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 une solution VOIP et de Messagerie Electronique - Superviser les serveurs et équipements critique et évaluer l'incidence de la VoIP sur le réseau. - 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 stephane.beteta@ecp-apprentissage.fr gabriel.beteta@ecp-apprentissage.fr

Lancement : 23/01/2026 – Fin : 17/04/2026

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

AP4

SECURITE CIVILE

SÉCURITÉ CIVILE

Date limite de réponse : Mercredi 25 Février 2026

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.

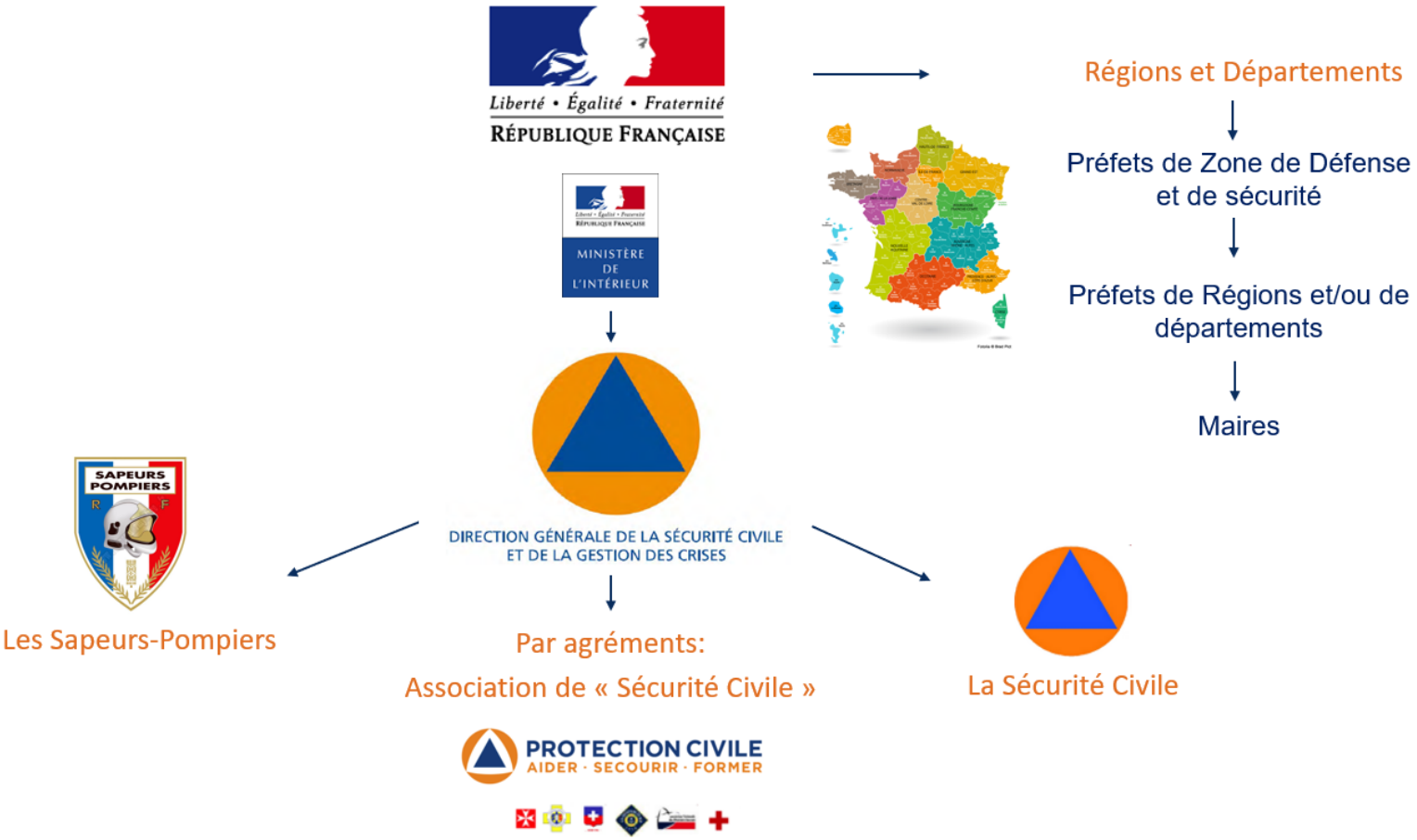
A ce titre, il est, sur le territoire de la République, responsable de l'ordre public, de la protection des personnes et des biens ainsi que de la sauvegarde des installations et ressources d'intérêt général.

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



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 :

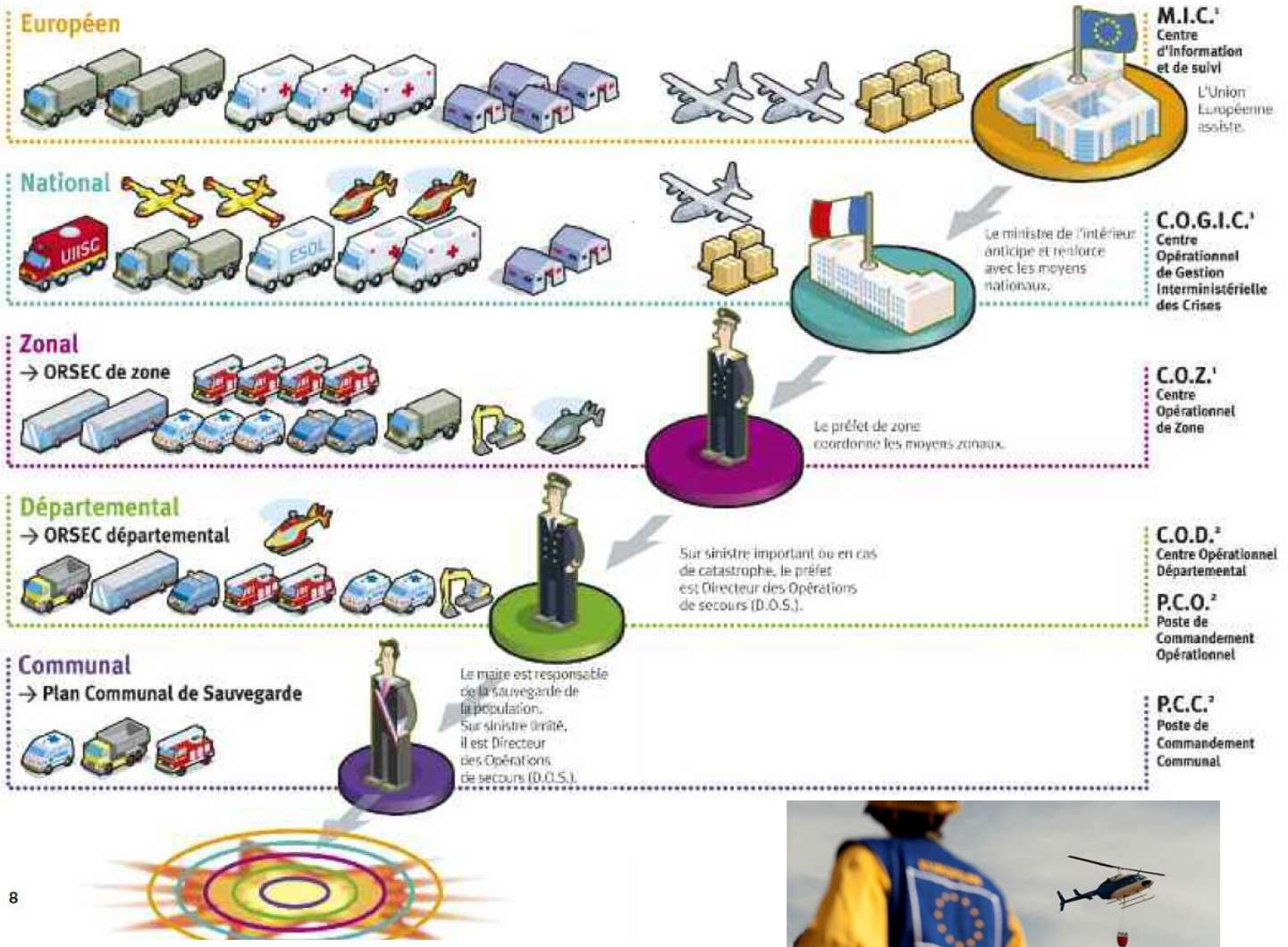
- L'Inspection de la Défense et de la Sécurité civiles ;
- La Direction des sapeurs-pompiers ;
- La sous-direction de la planification et de la gestion des crises qui anime le centre opérationnel de gestion interministérielle des crises (COGIC) ;
- La sous-direction des moyens nationaux ;
- Le Cabinet.

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

Elaboré 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 oeuvre 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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFECTURE

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.

Service interministériel de défense et de protection 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

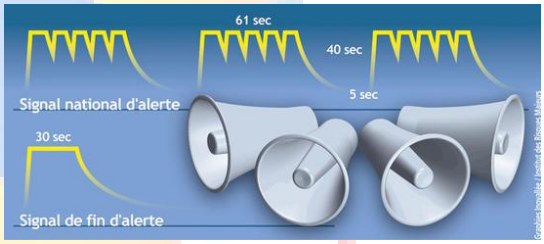
L'alerte aux populations

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
  - Téléphonie analogique, FAX
  - 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 la téléphonie ou 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, la téléphonie IP, 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. »

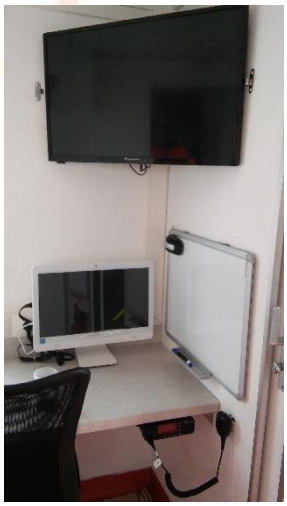
« Nous voulons également évaluer l'impact de la téléphonie sur le réseau et garantir son bon fonctionnement »

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
- Serveur voIP et logiciels de téléphonie IP uniquement en LAN/VPN RW
- L'ensemble des postes de travail sont sur Windows 11 Pro
- 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 téléphonie IpBX et déploiement d'un client softphone
4. Mise en œuvre d'1 serveur de messagerie et déploiement d'un client de messagerie -> Utilisation des comptes de l'Active Directory
5. 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
6. Mise en œuvre d'1 serveur Web avec l'application eBrigade *(archive .zip du logiciel open source fournie)*
7. Mise en œuvre d'une DMZ pour accéder au Serveur WEB E-Brigade (Avec règles de pare-feu adaptées)
8. 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…)
9. 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 (23 Janvier 2026) et de fin de projet (17 Avril 2026)
- 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

- La notation est individuelle.
- Le projet est à réaliser individuellement

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

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) Planning prévisionnel – AP4

S1.	Vendredi 23/01/26 matin :	LANCEMENT DU PROJET + Explications examens
S2.	Vendredi 06/02/26 matin :	Validation des choix de solutions et préparation livrable 1
S3.	Vendredi 20/02/26 matin :	Etudes et préparation de réponses au CdC
	Vendredi 27 Février 2026	LIVRABLE 1
S4.	Vendredi 06/03/26 matin :	ORAL 1
S5.	Vendredi 20/03/26 matin :	Réalisation maquette/expérimentation
S6.	Vendredi 03/04/26 Après-midi :	Réalisation maquette/expérimentation + pré-contrôle dossiers E6
	Lundi 13 Avril 2026	LIVRABLE 2
S7.	Lundi 13/04/26 matin :	BTS BLANC E5 « Oral Professionnel »
S8.	Vendredi 17/04/26 Après-midi :	ORAL 2 - BTS BLANC E6 / Sujets AP4 uniquement
	Du 16 au 25 mai 2026	*EXAMENS BTS SIO*
	Fin mai/début juin 2026 :	*EXAMENS « Oral professionnel et Epreuve technique »*

4.2.2) Planning de préparation des examens E5-E6

Respecter la forme des dossiers et la nomenclature du dossier zip qui sera remis (pour l'instant vous avez la version des documents pour la session 2025). Nous vous donnerons les documents pour la session 2026 dès réception de la circulaire du ministère (février/mars 2026).

23 janvier 2026 :

- Présentation des documents à produire pour l'examen
- Remise d'un dossier .zip avec les éléments (Session 2026 espérée, sinon 2025 pour démarrage)

Mars 2026 :

- Création/modification et diffusion du portefolio sur Internet
- Préparation du dossier E5 « Oral professionnel » :
  - Demander 1 certificat de travail (document scanné/imprimé OK)
  - Compléter le tableau de synthèse des réalisations professionnelles avec l'aide de votre maître d'apprentissage si nécessaire *(selon modèle de l'examen remis).*
  -
- Préparation du dossier E6 « Epreuve technique » :
  - Situation professionnelle 1 *(selon modèle de l'examen remis) + Documentation technique*
  - Situation professionnelle 2 *(selon modèle de l'examen remis) + Documentation technique*

Avril 2026 :

3 avril 2026 :

Pré-contrôle dossiers E5-E6

Première version de vos dossiers E5-E6 sur un dossier OneDrive individuel, partagé avec MM BETETA

13 avril 2026 :

- BTS BLANC E5 « Oral professionnel »

- Prévoir tableau de compétences + diaporama *(10 minutes de présentation, 20 minutes d'entretien)*

17 avril 2026 :

- BTS BLANC E6 « Epreuve technique »

- Prévoir vos VMs complètes de l'AP4 *(30 minutes de préparation, 60 minutes de pratique)*

Fin avril 2026, date à convenir :

- Version finale de vos dossiers à déposer sur Cyclades (dates et format des documents à respecter !)

Nota bene :
Le dépôt des dossiers doit se faire sur Cyclades avant une date limite (à vérifier sur votre espace candidat). Le contrôle de conformité est réalisé via Cyclades. Vous serez convoqué à une autre date pour les épreuves E5 et E6 (début juin certainement). Pour E5 « Oral pro » vous devrez certainement vous déplacer au Lycée René Cassin à Strasbourg. Pour l'épreuve E6 « Epreuve Technique », un jury externe se déplacera dans notre établissement.

Attention aux dates et à la conformité des dossiers (consignes sur Cyclades), en cas de non-conformité, vous ne pourrez subir l'épreuve et le diplôme ne pourra vous être délivré.

Fin Mai/Début Juin 2026 :

- Examens E5 « Oral professionnel » et E6 « Epreuve technique » + Oral d'Anglais

Fin juin / Début juillet 2026 :

- Résultats du BTS sur le site de l'académie de Strasbourg www.ac-strasbourg.fr
- Relevé de notes à télécharger sur Cyclades et conserver précieusement, il n'y a plus d'envoi

papier de vos résultats. https://cyclades.education.gouv.fr/cyccandidat/

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 VENDREDI 27 FEVRIER 2026

- 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 : LE VENDREDI 06 MARS 2026, 8H30

PRESENTATION ORALE : 20 minutes

10 minutes de présentation puis 10 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 LUNDI 13 AVRIL 2026

- 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 technique et peut-être demandée à l'examen « oral pro »

ORAL 2 : LE VENDREDI 17 AVRIL 2026, 08H30

PHASE 1 - PRESENTATION ORALE : 20 minutes

10 minutes de présentation puis 10 minutes de questions / réponses

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 : 30 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.

- La remise en retard des livrables 2 et 3 seront sanctionnés 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, pondéré selon le volume horaire théorique).**

CISCO : S'inscrire/être authentifié avec son adresse électronique personnelle ou réutiliser un compte existant avant de cliquer sur les liens.

P1 : Introduction à la Cybersécurité /rapide 6h
https://www.netacad.com/courses/introduction-to-cybersecurity?courseLang=fr-FR&instance_id=8a0c0dbf-6bfd-4246-bede-8b4a4aef7ea7

P2 : CCNA1 : Présentation des réseaux
https://www.netacad.com/courses/ccna-introduction-networks?courseLang=fr-FR&instance_id=c7b77b94-ba98-4b06-86dd-da50987b3798

P3 : Principes de cybersécurité
https://www.netacad.com/courses/cybersecurity-essentials?courseLang=fr-FR&instance_id=1fd2a67c-d8de-4f78-811f-2ec6689dc817

P4 : CCNA2 : Switching, Routing, and Wireless Essentials (SRWE)
https://www.netacad.com/courses/ccna-switching-routing-wireless-essentials?courseLang=fr-FR&instance_id=4071adba-3b66-495f-bc55-662ffc6934c5

Rapide / ½ journée :

https://secnumacademie.gouv.fr/

SecNumacadémie.gouv.fr
Formez-vous à la sécurité du numérique

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

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.