BULLETIN OFFICIEL DES ARMÉES

Édition Chronologique n° 17 du 20 avril 2015

PARTIE PERMANENTE
État-Major des Armées (EMA)

Texte 13

DIRECTIVE N° 33/DEF/DGSIC
retour d'expérience en cybersécurité au sein du ministère de la défense.

Du *5 février 2015*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

DIRECTIVE N° 33/DEF/DGSIC retour d'expérience en cybersécurité au sein du ministère de la défense.

Du 5 février 2015

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

Pièce(s) Jointe(s) :

Une annexe.

Classement dans l'édition méthodique : BOEM 161.4

Référence de publication : BOC n° 17 du 20 avril 2015, texte 13.

SOMMAIRE

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. **Présentation.**

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

Elle définit et organise le processus de retour d'expérience (RETEX) dans le domaine de la cybersécurité au sein du ministère de la défense. Ce processus a pour objectif d'améliorer l'efficience de la cybersécurité, en proposant des solutions aux lacunes constatées.

À cet effet, cette directive précise les responsabilités des acteurs de la cybersécurité et l'organisation mise en place pour exploiter les enseignements issus des résultats des audits, contrôles et inspections mais aussi de l'analyse des causes des incidents de sécurité ou encore des propositions suggérées par les utilisateurs.

1.2. **Niveaux de préconisation.**

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

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

1.3. **Modalités d'application.**

L'ensemble des règles définies dans cette directive s'applique aux organismes du ministère de la défense.

2. CADRE DOCUMENTAIRE.

2.1. **Documents applicables.**

[RGI]	:	Référentiel général d'interopérabilité, version 1.0 du 12 mai 2009. http://references.modernisation.gouv.fr/rgi.interoperabilite
[RGS]	:	Référentiel général de sécurité, version 2.0 du 13 juin 2014. http://www.ssi.gouv.fr/rgs
[IGI 1300]	:	Instruction générale interministérielle n° 1300 du 30 novembre 2011 (1) sur la protection du secret de la défense nationale. http://www.ssi.gouv.fr/fr/reglementation-ssi/systemes-d-information/
[PSSIE]	:	Politique de sécurité des systèmes d'information de l'État : circulaire du premier ministre n° 5725/SG du 17 juillet 2014 (1) relatif à la politique de sécurité des systèmes d'information de l'État. http://circulaire.legifrance.gouv.fr/pdf/2014/08/cir_38641.pdf
[II910]	:	Instruction interministérielle n° 910/SGDSN/ANSSI du 22 octobre 2013 (1) relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI). http://synoptic.intradef.gouv.fr/sites/default/files/cir_37647.pdf (intranet)
[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. http://synoptic.intradef.gouv.fr/sites/default/files/55308737d01.pdf (intradef)
[PSSI-M]	:	Instruction ministérielle n° 7326/DEF/CAB du 7 août 2014 (1) relative à la politique de sécurité des systèmes d'information du ministère de la défense. http://synoptic.intradef.gouv.fr/sites/default/files/20140807_np_cab_im-7326_pssi-mindef.pdf (intradef)

Normes et standards applicables :

[RFC 2119]	:	Mots-clés pour niveaux d'obligation

2.2. **Autres documents et sites de référence.**

[PIA]	:	Publication interarmées 7.7 relative au retour d'expérience des armées. Note n° 427/DEF/EMA/EMP.1 du 18 mars 2008 (1). http://www.cicde.defense.gouv.fr/IMG/pdf/20070318_np_ema_emp-1_pia-7-7-retex.pdf (intranet)
[DC CICDE]	:	Document cadre DC-002_RETEX(2014). Note n° 140/DEF/CICDE du 19 juin 2014 (1). http://www.cicde.defense.gouv.fr/IMG/pdf/20140619_np_cicde_dc-002-retex.pdf (intranet)
[Sites SSI]	:	Site de l'ANSSI à l'adresse internet : http://www.ssi.gouv.fr Site de sécurité des systèmes d'information (SSI) du ministère à l'adresse intradef : http://synoptic.intradef.gouv.fr/ssi

3. DOMAINE COUVERT ET EMPLOI.

3.1. **Définition.**

Le retour d'expérience consiste en une analyse méthodique et rigoureuse d'un évènement ou d'un exercice dans le but de comprendre les causes et les mécanismes ayant conduit, lors de la gestion, à des dysfonctionnements, ou à la mise en place de pratiques innovantes, afin d'en tirer des enseignements pour l'avenir.

Il s'agit d'une démarche nécessaire pour comprendre, en particulier, la nature et l'amplitude des écarts entre les pratiques mises en œuvre et les référentiels établis. Il peut conduire à faire évoluer le *corpus* réglementaire, renforcer la formation du personnel ou encore recommander l'application de nouvelles configurations matérielles ou logicielles.

Il est important de souligner dès à présent que le RETEX n'est pas un moyen d'identifier des responsabilités : il s'intéresse aux causes des évènements observés, et non pas aux individus impliqués.

Le retour d'expérience constitue ainsi un véritable outil dont l'objectif n'est pas de sanctionner mais d'apprendre pour progresser. À cet effet, la fluidité de circulation de l'information sera systématiquement recherchée. À ce titre, il faut clairement distinguer la procédure de traitement d'un évènement, qui pourra être classifiée si nécessaire, et le retour d'expérience dudit évènement, postérieur à son traitement, et qui sera non classifié dans la mesure du possible, par exemple en décontextualisant les faits (lieux, systèmes, domaines, etc.).

3.2. **Périmètre d'application.**

Les principes de retour d'expérience énoncés dans cette directive s'appliquent spécifiquement aux métiers de la cybersécurité dans son application quotidienne au ministère de la défense, y compris dans le cadre des opérations militaires, en complément des prescriptions spécifiées dans les documents de référence [PIA] et [DC CICDE].

4. LES RÈGLES.

4.1. **Organisation générale.**

Le processus de RETEX en cybersécurité s'articule en deux échelons principaux :

- un échelon ministériel d'animation et de synthèse du RETEX, pouvant être amené à conduire le retour d'expérience pour les faits les plus importants ;

- un échelon de conduite du RETEX, décentralisé au sein de chaque autorité qualifiée en SSI (AQ SSI) et de la chaîne de lutte informatique défensive (LID).

Cette organisation doit permettre un traitement du RETEX au bon niveau de responsabilité, et favoriser les échanges au sein d'un réseau de contacts préalablement identifiés.

4.1.1. ***Organisation de l'échelon ministériel.***

RO 1 : il est obligatoire qu'un officier chargé de l'animation du retour d'expérience en cybersécurité soit désigné au niveau ministériel.

Ce responsable sera prioritairement choisi au sein de la sous-direction SSI de la DGSIC.

RO 2 : il est OBLIGATOIRE qu'une commission spécialisée du RETEX en cybersécurité (CS-RETEX) soit mise en place au niveau ministériel.

Cette commission, présidée par le responsable ministériel du RETEX, sera composée de chaque responsable du RETEX au niveau des AQ SSI, du responsable du RETEX de la chaine LID, et du représentant du groupe de sécurité chargé du contrôle des systèmes de traitement automatique de données (GSTAD) en qualité d'équipe d'inspection du ministère. En fonction de l'ordre du jour, la commission pourra faire appel à un ou plusieurs spécialistes du sujet traité.

Les objectifs de cette commission sont de :

- synthétiser le retour d'expérience de chaque acteur, afin d'en dégager, le cas échéant, une tendance ministérielle ;

- établir le retour d'expérience des évènements les plus significatifs, ou ceux dont les implications dépassent la compétence du niveau de l'AQ SSI ou de la chaine LID ;

- favoriser la diffusion du RETEX entre les acteurs du ministère, et diffuser le RETEX provenant de sources extérieures au ministère ;

- capitaliser le retour d'expérience, en tenant à jour une base de connaissances librement consultable.

RO 3 : il est obligatoire que la commission spécialisée du RETEX en cybersécurité se réunisse *a minima* semestriellement.

Par ailleurs, il est possible de réunir la commission en session extraordinaire ou en comité restreint, en particulier en cas d'évènement nécessitant un traitement rapide, sur demande de l'un des acteurs, ou sur mandat particulier du haut fonctionnaire correspondant de défense et de sécurité ou de son adjoint, le directeur de la protection des infrastructures, moyens et activités de la défense (DPID).

RO 4 : il est obligatoire que la commission spécialisée du RETEX en cybersécurité propose, le cas échéant, un plan d'action suite aux enseignements identifiés.

Pour les actions simples, la commission pourra être l'organe décisionnel (par exemple la mise à jour d'une directive ministérielle). Les actions nécessitant une décision à plus haut niveau feront l'objet d'une inscription à l'ordre du jour des instances idoines (CMSSI pour l'évolution de la règlementation ministérielle, commission spécialisée de la formation cyber pour les aspects liés à la formation, etc.)

RO 5 : il est obligatoire que les enseignements identifiés soient capitalisés et diffusés le plus largement possible.

Une capitalisation du RETEX sera réalisée au niveau ministériel, sous la responsabilité de la DGSIC. Dès qu'un enseignement sera validé au niveau des AQ SSI, il sera transmis, à titre de compte-rendu, au niveau ministériel.

Une diffusion régulière des principaux enseignements sera mise en place, sous la forme d'une note d'information du RETEX. Cette diffusion s'adresse avant tout aux acteurs ministériels, mais pourra s'étendre aux entités extérieures au ministère (industriels de défense, etc.), selon la nature des sujets traités. L'autorisation de diffusion externe sera donnée par la commission spécialisée du RETEX.

La lettre d'information du RETEX sera également publiée sur le site Synoptic.

RO 6 : il est recommandé que l'échelon ministériel du RETEX détermine annuellement des axes prioritaires de recherche d'enseignements en cybersécurité.

Cette règle, inspirée du RETEX des opérations militaires [PIA], vise à réserver un traitement systématique et précis sur des domaines préalablement identifiés. Cela peut inclure le retour d'expérience consécutif à la mise en place de nouveaux équipements ou à la publication d'une nouvelle réglementation. Les enseignements relatifs à ces domaines identifiés feront l'objet d'une attention particulière dans le processus de RETEX.

4.1.2. ***Organisation du retour d'expérience au niveau des autorités qualifiées en sécurité des systèmes d'information et de la chaine de lutte informatique défensive.***

RO 7 : il est obligatoire que chaque AQ SSI et que la chaîne LID disposent d'une procédure formalisée décrivant le traitement du retour d'expérience en cybersécurité pour les unités sous leur autorité.

Cette formalisation (note d'organisation par exemple) aura vocation à être diffusée le plus largement possible. La DGSIC en sera destinataire à titre d'information.

RO 8 : il est obligatoire qu'un responsable central en charge du retour d'expérience en cybersécurité soit désigné au sein de chaque AQ SSI et au sein de la chaîne LID.

Ce responsable, appartenant au domaine de la cybersécurité, pourra être le point de contact privilégié pour toutes les questions relatives au RETEX, tant pour les entités relevant de son autorité que vers le niveau ministériel.

RO 9 : il est recommandé que chaque AQ SSI mette en place un ou plusieurs échelons locaux de traitement du RETEX.

Bien qu'aucune organisation particulière ne soit imposée, il est conseillé d'appliquer le principe de subsidiarité et de laisser à chaque échelon de responsabilité le soin de traiter le retour d'expérience des faits constatés localement. Seuls les faits dont l'importance ou la gravité nécessitent un traitement de plus haut niveau sont transmis aux échelons supérieurs.

À titre d'exemple, un échelon local peut être mis en place au niveau de l'officier de sécurité des systèmes d'information (OSSI) régional, pour les entités sous autorité de l'autorité qualifiée du chef d'état-major des armées (AQ CEMA), ou encore au niveau de l'OSSI d'un centre ou d'un site pour l'autorité qualifiée de la direction générale pour l'armement (AQ DGA). Dans tous les cas, le responsable du RETEX sera choisi parmi le personnel œuvrant dans le domaine de la cybersécurité.

RO 10 : il est obligatoire qu'une synthèse du RETEX traité soit réalisée par chaque AQ SSI et par la chaine LID et présentée en CS-RETEX.

Cette synthèse doit présenter une vue d'ensemble et une appréciation de situation sur les évènements survenus dans le domaine de la cybersécurité et les réponses apportées. Par ailleurs, certains évènements considérés comme significatifs y seront exposés de manière détaillée. Il peut s'agir d'enseignements pouvant intéresser les autres acteurs du ministère, ou, de manière systématique, les enseignements appartenant aux axes prioritaires définis par l'échelon ministériel (cf. règle RO 6).

Le format de la synthèse du RETEX est laissé à l'appréciation de chaque acteur. Néanmoins, elle devra faire apparaitre au minimum les points figurant ci-après.

Synthèse réalisée par l'AQ SSI:

- appréciation de situation sur la période écoulée ;

- nombre d'évènements ayant fait l'objet d'un retour d'expérience, et principales décisions afférentes ;

- enseignements issus des unités spécialisées sous responsabilité de l'AQ SSI. Il peut s'agir des équipes d'audit, des équipes de contrôle, des opérateurs, ou des évènements du domaine du chiffre ;

- enseignements relatifs aux exercices d'entraînement menés ;

- enseignements nécessitant une prise de décision de niveau ministériel.

Synthèse réalisée par la chaine LID :

- appréciation de situation sur la période écoulée ;

- analyse d'un ou plusieurs incidents significatifs et enseignements associés ;

- enseignements nécessitant une prise de décision de niveau ministériel.

RO 11 : il est recommandé que chaque AQ SSI mette en place un dispositif anonyme de recueil d'expérience en cybersécurité des utilisateurs.

Cette démarche, communément appelée « boîte à idées », met l'accent sur la nécessaire prise en compte du point de vue des utilisateurs qui sont au contact quotidien de la réalité. L'aspect anonyme doit permettre de favoriser la démarche de l'utilisateur, notamment lorsqu'il s'agit d'une anomalie constatée sans qu'un compte-rendu officiel ne soit rédigé.

Le dispositif peut s'inscrire dans une démarche plus générale d'innovation participative, et permet à la fois une reconnaissance des préoccupations de chacun, et une mobilisation de l'intelligence collective.

RO 12 : il est obligatoire que le processus de RETEX soit évoqué lors des séances de sensibilisation SSI du personnel.

Cette règle a pour objectif de présenter la nécessité du RETEX et son intérêt pour l'utilisateur. En particulier, la présentation de la « boîte à idées » pourra être réalisée ou rappelée à cette occasion.

*4.1.3. **Rôle des acteurs spécialisés dans le processus de retour d'expérience.***

Certaines unités ou organismes de cybersécurité du ministère de la défense occupent une place particulière dans le cadre du processus de retour d'expérience.

4.1.3.1. Équipes ministérielles d'audit.

Compte-tenu de la diversité des unités qu'ils sont amenés à rencontrer et des systèmes d'information évalués, les équipes d'audit SSI du ministère sont une source de retour d'expérience primordiale et ont de ce fait un rôle particulier au sein du processus RETEX.

RO 13 : il est obligatoire que chaque entité d'audit en SSI soumette une synthèse périodique du RETEX à destination de l'autorité qualifiée en SSI de rattachement.

La synthèse, rédigée sous format défini par chaque AQ SSI, a pour objectif de présenter les principaux faits marquants constatés au cours de leurs missions, en fournissant une analyse sommaire de leurs causes potentielles. À ce titre, elle pourra être réalisée sous forme d'une fiche RETEX rédigée avec le recueil des faits et l'identification des enseignements, accompagnée de proposition de décisions.

Il est important de mettre en évidence les points identiques et relevés sur des sites et des systèmes différents, ce qui renforce l'importance du constat. Un point particulier sera également réalisé dans le domaine des signaux parasites compromettants (SPC).

4.1.3.2. Équipe de contrôle de sécurité des systèmes d'information.

Au même titre que les équipes d'audit, le contrôle en SSI permet de dégager des enseignements pertinents dans le domaine de la cybersécurité grâce à la variété des unités visitées.

RO 14 : il est obligatoire que chaque équipe de contrôle en SSI soumette une synthèse périodique du RETEX à destination de l'autorité qualifiée en SSI de rattachement.

4.1.3.3. Gestion des autorités qualifiées en sécurité des systèmes d'information et utilisation du chiffre.

La spécificité et la sensibilité des évènements dans le domaine du chiffre et de la gestion des ACSSI imposent une analyse systématique identifiant clairement leurs causes et les mesures correctrices associées, y compris en cas de fausses alertes.

RO 15 : il est obligatoire qu'un retour d'expérience spécifique soit réalisé sur les évènements relatifs à la gestion des ACSSI ou de l'emploi du chiffre.

Une synthèse du retour d'expérience figurera dans la synthèse périodique des AQ SSI de rattachement.

4.1.3.4. Opérateurs.

Au contact direct des utilisateurs et de leurs préoccupations, l'opérateur dispose également d'une vision globale sur les réseaux dont il a la charge. Ainsi, il constitue une source d'information primordiale dans la démarche de retour d'expérience.

RO 16 : il est obligatoire que les opérateurs du ministère fournissent à l'AQ SSI de rattachement un retour d'expérience sur les principaux évènements constatés dans le domaine de la cybersécurité.

À titre d'exemple, à partir des demandes les plus fréquentes aux centres d'appel (SDK) sur des problèmes de cybersécurité, des enseignements pourront être dégagés et transmis à l'AQ SSI pour remédier aux causes identifiées. De même, les centres de gestion de la sécurité (SOC) des opérateurs identifieront des enseignements à partir des incidents traités.

4.1.3.5. Organismes de formation à la cybersécurité.

RO 17 : il est obligatoire que le processus de RETEX soit présenté au cours des stages d'adaptation ou des formations en cybersécurité.

Cette règle a pour objectif d'acculturer chaque acteur de la cybersécurité du ministère de la défense, et de lui enseigner la notion de « réflexe RETEX » lors d'un évènement.

4.2. **Processus de traitement du retour d'expérience en cybersécurité.**

Le retour d'expérience en cybersécurité suit un cycle comportant trois phases principales :

- la collecte ou le recueil des faits, qui consiste à rassembler le maximum d'éléments à la fois techniques et d'environnement pour décrire le plus finement possible la situation ;

- l'identification des enseignements, ayant pour objectif d'analyser et de déterminer les causes de l'évènement et de formuler des recommandations ou un plan d'actions correctif afin d'éviter une nouvelle occurrence des faits ou d'améliorer le niveau de sécurité ;

- la décision et la mise en œuvre, validant les propositions émises lors de la phase précédente au travers d'ordres ou de demandes particulières.

4.2.1. ***Le recueil des faits.***

RO 18 : il est recommandé que la procédure de collecte des faits soit initiée le plus rapidement possible après le début de l'évènement, et réalisée par un membre désigné au sein de l'équipe de gestion de l'évènement.

Une attente trop importante nuit en effet à la clarté et la précision des faits. Toutefois, il est évident que la priorité sera toujours donnée au traitement de l'évènement. En revanche, il faut avoir conscience que certaines traces pourront être utiles pour le processus de RETEX (cas des journaux d'évènements par exemple).

La collecte des faits nécessaires au RETEX étant une étape déterminante, elle devra être conduite par un responsable désigné et connu lors du traitement de l'évènement, en liaison avec l'échelon local de traitement du RETEX s'il existe.

RO 19 : il est obligatoire que la procédure de collecte des faits soit réalisée sous la forme d'une fiche pré-formatée.

Un exemple de fiche est fourni en annexe. Afin de faciliter le processus d'analyse ultérieur, il est souhaitable que chaque acteur du RETEX (AQ SSI et chaine LID) s'inspire de ce modèle en le complétant si besoin pour

l'adapter à ses spécificités.

RO 20 : il est obligatoire que les faits collectés soient identifiés à partir de mots clefs caractéristiques.

Ces mots-clefs ont pour objectif de faciliter la recherche lorsqu'il s'agit de déterminer si les faits ont déjà fait l'objet d'un retour d'expérience. Les mots-clefs seront choisis de manière à identifier rapidement le domaine concerné (exemples : incident, support amovible, code malveillant, équipement, formation, innovation, chiffre, réglementation, etc.). Le choix de ces mots est laissé à l'initiative du rédacteur, et pourront être modifiés par l'échelon central ou ministériel afin de regrouper les situations similaires.

RO 21 : il est déconseillé de faire figurer des éléments classifiés sur une fiche RETEX.

Cette règle a pour objectif de faciliter les échanges entre acteurs du retour d'expérience. À ce titre, il est le plus souvent possible de conserver la précision nécessaire dans la description des faits, avec pour objectif d'en tirer des enseignements, tout en décontextualisant suffisamment les faits.

4.2.2. ***L'identification des enseignements.***

RO 22 : il est obligatoire que l'identification des enseignements soit réalisée par un échelon spécialisé dans le RETEX.

Un enseignement est le résultat d'une analyse minutieuse des causes et effets de l'évènement, en prenant en compte l'ensemble des faits extérieurs (contexte, environnement, etc.). Selon la catégorie de l'évènement et sa gravité, l'identification des enseignements pourra être réalisée par l'échelon local ou l'échelon central, voire l'échelon ministériel du RETEX.

RO 23 : il est obligatoire que chaque enseignement soit classé au sein d'une ou plusieurs catégories caractéristiques de la cybersécurité.

Ces catégories, formant l'acronyme FORCIT, sont :

- formation : manque de compétences d'un acteur de l'évènement, pouvant aboutir à des évolutions des programmes de formation pour s'adapter à la réalité ;

- organisation : déficience dans le nombre de personnes affecté à un organisme ou dans la chaîne de responsabilité actuellement mise en place ;

- réglementation : cela peut être l'inapplicabilité d'un règlement dans un contexte particulier, ou au contraire l'absence de directive sur un domaine nouveau, une inadéquation constatée nécessitant une mise à jour, une proposition d'amélioration ;

- chiffre : enseignement relatif au domaine du chiffre (réseaux de chiffrement, gestion des ACSSI) ;

- infrastructure : enseignement relatif à l'environnement physique de l'évènement ;

- technique : évolutions de configurations matérielles ou logicielles.

Cette affectation permet de mobiliser éventuellement les acteurs du domaine concerné pour obtenir une expertise supplémentaire ou un avis avant décision de l'autorité.

RO 24 : il est recommandé que le responsable du retour d'expérience vérifie au préalable qu'un enseignement n'a pas déjà été identifié pour des faits similaires.

Cette règle permet de regrouper les enseignements relatifs à des faits récurrents (exemple : détection d'un même code malveillant par un antivirus). Dans ce cas, le responsable peut décider de reprendre l'enseignement existant tout en l'enrichissant de commentaires si nécessaire (exemple : les faits ont été

constaté à plusieurs reprises). Une mention sera apposée sur la fiche RETEX de l'évènement ainsi traité.

Au niveau local, cette vérification sera limitée à l'historique des évènements de l'organisme. Au niveau central, le responsable pourra consulter la base de données qui sera tenue à jour au niveau ministériel.

RO 25 : il est obligatoire que la phase d'identification des enseignements aboutisse à la formalisation d'un ou plusieurs axes d'amélioration.

Un axe d'amélioration est une proposition concrète visant à prendre en compte les enseignements identifiés. Il pourra s'agir d'une proposition de décision, ou d'un approfondissement du sujet au travers d'études complémentaires, auquel cas il pourra être proposé la création d'un groupe de travail spécifique.

4.2.3. ***La décision et la mise en œuvre.***

RO 26 : il est obligatoire que chaque fiche RETEX soit conclue par une décision ou un plan d'action.

Le niveau de décision est défini par chaque AQ SSI ou chaine LID en fonction de la portée des axes d'amélioration définis lors de la phase précédente.

Il est à noter que le classement sans suite d'une fiche RETEX constitue une décision de commandement à part entière.

RO 27 : il est obligatoire de s'assurer de la bonne mise en œuvre des décisions prises dans le cadre du processus RETEX.

Le contrôle s'effectue à la fois sur l'application effective des ordres jusqu'aux plus bas échelons, ainsi que sur la pertinence des actions correctrices décidées. Il appartient à l'autorité signataire des actions de procéder à cette vérification à l'aide d'unités organiquement placées sous son autorité (équipe d'audit ou de contrôle par exemple). Les impacts de certaines décisions pourront figurer au titre des domaines prioritaires identifiés annuellement par l'échelon ministériel.

Pour le ministre de la défense et par délégation :

L'ingénieur général hors classe de l'armement,
directeur général des systèmes d'information et de communication,

Marc LECLÈRE.

---

(1) n.i. BO.

ANNEXE.

MODÈLE DE FICHE RETOUR D'EXPÉRIENCE.

MODELE DE FICHE RETEX

<table>
<tr><th colspan="6">FICHE DE RETOUR D’EXPERIENCE EN CYBERSECURITE</th></tr>
<tr><td rowspan="6">PHASE 1 :
COLLECTE DES FAITS</td><td colspan="5">Numéro d’ordre dans l’année :</td></tr>
<tr><td colspan="2">Rédacteur :</td><td colspan="3">Date de rédaction :</td></tr>
<tr><td colspan="2">Niveau de sensibilité/ classification :</td><td>NP</td><td>DR</td><td>CD</td></tr>
<tr><td>Sujet général :</td><td colspan="4"></td></tr>
<tr><td>Faits</td><td colspan="4">Indiquer dans ce cartouche la chronologie factuelle de l’évènement, avec les actions immédiates prises si elles sont une source d’enseignements.</td></tr>
<tr><td>mots-clefs</td><td colspan="4"></td></tr>
<tr><td colspan="6"></td></tr>
<tr><td rowspan="4">PHASE 2 :
IDENTIFICATION DES ENSEIGNEMENTS</td><td rowspan="2">Enseignements</td><td colspan="4">Les enseignements seront regroupés par domaine caractéristique de cybersécurité (FORCIT)</td></tr>
<tr><td colspan="2">Enseignement nouveau</td><td colspan="2">Enseignement déjà identifié
Référence de la fiche :</td></tr>
<tr><td>Axes d’amélioration</td><td colspan="4"></td></tr>
<tr><td>Analyse réalisée par</td><td colspan="2"></td><td>Date</td><td></td></tr>
<tr><td colspan="6"></td></tr>
<tr><td rowspan="2">PHASE 3 : DECISION</td><td>Actions décidées ou avis complémentaires demandés</td><td colspan="4"></td></tr>
<tr><td>Autorité signataire</td><td colspan="2"></td><td>Date</td><td></td></tr>
</table>