BULLETIN OFFICIEL DES ARMÉES

Édition Chronologique n° 33 du 4 juillet 2014

PARTIE PERMANENTE
Administration Centrale

Texte 2

DIRECTIVE N° 32/DEF/DGSIC
portant sur la sécurité de l'hébergement des systèmes informatiques au sein du ministère de la défense.

Du *11 mars 2014*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

DIRECTIVE N° 32/DEF/DGSIC portant sur la sécurité de l'hébergement des systèmes informatiques au sein du ministère de la défense.

Du 11 mars 2014

NOR D E F E 1 4 5 0 5 5 8 X

Pièce(s) Jointe(s) :

Quatre annexes.

Classement dans l'édition méthodique : BOEM 161.4

Référence de publication : BOC n° 33 du 4 juillet 2014, texte 2.

SOMMAIRE

3.1.2.1.5. Maintien en condition de sécurité.

3.1.2.1.6. Gestion de configuration et conformité.

3.1.2.1.7. Choix des composants.

3.1.2.1.8. Cartographie et sondes.

3.1.2.2. Règles spécifique à l'hébergement mutualisé (virtualisation).

3.1.2.2.1. Configuration.

3.1.2.2.2. Administration de la couche virtualisation.

3.1.2.2.3. Réduction de la surface d’exposition.

3.1.2.2.4. Cloisonnement des systèmes clients.

3.1.2.2.5. Certification/qualification.

3.1.3. Services d'hébergement.

3.1.3.1. Service de maintien en conditions de sécurité.

3.1.3.2. Antivirus.

3.1.3.3. Sauvegarde et restauration.

3.2. Règles applicables à l'exploitation des systèmes informatiques clients par les opérateurs.

3.2.1. Règles applicables quel que soit le niveau.

3.2.1.1. Minimisation des protocoles autorisés et filtrage.

3.2.1.2. Préparation de l’exploitation.

3.2.2. Règles applicables à l'opérateur pour un niveau 3.

3.2.2.1. Antivirus.

3.2.2.2. Maintien en conditions de sécurité.

3.2.2.3. Configuration et contrôle de conformité de la configuration.

3.2.2.4. Accès aux interfaces d'administration.

3.2.2.5. Sauvegarde.

3.2.3. Règles applicables à l'opérateur pour un niveau 4.

3.2.3.1. Configuration et contrôle de conformité de la configuration.

3.2.3.2. Maintien en condition de sécurité.

3.2.3.3. Sauvegarde.

ANNEXE(S)

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. **Présentation.**

L'hébergement d'un système informatique (1) ou d'une application désigne la mise à disposition par un opérateur d'une pile logicielle et/ou de services (matériels, logiciels, humains) nécessaires au fonctionnement du système informatique ou de l'application sur un ou des serveurs et accessibles *via* un réseau.

En raison de leur accessibilité, notamment sur internet, les systèmes informatiques et applications hébergés au sein du ministère de la défense doivent répondre à un socle minimal d'exigences de sécurité pour garantir leur résilience en cas d'attaque. C'est l'objet de cette directive.

Cette directive s'inscrit dans les missions de la direction générale des systèmes d'information (DGSIC), aux termes du décret n° 2006-497 du 2 mai 2006 modifié, portant création de la direction générale des systèmes d'information et fixant l'organisation des systèmes d'information et de communication du ministère de la défense.

1.2. **Niveaux de préconisation.**

Les règles définies dans ce document ont différents niveaux de préconisation et sont conformes au référentiel général d'interopérabilité [RGI] (2) et à la « *request for comments* » [RFC 2119] :

- obligatoire : ce niveau de préconisation signifie que la règle édictée indique une exigence absolue de la directive ;

- recommandé : ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente ;

- déconseillé : ce niveau de préconisation signifie que la règle édictée indique une prohibition qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être comprises et le cas soigneusement pesé ;

- interdit : ce niveau de préconisation signifie que la règle édictée indique une prohibition absolue de la directive.

La directive introduit le niveau de préconisation conseillé, qui se rapproche des bonnes pratiques :

- conseillé : ce niveau de préconisation signifie que la règle édictée est une bonne pratique de sécurité des systèmes d'information. Il n'est pas nécessaire d'instruire une dérogation lorsqu'elle n'est pas respectée.

1.3. **Champs et modalités d'application.**

Cette directive, à destination des opérateurs de systèmes informatiques (1) du ministère, est applicable aux organismes du ministère de la défense, au sens de l'arrêté du 30 novembre 2011 modifié, portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale. Elle fait partie de la politique de sécurité du système d'information (SI).

L'application des règles sera contrôlée lors des inspections, des audits et des contrôles.

Cette directive est incluse au cadre de cohérence technique du ministère. Elle est précisée par les référentiels techniques et méthodologiques au sein de chaque armée, service ou direction.

Par la suite, le terme opérateur désignera un opérateur de systèmes informatiques du ministère.

1.4. **Gestion des dérogations aux règles de la directive.**

Les dérogations concernent les circonstances et justifications des exceptions à toute règle obligatoire, interdit, recommandé et déconseillé.

Tout dossier de dérogation est adressé pour information au directeur général des systèmes d'information et de communication dans le cas de règle obligatoire et interdit.

Le non respect d'une règle conseillé n'est pas soumis à dérogation.

2. DOMAINE COUVERT ET EMPLOI.

La présente directive définit les exigences de sécurité que doivent respecter les opérateurs du ministère en matière d'hébergement. Elle fournit les éléments nécessaires à l'identification, à l'atteinte et au maintien d'un niveau de risque acceptable à la fois pour le système d'information des opérateurs du ministère et les systèmes informatiques ou application hébergés qui bénéficient de la sécurité de la structure d'hébergement.

2.1. **Principes.**

Afin d'assurer l'exploitation et le fonctionnement des systèmes informatiques et des applications hébergés, l'opérateur met en œuvre son propre système d'information. Ce dernier est composé de :

- la structure d'hébergement qui comprend :
    - l'infrastructure d'accueil (bâtiment, ressources réseaux, électrique, climatisation, etc.) et les équipements actifs (routeurs, serveurs, etc.) ;
    - le système informatique permettant d'opérer et de faire fonctionner la structure d'hébergement (virtualisation, gestion du maintien en condition de sécurité (MCS) de ces systèmes informatiques, etc.) ;
    - les services d'hébergement (distribution de correctifs, offre d'antivirus, etc.), ces derniers devant être vus comme des prestations offertes au client ;
- les piles logicielles exploitées des systèmes informatiques clients ;
- les ressources humaines assurant :
    - l'administration (1) et l'exploitation (1) de la structure d'hébergement ;
    - l'exploitation des piles logicielles des systèmes informatiques clients.

Les ressources humaines ne sont pas traitées dans cette directive.

Chaque composante du système d'information de l'opérateur doit respecter un certain nombre de principes de sécurité pour atteindre un niveau de risques acceptable et permettre ainsi aux systèmes informatiques clients de disposer d'un socle de confiance.

Le détail des niveaux d'hébergements, dont les niveaux 2, 3 et 4 correspondent aux offres *infrastructure as a service* (IaaS), *platform as a service* (PaaS) et *software as a service* (SaaS) proposées sur les marchés grand public, est présenté en annexe II. Les notions d'administration et d'exploitation, fondamentalement différentes, sont rappelées en annexe III.

2.2. **Périmètre et limites.**

Cette directive s'applique aux opérateurs du ministère. Lorsque le système informatique ou l'application est hébergé à l'extérieur du ministère, les directions de projet peuvent s'inspirer des règles qui y sont contenues afin de rédiger le contrat avec l'opérateur. Elle n'a pas pour but d'imposer des architectures aux opérateurs au sein des *datacenters* (1), ni de traiter des réseaux de transit.

3. LES RÈGLES.

3.1. **Règles applicables à la structure d'hébergement des opérateurs.**

3.1.1. ***Infrastructure d'accueil.***

Règle 1 : il est recommandé que les infrastructures hébergeant les serveurs physiques des opérateurs du ministère soient conformes aux recommandations *Tier* 3 de l'institut *Uptime*.

Règle 2 : il est obligatoire que les opérateurs établissent un planning incluant *a minima* :

- une vérification annuelle des procédures de gestion de continuité d'activité ;

- une mise en œuvre réelle d'un plan de continuité d'activité par an de l'un de ses *datacenters*.

Règle 3 : il est obligatoire que les systèmes informatiques de niveaux de protection différents soient installés a minima dans des baies séparées et dont le positionnement physique respecte les règles liées aux signaux parasites compromettants.

Règle 4 : il est obligatoire que les règles d'accès aux installations (y-compris pour les serveurs de proximité) respectent la réglementation du niveau de confidentialité ou de protection maximal des données des systèmes informatiques hébergés.

Remarque : par exemple, si les données traitées par un système informatique hébergé sont de niveau secret défense, l'infrastructure d'accueil du serveur devra être apte à protéger des informations de niveau secret défense.

3.1.2. ***Système d'information de la structure d'accueil (virtualisation et services vus du côté systèmes informatiques clients).***

Règle 5 : il est obligatoire d'homologuer le système d'information de la structure d'accueil.

Remarque : les systèmes informatiques hébergés par cette structure d'accueil héritent *de facto* des mesures apportées par l'homologation. Ainsi, le périmètre des éventuels audits sur des systèmes informatiques hébergés se restreindra au niveau des *datacenters* à la pile logicielle particulière du système informatique hébergé.

3.1.2.1. Règles générales.

3.1.2.1.1. Enrôlement auprès du centre d'analyse et de lutte informatique défensive.

Règle 6 : il est obligatoire que l'opérateur soit référencé au centre d'analyse et de lutte informatique défensive (CALID) en tant que tel.

Règle 7 : il est obligatoire que l'opérateur enrôle au CALID les systèmes informatiques supports des services d'hébergement. Il doit lui communiquer toute mise à jour de la pile logicielle.

3.1.2.1.2. Administration.

Règle 8 : il est recommandé d'utiliser des protocoles d'administration sécurisés.

Règle 9 : il est recommandé d'utiliser un réseau spécifique à l'administration, à défaut un *virtual local area network* (VLAN).

Règle 10 : il est déconseillé d'employer des protocoles d'administration ou de supervision (1) ne protégeant pas la confidentialité des flux (ftp, telnet, snmp v1, http, etc.).

Remarque : les dérogations à la règle précédente sont traitées dans le processus d'homologation du système.

Règle 11 : il est obligatoire que l'accès aux interfaces d'administration soit réalisé *via* des comptes nominatifs dédiés exclusivement aux seules activités d'administration.

Règle 12 : il est obligatoire que l'accès aux mécanismes d'administration soit restreint aux seuls postes d'administration autorisés.

Règle 13 : il est recommandé que l'accès aux interfaces d'administration soit réalisé par un dispositif de confiance permettant une journalisation (1) intègre des actions des administrateurs.

Remarque : le dispositif de confiance peut être une passerelle administrée par un nombre très restreint d'administrateur de sécurité.

3.1.2.1.3. Journalisation et supervision.

Règle 14 : il est obligatoire que l'opérateur définisse une politique de journalisation et de traitement des traces compatible avec les exigences de sécurité de son système d'information et avec la [DTRACSE].

3.1.2.1.4. Principe de minimalisation.

Les règles *infra* sont issues de la politique de sécurité des systèmes d'information (SSI) du ministère. Elles sont reprises ici dans un souci de cohérence globale de la directive.

Règle 15 : il est obligatoire que les ports ouverts sur les différents équipements actifs du réseau soient restreints au strict besoin. Tous les ports non utiles sont fermés.

Règle 16 : il est obligatoire que seuls les services nécessaires au fonctionnement de l'équipement et des systèmes informatiques de la structure d'hébergement soient actifs.
Les services inutiles sont désactivés ou désinstallés lorsque c'est possible.

Règle 17 : il est obligatoire que les privilèges des utilisateurs et des processus s'exécutant sur les différents équipements de la structure d'hébergement soient réduits au strict nécessaire pour permettre le fonctionnement des systèmes d'information de cette dernière (application principe du moindre privilège).

Règle 18 : il est obligatoire que lorsqu'un service applicatif ne nécessite pas de privilèges élevés pour fonctionner, il soit exécuté sous un compte non privilégié.

Règle 19 : il est obligatoire que les droits d'accès aux fichiers de configuration soient restreints au strict nécessaire.

3.1.2.1.5. Maintien en condition de sécurité.

Règle 20 : il est obligatoire que les opérateurs du ministère mettent en place un système de maintien en conditions de sécurité pour leur système d'information. Les procédures de contrôle d'innocuité des mises à jour doivent être décrites.

Remarque : la mise en place du MCS du système d'information d'un opérateur peut être décrite au sein de document de plus haut niveau (politique opérateur) et déclinée au sein de la structure d'hébergement. Elle doit respecter les préconisations [DMCS].

Règle 17 : il est obligatoire que les opérateurs mettent en place une politique de sécurité vis-à-vis des projets ou des clients en interface.

Remarque : cette politique doit notamment prendre en compte la sécurité sur toutes les interfaces des projets (couche virtualisation le cas échéant, etc.).

3.1.2.1.6. Gestion de configuration et conformité.

Remarque : la mise en place d'une gestion de configuration et du contrôle de la conformité peut être décrite au sein de document de plus haut niveau (politique opérateur) et déclinée au sein de la structure d'hébergement.

Règle 22 : il est obligatoire que l'opérateur mette en place une gestion de la configuration de son système informatique.

Remarque : il s'agit ici de connaître l'ensemble des versions des logiciels utilisés dans la structure. Seule la connaissance précise des briques logicielles et de leur version (déployée, en cours de déploiement, prévue dans le maintien en condition opérationnelle (MCO) permet d'identifier les impacts d'une vulnérabilité et de réagir en conséquence. Cette gestion de configuration pourra être outillée afin de faciliter sa mise en œuvre.

Règle 23 : il est obligatoire que toute mise à jour de la pile logicielle du système informatique de l'opérateur ayant un impact sur les interfaces avec les systèmes informatiques clients soit signifiée à ces derniers. Il indique notamment la date à compter de laquelle la mise à jour sera effectuée.

Règle 24 : il est obligatoire que toute évolution fonctionnelle d'un des systèmes informatiques de l'opérateur ayant un impact sur les interfaces avec les systèmes informatiques clients soit signifiée à ces derniers. La date de la mise en œuvre de cette évolution doit permettre aux systèmes informatiques impactés de réaliser les modifications nécessaires à leur fonctionnement.

Règle 25 : il est obligatoire qu'un système de contrôle de la configuration du système informatique de l'opérateur soit mis en place et supervisé en temps réel.

Remarque : la décision à prendre en cas de modification de la configuration relève de l'opérateur. Le système devra en outre traiter pour un système informatique la configuration appliquée et la configuration applicable (cas d'une nouvelle version en cours de déploiement et qui modifie la configuration).

Règle 26 : il est recommandé de mettre un place un contrôle d'intégrité des applicatifs non évolutifs et considérés comme sensibles par l'opérateur.

3.1.2.1.7. Choix des composants.

Règle 27 : il est obligatoire de soumettre le choix des briques logicielles « *components on the shelf* » : composants sur étagère (COTS), liées aux fonctions de sécurité du système informatique de la structure d'accueil au comité directeur des intranets.

3.1.2.1.8. Cartographie et sondes.

Règle 28 : il est obligatoire que les opérateurs du ministère disposent d'une cartographie des services hébergés. Cette cartographie doit comprendre :

- par site, la liste des services hébergés classés par réseau support ;

- au sein d'un site, par serveur physique ou logique, la liste des services hébergés.

Règle 29 : il est obligatoire que toute structure d'hébergement hébergeant un système informatique critique (3) soit supervisée par le *security operation center* (SOC) de l'opérateur.

Règle 30 : il est obligatoire que la solution de supervision inclue une sonde pour les structures hébergeant des systèmes informatiques clients qui sont critiques.

Remarque : l'objectif de la sonde est de détecter notamment un comportement anormal.

3.1.2.2. Règles spécifique à l'hébergement mutualisé (virtualisation).

3.1.2.2.1. Configuration.

Règle 31 : il est obligatoire que la configuration du logiciel de virtualisation prenne en compte les guides ministériels de sécurisation existants. Tout écart doit être justifié.

3.1.2.2.2. Administration de la couche virtualisation.

Règle 32 : il est recommandé d'utiliser une authentification forte des administrateurs pour administrer la couche logicielle de virtualisation.

Règle 33 : il est recommandé de dédier une équipe d'administration à la solution de virtualisation distincte de celle des systèmes invités ou des services d'hébergement.

Remarque : l'équipe d'administration de la solution de virtualisation doit avoir notamment en charge :

- l'administration des équipements de stockage physiques [*network attached storage* (NAS)/*storage area network* (SAN)] ;

- l'administration des équipements réseau physiques (et virtuels le cas échéant) ;

- l'administration de la solution de virtualisation (dans son ensemble) ;

- la gestion de la sécurité associée à la virtualisation et plus particulièrement le maintien d'un cloisonnement des instances hébergées du fait du partage de ressources ;

- éventuellement l'audit et la supervision des machines hôtes.

Règle 34 : il est obligatoire que l'habilitation de l'équipe d'administration de la couche virtualisation soit compatible des données manipulées par les systèmes clients sauf à ce qu'elles soient chiffrées de telle sorte que l'équipe d'administration ne puisse techniquement y accéder.

Remarque : par exemple, lorsque des données diffusion restreinte de l'organisation du traité de l'Alantique Nord (OTAN) sont traitées par les systèmes informatiques clients, une habilitation secret OTAN est nécessaire pour les administrateurs conformément à la directive n° AC/322-D/0048 (4) du 9 décembre 2011 INFOSEC *technical implatation directive for computer and local area network security* de l'OTAN.

3.1.2.2.3. Réduction de la surface d'exposition.

Les règles *infra* sont issues de la politique SSI du ministère. Elles sont reprises ici dans un souci de cohérence globale de la directive.

Règle 35 : il est obligatoire de changer les éléments d'authentification par défaut avant la mise en service opérationnelle de la solution.

3.1.2.2.4. Cloisonnement des systèmes clients.

Règle 36 : il est obligatoire que les systèmes informatiques clients soient cloisonnés de façon à interdire tout échange sans passer par l'hyperviseur (1).

Règle 37 : il est conseillé d'utiliser du matériel (contrôleur disque, carte réseau, processeur, etc.) gérant le cloisonnement.

3.1.2.2.5. Certification/qualification.

Règle 38 : il est conseillé d'utiliser des solutions de virtualisation certifiées.

3.1.3. ***Services d'hébergement.***

Les services d'hébergement décrits dans les points qui suivent doivent être considérés comme des prestations offertes aux systèmes informatiques clients de la structure d'hébergement. Les services applicatifs communs [*network time protocole* (NTP), etc.] ne sont pas abordés dans la directive.

Règle 39 : il est obligatoire que lorsqu'un service est redondé, la partie redondée soit située dans un *datacenter* différent de la partie nominale.

3.1.3.1. Service de maintien en conditions de sécurité.

Règle 40 : il est obligatoire que l'opérateur mette en place un service de mise à disposition des correctifs *a minima* des briques logicielles qu'il exploite.

Règle 41 : il est recommandé que l'opérateur mette à disposition *via* ce service les correctifs des applicatifs largement utilisés sur les réseaux, mais hors de la pile logicielle qu'il exploite.

Règle 42 : il est obligatoire que les correctifs mis à disposition *via* ce service soient compatibles du service d'hébergement.

Remarque : cette règle permet d'éviter qu'un correctif de sécurité non compatible par exemple avec la couche de virtualisation entraine une indisponibilité de tous les systèmes d'information ayant fait l'objet d'une homologation sommaire. En effet, pour ces derniers, les correctifs de sécurité critiques sont appliqués sans tests de régression ou de compatibilité.

Lorsque l'application d'un correctif sécurité entraîne l'indisponibilité d'un système d'information ayant fait l'objet d'une homologation sommaire, c'est à la direction de projet du système d'information de prendre les mesures nécessaires pour assurer la remise en service du système informatique concerné (en liaison avec l'opérateur).

Règle 43 : il est obligatoire de protéger les correctifs en intégrité lors de leur diffusion par ce service.

Règle 44 : il est obligatoire que ce service permette de connaître l'état de diffusion d'un correctif sur l'ensemble de la structure d'hébergement et les systèmes informatiques clients.

Règle 45 : il est obligatoire que l'opérateur décline et fournisse aux clients sa politique de mise à disposition des correctifs.

Remarque : concernant cette dernière règle, la connaissance de l'état de diffusion d'un correctif sur l'ensemble d'un réseau peut être réalisée par un logiciel différent.

3.1.3.2. Antivirus.

Règle 46 : il est obligatoire que l'opérateur définisse une stratégie de lutte antivirale. Il met à disposition les anti-virus (licences comprises) et les mises à jour.

Règle 47 : il est obligatoire que les signatures soient rendues disponibles *via* ce service dans le jour qui suit leur parution.

:

Règle 48 : il est recommandé que les moteurs des anti-virus soient rendus disponibles à l'issue d'une phase de test sur une ou plusieurs instances représentatives de la pile logicielle.

Règle 49 : il est obligatoire que l'opérateur supervise les alertes virales sur l'ensemble des réseaux opérés.

Règle 50 : il est obligatoire que l'opérateur décline et fournisse aux clients sa politique de mise à jour des signatures et moteurs antiviraux.

3.1.3.3. Sauvegarde et restauration.

Règle 51 : il est obligatoire que l'opérateur mette en place un système de sauvegarde couvrant les données suivantes :

- données systèmes (1) ;

- données structurées (1) ;

- données non structurées (1).

Règle 52 : il est obligatoire que le contrat de service précise le périmètre et la périodicité des sauvegardes réalisée par l'opérateur.

3.2. **Règles applicables à l'exploitation des systèmes informatiques clients par les opérateurs.**

Il n'y a pas de règle spécifiquement applicable aux niveaux d'hébergement 1 et 2 puisque par définition il n'y a pas d'exploitation du système informatique par l'opérateur.

Ce tableau définit la répartition des actions selon le niveau d'hébergement d'un système d'information. Chaque action fait référence à une ou plusieurs règles de la directive.

ACTION.	RÈGLES ASSOCIÉES.	RESPONSABLE EN FONCTION DU NIVEAU DE SERVICES.		
		1 ET 2.	3.	4.
Fourniture d'un antivirus	Règle 41	Opérateur	Opérateur	Opérateur
Installation et paramétrage de l'antivirus	Règle 51	Client/TME	Opérateur	Opérateur
Supervision des alertes virales	Règle 44	Opérateur	Opérateur	Opérateur
MCS de l'OS	Règles 37,38, 52, 53	Client/TME	Opérateur (5)	Opérateur (5)
MCS du système de gestion de base de données (SGBD)	Règles 37, 38, 52, 53	Client/TME	Opérateur (5)	Opérateur (5)
MCS du système informatique (hors SGBD et OS)	Règles 37, 38, 70, 71	Client/TME	Client/TME	Opérateur (5)
Mise en place et paramétrage d'un pare-feu	Règle 49	Client/TME	Opérateur	Opérateur
Configuration de l'OS	Règles 54, 55	Client/TME	Opérateur	Opérateur
Configuration du SGBD	Règles 54, 56	Client/TME	Opérateur	Opérateur
Configuration du système informatique (hors SGBD et OS)	Règles 68, 69	Client/TME	Client/TME	Opérateur
Fourniture des indicateurs relatifs à la sécurité	Règles 40, 44, 57	Opérateur	Opérateur	Opérateur
Paramétrage du contrôle de conformité de la configuration	Règle 57	Client/TME	Opérateur	Opérateur
Supervision du contrôle de conformité de la configuration	Règle 57	Client/TME	Opérateur	Opérateur
Paramétrage de la journalisation (OS et SGBD)	Règles 54, 55	Client/TME	Opérateur	Opérateur
Paramétrage de la journalisation (hors OS et SGBD)	Règles 68, 69 et [DRACES]	Client/TME	Client/TME	Opérateur

Exploitations des traces (OS et SGBD)	[DTRACES]	Client/TME	Opérateur	Opérateur
Exploitations des traces (hors OS et SGBD)	[DTRACES]	Client/TME	Client/TME	Opérateur

Remarque : concernant l'exploitation des traces, l'opérateur (et notamment son SOC) peut toutefois y accéder quel que soit le niveau d'hébergement dans le cadre de sa mission.

Concernant le maintien en conditions de sécurité, l'opérateur n'est chargé que du déploiement des correctifs sur le système d'information hébergé. Sauf mention contraire dans le contrat de service, la qualification d'une mise à jour (tests de compatibilité, de non régression, etc.) est à la charge de la direction de projet ou de programme.

3.2.1. ***Règles applicables quel que soit le niveau.***

Règle 53 : il est obligatoire que les opérateurs ministériels disposent d'une cartographie des systèmes d'information hébergés. Cette cartographie doit comprendre :

- par site, la liste des systèmes informatiques hébergés classés par réseau support ;

- au sein d'un site, par serveur, la liste des systèmes informatiques hébergés.

Règle 54 : il est obligatoire que l'opérateur dispose de la liste des sous-traitants extérieurs au ministère assurant des tâches d'exploitation sur les systèmes informatiques hébergés.

Remarque : cette information doit être communiquée par la direction de projet du système informatique hébergé.

Règle 55 : il est obligatoire que l'opérateur dispose par sous-traitant de la liste des systèmes informatiques exploités ainsi que le périmètre de l'exploitation sous-traitée.

3.2.1.1. Minimisation des protocoles autorisés et filtrage.

Règle 56 : il est obligatoire que le trafic réseau en provenance et à destination des systèmes hébergés fasse l'objet d'un contrôle permanent afin de n'autoriser que les flux légitimes.

Remarque : une matrice de flux (inventaire des flux légitimes) est fournie par la direction de projet. La politique de filtrage est définie à partir de la matrice des flux. Les dispositifs de filtrage sont bloquants par défaut, tout ce qui n'est pas explicitement autorisé étant interdit.

3.2.1.2. Préparation de l'exploitation.

Règle 57 : il est recommandé que l'opérateur dispose d'une liste de vérification, contrôlée lors de la prise en charge de l'exploitation (notamment sur la conformité à la présente directive).

3.2.2. ***Règles applicables à l'opérateur pour un niveau 3.***

3.2.2.1. Antivirus.

Règle 58 : il est obligatoire que l'opérateur configure l'antivirus conformément aux PES du système d'information et assure sa mise à jour.

3.2.2.2. Maintien en conditions de sécurité.

Règle 59 : il est obligatoire que l'opérateur assure le MCS du système d'exploitation et du SGBD le cas échéant, dans le cadre du contrat de service.

Remarque : le déploiement des correctifs peut toutefois être soumis à accord préalable du RSSI. Ce point est traité dans le contrat de service.

Règle 60 : il est obligatoire que l'opérateur configure ce service pour mettre à jour automatiquement l'OS et le SGBD des systèmes informatiques clients ayant fait l'objet d'une homologation sommaire avec les correctifs de sécurité critiques.

3.2.2.3. Configuration et contrôle de conformité de la configuration.

Règle 61 : il est obligatoire que lorsqu'ils existent, les guides ministériels [guides de recommandations de la direction générale pour l'armement - maitrise de l'information (DGA/MI), guides de recommandation de la direction interarmées des réseaux d'infrastructure et des systèmes d'information du ministère de la défense (DIRISI), etc.] soient déclinés pour chaque système d'exploitation ou SGBD utilisés avec fourniture d'une matrice d'implémentation qui indique les mesures prises et justifie les mesures non appliquées.

Règle 62 : il est obligatoire que l'opérateur configure l'OS et le SGBD client conformément à la documentation d'installation du système informatique.

Règle 63 : il est obligatoire que lorsque le SGBD est partagé par plusieurs systèmes informatiques clients, l'opérateur cloisonne ces systèmes au sein du SGBD.

Remarque : le cloisonnement peut être basé sur un mécanisme logique adossé à un contrôle d'accès. Si la direction de projet a des besoins de cloisonnement plus forts, il lui appartient de mettre en place des moyens complémentaires. De la même façon le système d'hébergement et de sauvegarde étant mutualisé, il revient à la direction de projet d'un système d'information de prendre les mesures nécessaires pour gérer le besoin d'en connaître.

Règle 64 : il est recommandé que l'opérateur mette en place le contrôle de la conformité de la configuration et assure sa supervision.

Remarque : l'opérateur doit donc disposer de la configuration de référence qui lui est remise par la DP.

3.2.2.4. Accès aux interfaces d'administration.

Règle 65 : il est recommandé d'utiliser des protocoles d'administration sécurisés.

Règle 66 : il est obligatoire que l'accès aux interfaces d'administration soit réalisé via des comptes nominatifs.

3.2.2.5. Sauvegarde.

Règle 67 : il est obligatoire de réaliser une sauvegarde des données système avant et à l'issue d'une modification majeure de ces dernières.

Remarque : une modification majeure est, par exemple, l'application d'un « *service pack* ».

Règle 68 : il est obligatoire qu'à l'issue d'une restauration des données système, les correctifs de sécurité installés depuis la dernière sauvegarde soient réinstallés avant la remise en production du système d'information.

Règle 69 : il est recommandé de sauvegarder les données systèmes au moins une fois par mois et de conserver les trois dernières sauvegardes.

Règle 70 : il est recommandé de faire une sauvegarde incrémentale des données structurées tous les jours et de conserver ces dernières pendant trois mois.

Règle 71 : il est recommandé de faire une sauvegarde complète des données structurées toutes les semaines et de conserver ces dernières pendant trois mois.

Règle 72 : il est obligatoire de conserver les sauvegardes sur un serveur physique différent de celui hébergeant le système informatique sauvegardé.

Règle 73 : il est recommandé de conserver les sauvegardes dans un local distinct de celui contenant le serveur physique du système informatique hébergé.

3.2.3. ***Règles applicables à l'opérateur pour un niveau 4.***

Règle 74 : il est obligatoire que l'opérateur applique les règles relatives à un hébergement de niveau 3.

3.2.3.1. Configuration et contrôle de conformité de la configuration.

Règle 75 : il est obligatoire que lorsqu'ils existent, les guides ministériels (guides de recommandations de DGA/MI, guides de recommandation de la DIRISI, etc.) soient déclinés pour chaque composant utilisé avec fourniture d'une matrice d'implémentation qui indique les mesures prises et justifie les mesures non appliquées.

Règle 76 : il est obligatoire que l'opérateur configure les composants du système informatique client conformément à la documentation d'installation du système d'information.

3.2.3.2. Maintien en condition de sécurité.

Règle 77 : il est obligatoire que l'opérateur assure le MCS de l'ensemble de la pile logicielle du système informatique client, dans le cadre du contrat de service.

Remarque : le déploiement des correctifs peut toutefois être soumis à accord préalable du RSSI.

Règle 78 : il est obligatoire que l'opérateur configure ce service pour mettre à jour automatiquement l'ensemble de la pile logicielle des systèmes informatiques clients ayant fait l'objet d'une homologation sommaire avec les correctifs de sécurité critiques.

3.2.3.3. Sauvegarde.

Règle 79 : il est recommandé de faire une sauvegarde incrémentale des données non structurées tous les jours ouvrables et de conserver les quatre dernières versions.

Règle 80 : il est recommandé de faire une sauvegarde complète des données non structurées une fois par semaine. Seule la dernière version est conservée.

Pour le ministre de la défense et par délégation :

Le général de corps d'armée,
directeur général des systèmes d'information et de communication,

Gérard LAPPREND.

---

(1) Cf. annexe I.

(2) Les mots entre crochets ([ ]) figurent dans le cadre documentaire.

(3) Cf. directive n° 17/DEF/DGSIC du 6 juillet 2011 modifiée, portant sur l'identification et le suivi des systèmes critiques.

(4) n.i. BO.

(5) Le déploiement des correctifs peut toutefois être soumis à accord préalable du responsable de la sécurité du système d'information (RSSI). Ce point est traité dans le contrat de service.

ANNEXE I.

DÉFINITIONS.

Administration	:	cf. annexe III.
Datacenter	:	centre de traitement des données informatiques incluant le système de production. La notion de Datacenter intègre tous les constituants qui composent l'environnement informatique. Cela comprend les locaux, les racks, les systèmes d'alimentation et leur redondance, les équipements serveurs, les équipementsréseaux, les éléments de sauvegarde, de stockage, les consoles d'administration locales ainsi que la climatisation, le système de prévention contre l'incendie, les éléments permettant de sécuriser les accès tels que les lecteurs de badges, systèmes de code d'accès, les caméras et systèmes d'alertes divers etc.
Données système	:	ensemble des données constituant le « système d'exploitation » des serveurs hébergés.
Données structurées	:	ensemble des données contenues dans des bases de données, quel que soit le moteur de la base.
Données non structurées	:	ensemble des données non incluses dans les données système ou les données structurées.
Exploitation	:	cf. annexe III.
Hyperviseur	:	système ou programme qui permet à de multiples systèmes d'exploitation et programmes de fonctionner sur un même serveur en parallèle. L'hyperviseur repose sur la machine physique et gère les machines virtuelles. C'est le moteur de la virtualisation.
Journalisation	:	enregistrement des événements relatifs à l'utilisation et au fonctionnement d'un système d'information.
Opérateur de systèmes informatiques	:	toute entité du ministère assurant l'exploitation d'un réseau informatique ou fournissant un service d'hébergement et/ou d'exploitation de systèmes informatiques et d'applications.
Supervision	:	cf. annexe III.
Système d'information	:	ensemble organisé de ressources (personnels, finances, matériels, logiciels) permettant de collecter, stocker, traiter et communiquer les informations. Le système d'information appuie les activités de l'organisation et contribue à l'atteinte des objectifs.
Système informatique	:	tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure, ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données [décret n° 2006-580 du 23 mai 2006 (A)].

(A) n.i. BO ; JO n° 120 du 24 mai 2006, p. 7568, texte n° 2.

ANNEXE II.

NIVEAUX D'HÉBERGEMENT D'UN SYSTÈME INFORMATIQUE.

1. HÉBERGEMENT DE NIVEAU 0.

Le système est totalement pris en charge par l'équipe de projet. L'ensemble des règles liées à la sécurité de ce système d'information s'appliquent néanmoins, l'équipe de projet pouvant être vue comme son propre opérateur.

2. HÉBERGEMENT DE NIVEAU 1.

L'opérateur fournit uniquement l'infrastructure d'hébergement (place dans une salle serveur, climatisation, accès aux réseaux électrique et informatique). Le contrôle d'accès aux équipements est assuré par l'opérateur.

L'achat, la livraison, l'installation, la maintenance et l'exploitation du matériel et des logiciels incombent entièrement à la direction de projet du système informatique hébergé. Le retrait, le recyclage et le traitement des supports sont assurés par la direction du projet.

La tierce maintenance d'exploitation (TME) qui est éventuellement mise en place par la direction de projet du système d'information est placée sous sa responsabilité.

La supervision des couches applicatives est envisageable sous réserve que les outils utilisés par l'opérateur soient compatibles avec les briques logicielles du système informatique.

3. HÉBERGEMENT DE NIVEAU 2 - INFRASTRUCTURE AS A SERVICE.

L'opérateur fournit et exploite les couches basses (réseau, matériels, virtualisation, stockage SAN) et assure la sauvegarde de la configuration et des données de l'application. Le retrait, le recyclage et le traitement des supports sont assurés par l'opérateur.

L'exploitation de la couche technique applicative reste à la charge de la direction du projet du système d'information (bases de données comprises).

La tierce maintenance d'exploitation (TME) qui est éventuellement mise en place par la direction de projet du système d'information est placée sous sa responsabilité.

L'opérateur supervise uniquement les couches basses. La supervision des couches applicatives est envisageable sous réserve que les outils utilisés par l'opérateur soient compatibles avec les briques logicielles du système informatique.

4. HÉBERGEMENT DE NIVEAU 3 - PLATEFORM AS A SERVICE.

En plus des prestations de niveau 2, l'opérateur assure l'exploitation technique des bases de données du système informatique sous réserve qu'elles soient référencées dans la liste des briques logicielles exploitées par l'opérateur. Les bases de données peuvent être mutualisées avec d'autres systèmes informatique. La direction de projet doit donc respecter les règles d'exploitation de l'opérateur.

L'exploitation du reste de la pile logicielle du système informatique est à la charge de l'équipe de projet.

La tierce maintenance d'exploitation (TME) qui est éventuellement mise en place par la direction de projet du système d'information est placée sous sa responsabilité.

La supervision des couches applicatives est envisageable sous réserve que les outils utilisés par l'opérateur soient compatibles avec les briques logicielles du système informatique.

5. HÉBERGEMENT DE NIVEAU 4 - SOFTWARE AS A SERVICE.

L'opérateur assure l'exploitation et la supervision de l'ensemble des couches basses et de la couche technique applicative (OS, serveur applicatif, serveur de présentation, bases de données) sous réserve que les composants de cette dernière appartiennent à ceux référencés dans la liste des briques logicielles exploitées par l'opérateur.

ANNEXE III.

ADMINISTRATION ET EXPLOITATION.

1. L'ADMINISTRATION.

1.1. **L'administration technique.**

L'administration technique recouvre l'ensemble des opérations visant à garantir la disponibilité et le maintien à niveau du système informatique dans un objectif de qualité, de productivité et de sécurité. Elle regroupe les actions techniques de configuration, de paramétrage, d'installation, de gestion des configurations et de mise à jour du système informatique (hors patch et correctifs).

Les opérations d'administration sont complémentaires de l'exploitation axée sur la recherche permanente d'un fonctionnement optimal des outils, systèmes et réseaux sous sa responsabilité.

1.2. **L'administration fonctionnelle.**

L'administration fonctionnelle recouvre l'ensemble des opérations réalisées dans un domaine métier via des outils et des interfaces qui ne nécessitent pas forcément d'avoir un profil d'exploitant, et qui concourent à permettre aux usagers finaux de mettre en œuvre le système en fonction du rôle qu'ils ont à y tenir. Ces opérations sont réalisées par des fonctionnels du domaine concerné.

2. L'EXPLOITATION.

L'exploitation regroupe l'ensemble des opérations de mise en œuvre des infrastructures de production dans le respect des plannings et de la qualité attendue. Elle comprend la surveillance du fonctionnement des équipements informatiques physiques et logiques du centre de production, dans le cadre des normes, méthodes d'exploitation et de sécurité. Les tâches prévues au titre de cette activité sont les suivantes :

- contrôle au quotidien du fonctionnement du système (charge, performance, sécurité, disponibilité) ;

- analyse des dysfonctionnements, remontée des incidents vers les équipes de support ;

- réalisation des opérations de sauvegarde, vérification des supports de sauvegarde ;

- rédaction des consignes, stabilisation, amélioration en permanence de l'environnement d'exploitation ;

- rédaction des dossiers de sécurité, et respect de ces consignes en permanence ;

- application des patchs et correctifs ;

- mise à jour des indicateurs (déterminés en coordination avec l'opérateur et la direction de projet) du tableau de bord du bénéficiaire.

La supervision fait partie de l'exploitation. Elle consiste en :

- la surveillance des matériels et services spécifiés ;

- l'émission d'alertes sur l'état de santé des systèmes (couches basses et applicatifs) en fonction d'indicateurs préétablis.

Les indicateurs sont de trois types :

- les indicateurs techniques, utilisés au quotidien par les équipes d'exploitation pour assurer la continuité de service. On parle de supervision technique ;

- les indicateurs fonctionnels, proposés aux directions de projet pour visualiser l'utilisation et le comportement de leur système informatique. On parle de supervision fonctionnelle ;

- les indicateurs de capacité, utilisés par l'opérateur pour anticiper l'évolution des ressources (bande passante, disque, mémoire, processeurs, etc.) requises par le système informatique.

ANNEXE IV.

CADRE DOCUMENTAIRE.

1. DOCUMENTS APPLICABLES.

[CP]	:	code pénal.
[CNIL]	:	loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés (version consolidée au 27 août 2011) - (disponible sur le site legifrance.gouv.fr).
[RGS]	:	référentiel général de sécurité, version 1.0 du 6 mai 2010.
[RGI]	:	arrêté du 9 novembre 2009 (A) - référentiel général d'interopérabilité.
[IGI 1300]	:	instruction générale interministérielle n° 1300/SGDSN/PSE/SSD du 30 novembre 2011 (1) sur la protection du secret de la défense nationale.
[PSI]	:	politique du système d'information du ministère - disponible sur le site synoptic (intradef).
[PSSI]	:	instruction n° 133/DEF/SEC/DIR/SIC du 18 mars 2002 modifiée, relative à la politique de sécurité des systèmes d'information du ministère de la défense.
[IM 900]	:	instruction ministérielle n° 900/DEF/CAB/-- du 26 janvier 2012 (1) relative à la protection du secret de la défense nationale au sein du ministère de la défense.
[DTRACES]	:	directive n° 29/DEF/DGSIC du 12 novembre 2009 (1) portant sur les traces et leur gestion au sein du ministère de la défense - disponible sur le site synoptic (intradef).
[DMCS]	:	maintien en condition de sécurité des systèmes d'information au sein du ministère de la défense n° D-11000976/DEF/EMA/CPI/SSI/-- du 4 février 2011 (1).
[RFC 2119]	:	types de préconisations.
[décret n° 2006-580]	:	décret n° 2006-580 du 23 mai 2006 (B) portant publication de la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001.

2. SITES DE RÉFÉRENCES.

[site ANSSI]	site SSI de l'ANSSI sur internet	www.ssi.gouv.fr
[synopTIC]	site SSI du ministère sur intradef	www.synoptic.intradef.gouv.fr
[site DGSIC]	site de la DGSIC sur intradef	www.dgsic.defense.gouv.fr

---

(A) n.i BO ; JO n° 262 du 11 novembre 2009, p. 19593, texte n° 32.

(1) n.i. BO.

(B) n.i BO ; JO n° 120 du 24 mai 2006, p. 7568, texte n° 2.