservée. Les nouvelles versions P.P.I.sont des dispositions spécifiques.

Les P.P.I. sont réalisés pour faire face à un risque, lié à des installations fixes, pouvant avoir des conséquences sur la population. Sont concernées :

- les installations nucléaires - 39 sites,
- les usines chimiques, pétrolières, installations classées dites « Seveso » - 605 installations,
- les stockages souterrains de gaz - 24 sites,
- les « grands barrages » - 99 ouvrages,
- les infrastructures liées au transport des matières dangereuses - 50 sites,
- les laboratoires utilisant des micro-organismes hautement pathogènes - 2 sites.

Le préfet peut également élaborer un P.P.I.pour prendre en compte la situation particulière d'un site même s'il n'atteint pas les seuils définisréglementairement.

Mise au point d'une disposition spécifique

1 Analyse du risque

Connaissance de l'aléa :
les phénomènes possibles, leurs effets, les zones concernées ...

Identification des enjeux :
les communes et populations concernées, les infrastructures et établissements particuliers menacés ...

2 Réponse opérationnelle

Choix des stratégies de protection des populations et des interventions :
confinement ou évacuation...

Décliner la stratégie :
Définition des objectifs et de leur mise en œuvre
Déclinaison des missions
Répartition entre les acteurs

Chaque acteur doit ensuite intégrer dans sa propre organisation les missions qui lui sont confiées.

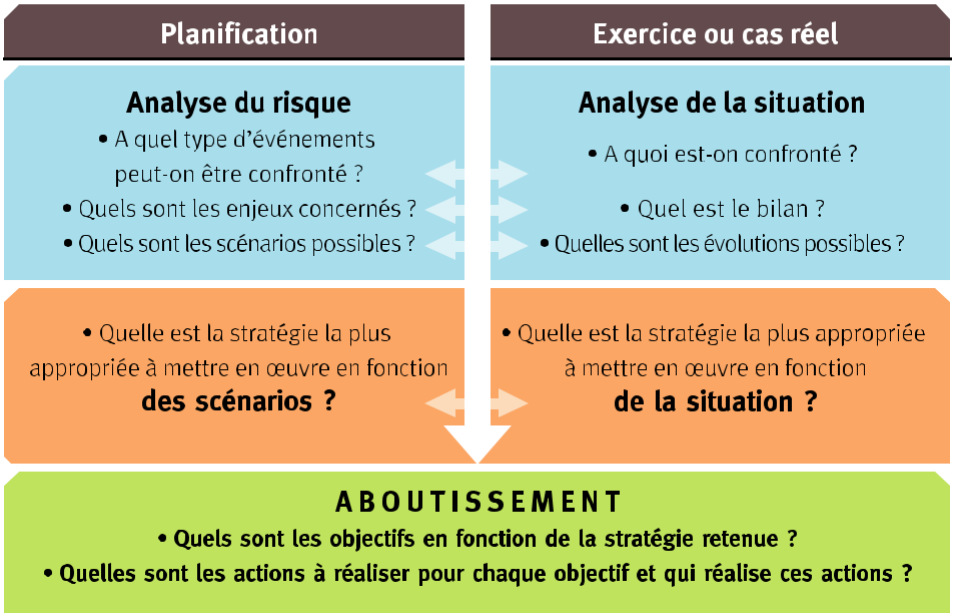
Garantir la pérennité du dispositif : les exercices et le retourd'expérience

La réalisation d'une disposition spécifique est l'occasion pour tous les acteurs impliqués en cas d'événement de **se préparer et de se former ensemble à la gestion opérationnelle.** Elle constitue le premier niveau d'exercice.

Pour que le dispositif **soit opérationnel**, des **formations et des exercices** doivent être organisés régulièrement. **Les exercices** renforcent le niveau d'appropriation des acteurs et les habitudes de travail en commun développées lors la planification.

Cet investissement lors de la préparation se retrouve lors de la gestion d'un événement car le raisonnement utilisé dans les deux cas est identique.

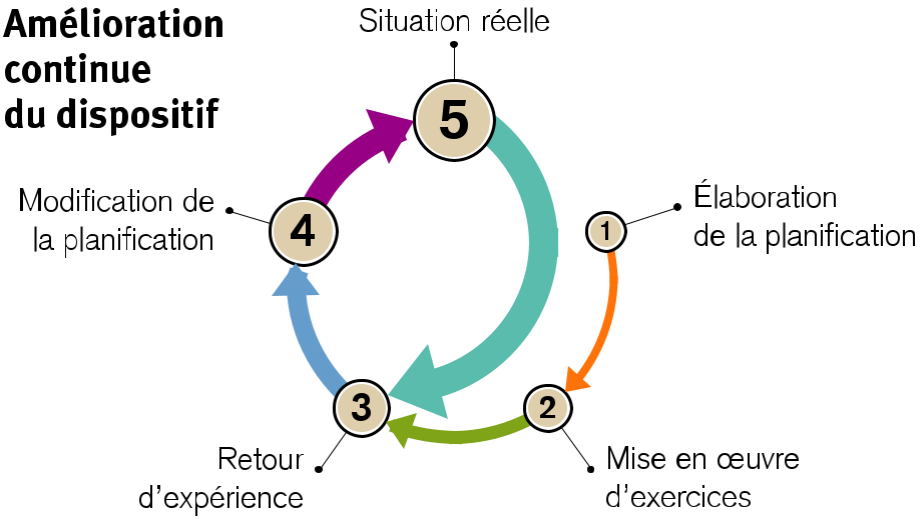
Similitudes des raisonnements entre préparation et réalité



Ainsi, même si
les événements sont rarement conformes aux scénarios envisagés ou joués, les acteurs ont acquis :
• un savoir-faire
• des réflexes
leur permettant de **s'adapter à la situation inédite.**

Chaque mise en œuvre du dispositif O.R.SE.C., (exercice ou d'une situation réelle) doit donner lieu à un retour d'expérience. Les enseignements et le plan d'actions qui en sont issus permettent de faire évoluer le dispositif et de garantir la mobilisation des acteurs.

Amélioration continue du dispositif



En savoir plus :

Loi n°2004-811 du 13 août 2004 de modernisation de la sécurité civile (articles 13 à 29)
Site Internet : www.interieur.gouv.fr/rubrique sécurité civile

Direction de la Sécurité Civile

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR
DE L'OUTRE-MER
ET DES COLLECTIVITÉS
TERRITORIALES

Pour faire face à une situation difficile il faut :

Anticiper pour réagir

Se préparer pour agir

Tels sont les éléments clés pour être prêt

Les pouvoirs publics se préparent au travers de l'

Organisation de la Réponse de SEcurité Civile

Mais la sécurité civile est l'affaire de tous.

Et vous, êtes-vous prêt ?

Connaissez-vous :
- les risques auxquels vous pouvez être confrontés ?
- vos interlocuteurs en cas de situation d'urgence ?
- votre rôle dans le dispositif O.R.SE.C. ?

Avez-vous :
- préparé votre organisation ?
- informé, formé votre personnel, vos administrés, votre famille ?
- réalisé des exercices ?

Réalisation : www.navis-print.com - Conception graphique : IKONEO (Tél.: 01 49 73 30 54) - Photos : IRMA - Sébastien Gominet - DSC - Joachim Bertrand

ANNEXE 4

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET DE LA
ZONE DE DÉFENSE
ET DE SÉCURITÉ EST

La Préfecture de la Zone de Défense et de Sécurité Est

Espace Riberpray 10 rue Belle Isle 57036 METZ
Tél : 03.87.16.10.68

Août 2017

ÉDITO

Créées en 1959, les zones de défense et de sécurité sont des échelons administratifs spécialisés dans l'organisation de la sécurité nationale et de la défense civile et économique.

La préfecture de zone travaille à la mise en cohérence et à la coordination des politiques de sécurité de l'État. Elle intervient en complément de l'action des préfectures de département, si elles le jugent nécessaire, et coordonne leurs actions dès lors qu'un dossier ou un incident dépasse le cadre du département.

A ce titre, elle doit faire face à des exigences fortes, afin :

- de mieux préparer et organiser les réponses de l'État dans les domaines de la sécurité : sécurité intérieure, sécurité civile et sécurité économique,
- d'assurer l'efficacité opérationnelle des services de lutte contre la délinquance, au travers notamment de la gestion du parc automobile, de l'immobilier et de l'armement des services de police et de gendarmerie,
- de coordonner et renforcer les moyens de la sécurité civile dans les départements,
- d'assurer la fiabilité, la protection et la continuité de l'informatique et des transmissions du ministère de l'intérieur.

Son positionnement géographique favorise par ailleurs le développement de coopérations transfrontalières avec la Belgique, le Luxembourg, l'Allemagne et la Suisse, dans les domaines de la prévention de la délinquance et de la gestion de crises notamment.

Elle coexiste avec l'organisation militaire qui désigne un officier général de zone de défense, lequel coordonne la mise en place de moyens militaires, dans certains cas, à disposition des préfets de département.

Un millier d'agents œuvre au sein des services qui composent la préfecture de zone. Leurs missions vous sont présentées dans cette brochure.

Jean-Luc MARX
Préfet de la zone de défense et de sécurité Est
Préfet de la région Grand Est
Préfet du Bas-Rhin

POURQUOI UNE ZONE DE DÉFENSE ET DE SÉCURITÉ ?

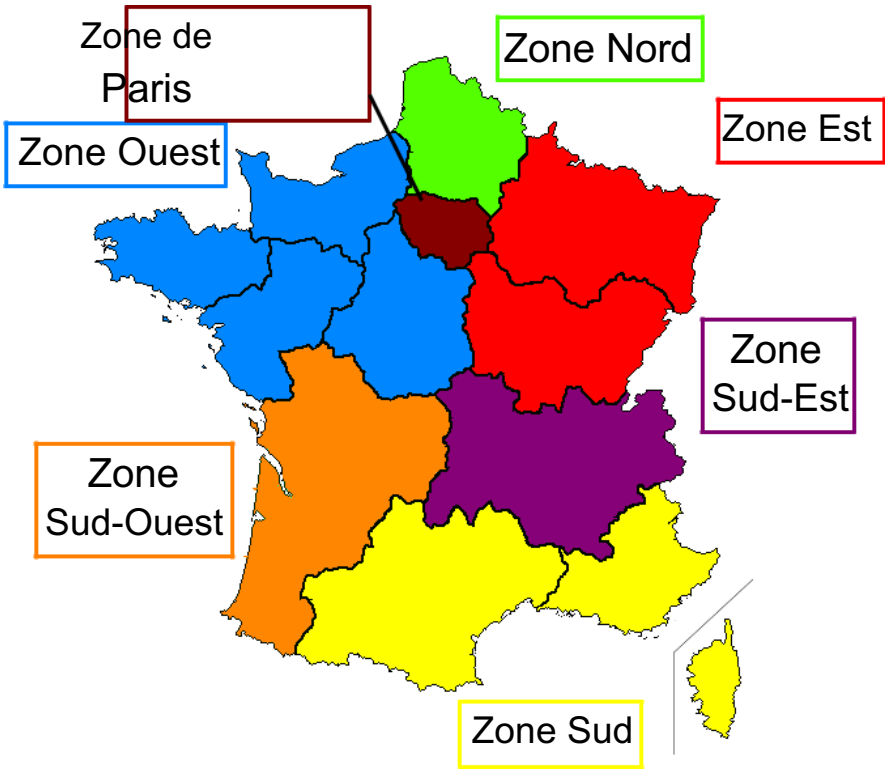
Un échelon intermédiaire entre le niveau central et les préfectures de région et de département

L'État s'organise en trois échelons administratifs :
- les départements,
- les régions,
- les zones de défense depuis 1959.

Les décrets n°2010-224 et n°2010-225 du 4 mars 2010 précisent et développent les compétences des préfectures de zone de défense et de sécurité.

Il existe 7 préfectures de zone de défense et de sécurité en métropole.

A leur tête :
- un préfet de zone de défense et de sécurité (préfet de région et préfet de département),
- assisté depuis 1993, d'un préfet délégué pour la défense et la sécurité en charge de la direction des services de la zone de défense et de sécurité.



Leur siège :
- Strasbourg (Est),*
- Lille (Nord),
- Rennes (Ouest),
- Lyon (Sud-Est),
- Bordeaux (Sud-Ouest),
- Marseille (Sud),
- Paris (Ile-de-France).

Un échelon créé pour renforcer les capacités de l'État à assurer la sécurité

La zone dispose de compétences destinées à faciliter la gestion d'un événement ou d'une situation de crise dépassant le cadre départemental.

Cadre géographique commun, coordonnant les efforts civils et militaires, ses compétences sont :
- l'élaboration de mesures non militaires de défense et la coopération avec l'autorité militaire,
- la coordination des moyens de sécurité civile dans la zone, notamment grâce à un réseau de diffusion et de coordination de l'information,
- l'administration des moyens de la police et de la gendarmerie nationales et des transmissions du ministère de l'Intérieur.

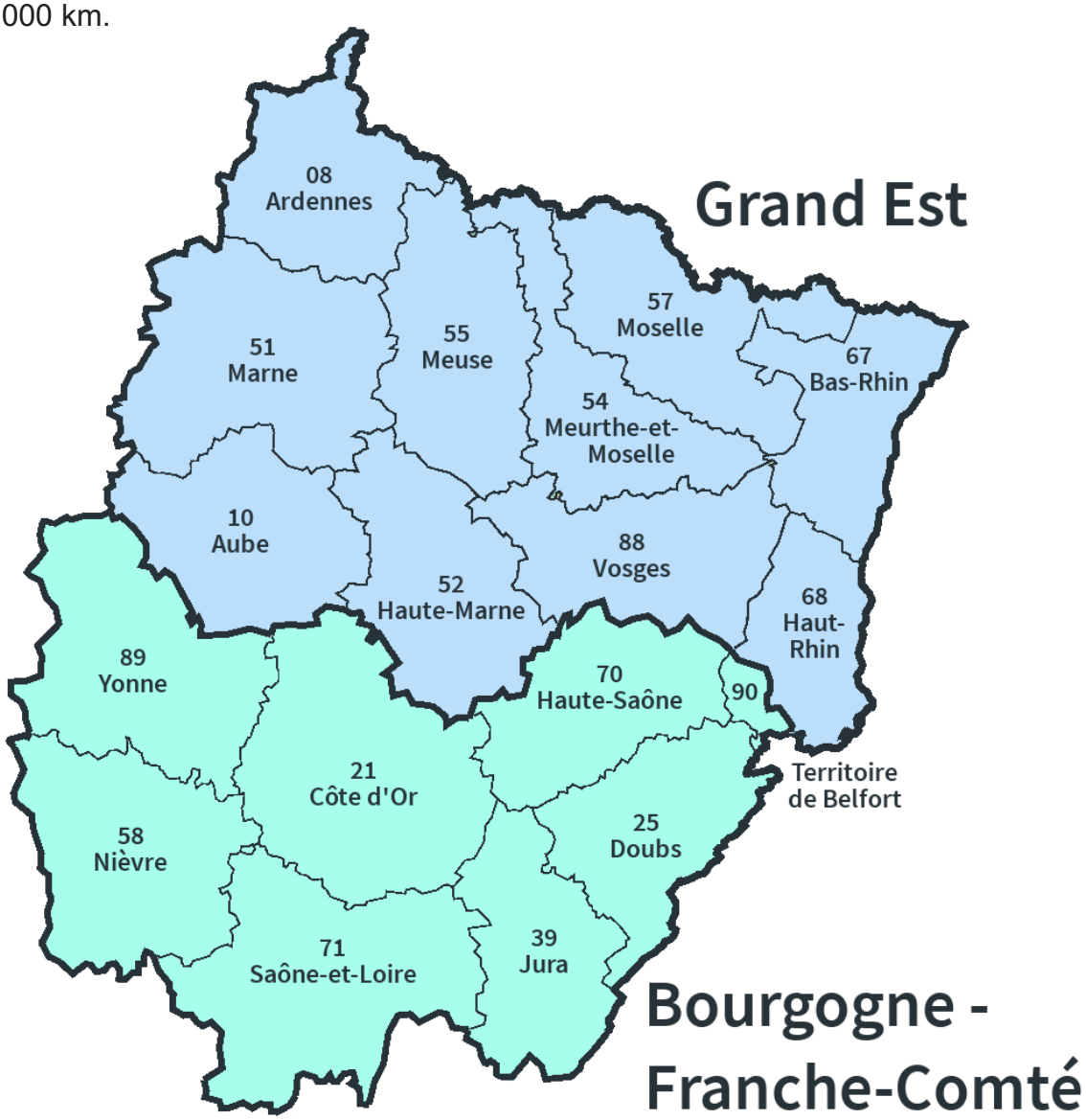
*La configuration géographique de la zone Est est singulière. Le préfet de la zone de défense et de sécurité Est est le préfet de la

région Grand Est, préfet du Bas-Rhin, à Strasbourg. Le préfet délégué pour la défense et la sécurité ainsi que tous les services de la préfecture de la zone Est sont à Metz

ZOOM SUR LA ZONE DE DÉFENSE ET DE SÉCURITÉ EST

La zone de défense et de sécurité Est occupe tout le grand quart Nord-Est de la France. Par rapport aux autres zones, elle se situe au 3ème rang en termes de superficie et de population.

Elle partage ses frontières avec 4 autres pays (Belgique, Luxembourg, Allemagne et Suisse) sur près de 1 000 km.



La Zone Est, c'est...

- 2 grandes régions comprenant 18 départements :
  Grand Est,
  Bourgogne - Franche-Comté.
- 105 217 km², soit 20% de la superficie totale de la France.
- 8,35 millions d'habitants, dont 60% en zone urbaine.
- 9 018 communes, dont 11 agglomérations de plus de 100 000 habitants.
- 4 centrales nucléaires et près de 100 sites industriels et miniers.
- des institutions européennes situées à Strasbourg.

L'ORGANISATION DE LA PRÉFECTURE DE ZONE

Pour toutes les missions concourant à la sécurité intérieure, à la sécurité civile, à la sécurité économique et à la défense à caractère non militaire, le préfet de zone s'appuie sur la **préfète déléguée pour la défense et la sécurité**.

L'état-major interministériel de zone (EMIZ), le secrétariat général pour l'administration du ministère de l'intérieur (SGAMI) et le cabinet sont placés sous son autorité.

En tout, un millier d'agents œuvre au quotidien pour apporter tout le soutien nécessaire aux préfectures de département et aux services de police et de gendarmerie.

Sylvie HOUSPIC
Préfète déléguée pour la défense et la sécurité

Préfet de zone de défense et de sécurité Est

Préfète déléguée pour la défense et la sécurité

CABINET

- Sécurité intérieure
- Gestion des crises routières
- Coopération transfrontalière
- Emploi des forces mobiles
- Dossiers transversaux
- Affaires réservées
- Communication
- Courrier

EMIZ

- Veille opérationnelle permanente (COZ H24)
- Planification et gestion de crises
- Défense non militaire
- Sécurité civile
- Sécurité économique

SGAMI

- Fonction soutien de la police et de la gendarmerie nationales
- Finances
- Ressources humaines
- Équipement et logistique
- Immobilier
- Systèmes d'information et de communication
- Contrôle de gestion

Le cabinet

Le **cabinet** est chargé d'assister la préfète déléguée pour la défense et la sécurité sur l'ensemble de ses compétences, de suivre les dossiers transversaux. Dirigé par un commissaire de police, il est composé d'un pôle cabinet et d'un pôle sécurité intérieure créé en juillet 2017 par le regroupement des cellules opérationnelles compétentes en la matière (mission police, ex-CRICR, cellule sécurité intérieure).

Parmi les attributions du pôle cabinet, on retrouve :

- La gestion des dossiers transversaux,
- Le suivi des affaires réservées,
- La communication de la préfecture de zone (site intranet, lettre interne…),
- l'organisation des cérémonies et la gestion des affaires protocolaires,
- la mise à jour des arrêtés de délégation de signature,
- la répartition et le suivi du budget de la réserve civile des services de police,
- le traitement du courrier de l'ensemble des services de la préfecture de zone et des services présents sur le site de Riberpray (CNAPS, IGPN, Météo France…),
- la gestion des accès et la sécurisation du site de Riberpray et la gestion du poste de garde.

Cérémonie à la mémoire des policiers morts pour la France
le 9 mai 2017

Le **pôle sécurité intérieure** regroupe les cellules chargées de la sécurité intérieure, de la gestion de crise routière et de la coopération internationale, ainsi que l'unité zonale de coordination des forces mobiles.

La cellule sécurité intérieure est chargée de la mise à jour, du suivi et de la mise en œuvre des plans zonaux PIRATE, du suivi de la mise en œuvre du plan Vigipirate, du suivi et de la gestion des réquisitions des forces de 3° catégorie dans le cadre du plan Vigipirate (dispositif Sentinelle) et des mesures liées à l'état d'urgence, du suivi des problématiques de radicalisation et de l'organisation des réunions zonales de sécurité.

La cellule gestion de crise routière, composée de fonctionnaires de police et de militaires de la gendarmerie, vise à garantir, en permanence (astreinte H 24), l'information de l'autorité préfectorale zonale et la coordination des mesures de gestion du trafic. Elle a en charge la planification, la coordination et le suivi des opérations zonales de sécurité routière. Sa compétence couvre 4.000 kilomètres au titre du réseau routier national (autoroutes et routes nationales).

Partageant ses frontières avec 4 pays (Belgique, Grand-Duché de Luxembourg, Allemagne et Suisse), la zone de défense et sécurité Est est particulièrement sollicitée sur des problématiques de coopération transfrontalière. La cellule coopération internationale est, d'une part, très impliquée dans le suivi ou la coordination des actions résultant des différents accords qui prévoient entre autres, la mise en place de centres de coopération policière et douanière (CCPD) et une coopération directe entre unités de police, de gendarmerie et de douane implantées en zone frontalière. D'autre part, elle participe à un certain nombre de groupes de travail thématiques, tant dans le cadre de la Grande Région (prévention de la criminalité, coopération policière, sécurité routière) qu'en application de l'article 23.2 de l'Accord de Mondorf (lutte contre les atteintes à l'environnement, sécurité routière, maintien de l'ordre).

L'unité zonale de coordination des forces mobiles (UZCFM) est en charge de la coordination zonale de l'emploi des 33 unités de forces mobiles implantées sur la zone Est (22 escadrons de gendarmerie mobile et 11 compagnies républicaines de sécurité). Elle a pour mission de répondre aux demandes de concours de forces mobiles émanant des préfets de département à des fins de maintien de l'ordre ou de sécurisation générale. A cette fin, elle centralise les demandes émanant des 18 préfectures de la zone EST, les étudie en liaison avec les services zonaux de la gendarmerie et des CRS et l'UCFM à Paris et rédige les télégrammes de décisions quant à la mise à disposition ou non, des unités de forces mobiles. Elle joue également un rôle de conseiller technique, tant pour le Préfet délégué que pour les services des cabinets des Préfectures de la Zone, et assure une permanence opérationnelle 24h sur 24, 7 jours sur 7.

L'État-major interministériel de zone (EMIZ)

L'état-major interministériel de zone (EMIZ) est une structure interministérielle constituée de cadres et agents de différentes origines (sapeurs-pompiers, militaires des formations militaires de la sécurité civile, police, gendarmerie, commissariat à l'armée de terre, douanes).

En liaison avec les préfets de département, l'EMIZ prépare et met en œuvre les mesures concourant à la sécurité nationale.

Ses activités portent essentiellement sur la planification dans les domaines de la sécurité civile et de la sécurité économique, la préparation, la veille, le suivi et la gestion des crises, réparties en 3 pôles :

- le pôle anticipation et préparation des crises réunit les missions dédiées à la prévention des crises en relation avec l'ensemble des services concernés. Dans le domaine de la sécurité civile, il organise la formation des sapeurs-pompiers, suit et renforce les moyens des SDIS, coordonne la planification. Sur le plan économique, il traite de la continuité économique des entreprises et des infrastructures. Il anime également la politique zonale de sécurité des activités d'importance vitale face aux risques et menaces.
- le pôle opérations et gestion des crises couvre la préparation et la veille opérationnelle. Il établit les procédures d'intervention et conduit les opérations en cas d'exercice ou de crise. Il coordonne le réseau d'intervenants et mobilise les moyens en renfort. Il organise et maintient la vigilance. C'est au sein de ce pôle que l'on trouve le centre opérationnel de zone (COZ).
- le pôle soutien administratif assure les missions d'administration générale, de coopération transfrontalière, d'animation des réseaux et de communication. Il apporte son appui technique en matière de gestion et de maintenance des systèmes d'information et de communication et son soutien administratif aux deux autres pôles.

Le secrétariat général pour l'administration du ministère de l'intérieur (SGAMI)

Le **secrétariat général pour l'administration du ministère de l'intérieur** est chargé de la fonction soutien des services de police, des unités de gendarmerie et, pour certaines tâches, des préfectures. Il est compétent en matière financière, de ressources humaines, de logistique, d'immobilier et de système d'information et de communication.

Il comprend 5 directions :

- la direction de l'administration générale et des finances,
- la direction des ressources humaines,
- la direction de l'équipement et de la logistique,
- la direction de l'immobilier,
- la direction des systèmes d'information et de communication,
- et une cellule de conseil en gestion.

La direction de l'administration générale et des finances

La direction de l'administration générale et des finances est composée de 4 bureaux :

- le bureau des budgets, chargé de la préparation budgétaire, de la répartition des crédits, du suivi de l'exécution et de l'analyse budgétaire ;
- le bureau de la commande publique, chargé de la préparation, de la passation, de l'exécution et du suivi des marchés publics ;
- le centre de services partagés (plate-forme chorus) composé du bureau des dépenses courantes, du bureau des compétences transverses et du bureau des dépenses spécifiques, chargé de l'exécution des dépenses et des recettes, ainsi que de leur suivi et de leur compte-rendu d'exécution ;
- le bureau du contentieux et de la veille juridique, chargé notamment de la protection fonctionnelle des agents et du contentieux juridictionnel et statutaire des personnels.

La direction des ressources humaines

La gestion des carrières est assurée par ce service, du recrutement jusqu'à la retraite. Elle décline la politique des ressources humaines du ministère de l'intérieur et les instructions de la direction des ressources et des compétences de la police nationale.

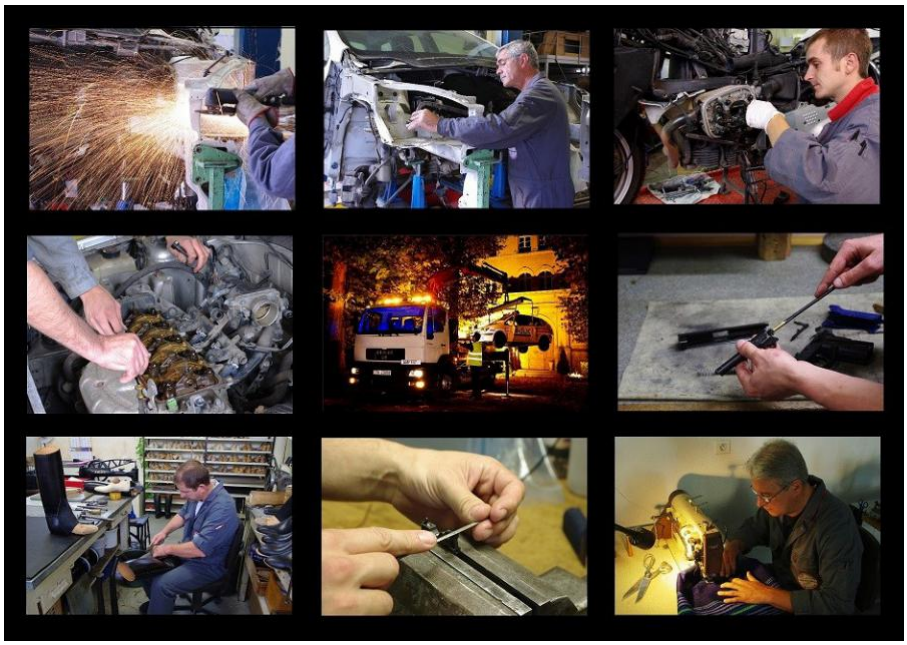
La direction des ressources humaines est composée :

- de la mission accompagnement au changement et appui au pilotage, chargée de préparer et participer à la conduite et à l'accompagnement des démarches de changement,
- du service des personnels, composé du bureau du recrutement, du bureau des personnels actifs, du bureau des personnels administratifs et du bureau des personnels techniques et spécialisés, assurant la gestion RH de 14 000 agents,
- du pôle des affaires médicales et des relations sociales, chargé notamment d'assurer la protection statuaire accordée aux personnels en matière de maladie et accident de service,
- du pôle d'expertise et de services, chargé de la paye de l'ensemble des fonctionnaires du périmètre du ministère de l'intérieur affectés dans la zone de défense et de sécurité(19 000 payes en portefeuille)

La direction de l'équipement et de la logistique

La direction de l'équipement et de la logistique est composée :

- du bureau de la maintenance automobile, chargé du maintien en condition opérationnelle du parc automobile de la police et de la gendarmerie nationales, (8 000 véhicules), ainsi que des moyens nautiques de cette dernière ;
- du bureau de l'administration et des moyens généraux, chargé notamment de la mise à disposition de fournitures et de matériels au bénéfice de la police et de la gendarmerie nationales,
- du bureau de l'armement et des munitions, chargé du maintien en condition opérationnelle des équipements d'armement, de l'approvisionnement, du stockage et de la distribution de ces matériels



La direction de l’immobilier

La direction de l'immobilier est composée :

- du bureau de l’administration immobilière, chargé de l’exécution et du suivi des marchés publics d’études, d’ingénierie et de conduite des opérations immobilières de la police et de la gendarmerie nationales ;
- du bureau des opérations et de la maintenance immobilière, chargé de la maîtrise d’ouvrage, et selon le degré de technicité de la maîtrise d’œuvre, des opérations immobilières de constructions et réhabilitations au bénéfice de la police et de la gendarmerie nationales, de la maintenance des bâtiments police (hors travaux d’aménagement et travaux d’entretien) et de la maintenance spécialisée pour la gendarmerie, de la conduite de certaines opérations immobilières de sécurité civile ou de préfectures.

Le nouvel hôtel de police de Longwy-Mont-St-Martin, ouvert le 20 décembre 2016 : une belle réalisation pilotée par la direction de l'immobilier du SGAMI Est

- du bureau des études et du suivi des opérations sensibles, chargé du traitement de toutes les études préalables d’opportunité et de faisabilité et du suivi des opérations sensibles et des montages d’opérations diverses.

Le parc immobilier sous gestion SGAMI est constitué de 1 124 bâtiments (2,4 millions de m²).

La direction des systèmes d’information et de communication

La direction des systèmes d'information et de communication a pour missions de :

- déployer et maintenir en fonctionnement les systèmes d'information en veillant à la continuité gouvernementale (préfectures, police, sécurité civile,...),
- piloter les grands programmes nationaux en zone Est,
- moderniser les centres d'information et de commandement de la police,
- gérer les équipements téléphoniques et de réseau informatique,
- optimiser le réseau radio numérique ACROPOL de la police, ou celui des pompiers, ANTARES.

A cela s'ajoutent des missions nationales, telles que l'élaboration des règles nationales d'ingénierie en matière de sécurité informatique, l'exploitation et la supervision des plates formes internet, l'organisation de l'observatoire zonal interministériel de la sécurité informatique, le développement et l'exploitation des logiciels (gestion de crises, cartographie, remontées police, délinquance, accidentologie), l'hébergement national sécurisé d'applications web intranet et internet et des missions zonales avec, par exemple, le déploiement d'outils de gestion électronique des documents, l'audit réseau et de sécurité en relation avec les services SIC de toutes les entités.

Pour mener à bien ces missions, la DSIC est composée :

- du pôle défense et sécurité des systèmes d'information,
- du département du pilotage, de la coordination et des moyens,
- du département des systèmes d'information et du soutien informatique,
- du département des réseaux mobiles,
- du département des réseaux fixes.

Sont également rattachés au SGAMI :

La cellule de conseil en gestion

La cellule de conseil en gestion est chargée du pilotage de la performance, du contrôle de gestion, du contrôle interne financier, ainsi que de la coordination de la veille juridique, technique et managériale.

La délégation régionale de Dijon

La délégation régionale de Dijon est chargée d'assurer la mise en œuvre des missions qui lui sont confiées dans le cadre des orientations définies au niveau du SGAMI à Metz.

Elle est la plus importante des 28 implantations du SGAMI, dont certaines regroupent plusieurs activités, dans les cinq régions de la zone Est, au plus près des services opérationnels.

L'organisation de la délégation régionale découle des directions du SGAMI.

La répartition des attributions entre les sites de Metz et Dijon est, selon les domaines, géographique ou fonctionnelle.

On y retrouve :

- le bureau des affaires générales,
- le bureau des ressources humaines,
- le bureau de la logistique,
- le bureau des affaires immobilières.

Le service médical statuaire et de contrôle de la police nationale

Le service médical de la police nationale est chargé de la médecine statutaire.

Il a pour missions :

- de veiller à l'aptitude de l'ensemble des personnels de la police nationale à exercer leurs fonctions,
- de rendre un avis sur l'aptitude à la titularisation et à la reprise de service,
- d'assurer la fonction de conseil technique auprès du préfet délégué pour la défense et la sécurité.

Ces missions sont assurées par 2 médecins inspecteurs régionaux, le premier basé à Metz, le second à Dijon. De plus, ils s'appuient sur un réseau de 20 personnels de santé implantés sur 12 sites pour être au plus près des fonctionnaires.

ANNEXE 5

PROTECTION CIVILE
AIDER · SECOURIR · FORMER
| BAS-RHIN

PSC 1 Prévention et Secours Civique de niveau 1

Objectifs :

Faire acquérir à toute personne, les capacités nécessaires pour concourir par son comportement à la sécurité civile.

Elle sera capable d'exécuter une action citoyenne d'assistance à personne en réalisant les gestes élémentaires de secours. En particulier, elle doit être capable :

- **D'assurer une protection immédiate, adaptée et permanente pour elle-même, la victime et les autres personnes des dangers environnants**
- **D'assurer la transmission de l'alerte au service le plus adapté**
- **D'assurer immédiatement les premiers gestes de secours face à :***
  - **Une obstruction des voies aériennes**
  - **Un saignement abondant**
  - **Une personne inconsciente qui respire**
  - **Une personne en arrêt cardiaque**
  - **Un malaise**
  - **Un traumatisme**

Cette formation permet, en 1 journée, d'apprendre les principaux gestes de secours à effectuer face aux accidents de la vie courante.

Contenu de la formation :

- **Accueil et présentation de la formation et des participants**
- **Malaise, alerte des secours**
- **Plaies protection**
- **Brûlures**
- **Traumatismes**
- **Hémorragie externe**
- **Obstruction des voies aériennes**
- **Perte de connaissance, dégagement d'urgence**
- **Arrêt cardiaque**
- **Alerte aux populations et protection du citoyen**
- **Evaluation et clôture de la formation**

Méthodes pédagogiques :

- **Remue-méninge pédagogique**
- **L'étude de cas d'amorçage**
- **L'exposé**
- **Les démonstrations pratiques**
- **L'atelier d'apprentissage du geste et du matériel**
- **Le cas concret**

Conditions de validation :

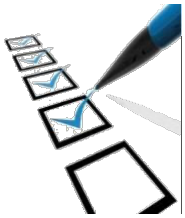
Le certificat de compétence de citoyen de sécurité civile est délivré aux personnes qui ont participé à toutes les phases de la formation, réalisé tous les gestes de premier secours lors des phases d'apprentissage pratique et participé une fois au moins, comme sauveteur à une activité d'application.

Participants
1 formateur pour 10 apprenants

Durée
7 heures

Coût
67€ / pers
Prix de groupe
Nous consulter

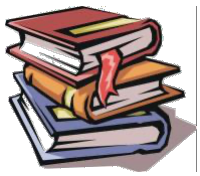
Lieu de formation
Dans nos locaux ou dans les vôtre



Pré-requis
Âge minimum 10 ans

Formation continue
Non obligatoire

Qualifications des formateurs
Formateur SST PAE PSC PAE PS



Textes officiels
Arrêté du 24/07/2011
Recommandations PSC 1 DGSCGC
RIFC PSC1 FNPC

ANNEXE 6

Filière des systèmes d'information et de communication

Ministre de l'Intérieur

Ingénieur des SIC

Les ingénieurs des systèmes d'information et de communication sont classés dans un corps de la **catégorie A** des fonctionnaires de l'État.
Les ingénieurs des systèmes d'information et de communication concourent à des fonctions de conception, de mise en œuvre, d'expertise ou de contrôle dans les services chargés de définir et d'appliquer la politique du ministère de l'Intérieur en matière de systèmes d'information et de communication. Ils peuvent aussi être en charge de la gestion ou du pilotage de ces services. Ils assurent l'encadrement des agents placés sous leur autorité.

Plus de renseignements

Technicien des SIC

Les techniciens des systèmes d'information et de communication sont classés dans un corps de la **catégorie B** des fonctionnaires de l'État. Les techniciens des systèmes d'information et de communication sont chargés de fonctions requérant des compétences techniques particulières, de contrôle, d'application et d'études dans le domaine des systèmes d'information et de communication, d'exploitation et de production ainsi que de fonctions d'installation, de gestion et de maintien en condition opérationnelle des matériels et logiciels nécessaires aux systèmes d'information et de communication. Ils établissent les documentations techniques s'y rapportant. Ils peuvent également être chargés de fonctions d'encadrement.

Plus de renseignements

Agence nationale de la sécurité des systèmes d'information

-

https://www.ssi.gouv.fr/recrutement/nos-offres-demploi/

https://www.sengager.fr/decouvrez-l-armee-de-terre/nos-actualites/les-sic-dans-larmee-de-terre-cest-quoi