*BULLETIN OFFICIEL DES ARMEES*

**Edition Chronologique n°44 du 21 octobre 2011**

PARTIE PERMANENTE
Administration Centrale

Texte n°1

**DIRECTIVE N° 17/DEF/DGSIC**
portant sur l'identification et le suivi des systèmes critiques.

Du *6 juillet 2011*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

**DIRECTIVE N° 17/DEF/DGSIC portant sur l'identification et le suivi des systèmes critiques.**

*Du 6 juillet 2011*

NOR D E F E 1 1 5 1 3 4 4 X

---

*Pièce(s) Jointe(s) :*

Deux annexes.

*Classement dans l'édition méthodique :* BOEM 160.1

*Référence de publication :* BOC N°44 du 21 octobre 2011, texte 1.

---

SOMMAIRE



ANNEXE(S)

# 1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

## 1.1. **Présentation.**

La présente directive définit la méthode à mettre en œuvre par les organismes du ministère de la défense en matière de systèmes critiques (cf. annexe I.). Elle définit les critères d'identification et de caractérisation de ces systèmes, et les dispositions de suivi de leur état de préparation.

Cette directive fait partie du *corpus* doctrinal dans le domaine de la gestion du risque.

Elle est dérivée de la méthode pour identifier et caractériser les systèmes vitaux (SYVIT) réalisée par le bureau assistance et conseil de l'agence nationale de la sécurité des systèmes d'information (ANSSI).

## 1.2. **Champ et modalités d'application.**

Conformément aux règles de l'organisation générale de la défense, le gouvernement et chaque ministre concerné doivent définir, par secteur d'activité d'importance vitale, des mesures planifiées et graduées de vigilance, de prévention, de protection et de réaction contre toute menace, notamment à caractère terroriste. Parmi les mesures nécessaires à la prise en compte des menaces stratégiques ou terroristes, le plan gouvernemental de vigilance, de prévention et de protection face aux menaces d'actions terroristes « Vigipirate » demande aux ministères d'effectuer une cartographie de leurs éléments vitaux dans le cadre de l'identification et de la gestion des risques des sécurités des systèmes de sécurité (SSI).

Cette directive est destinée aux autorités qualifiées (cf. annexe I.) et aux autorités d'emploi (cf. annexe I.) des systèmes critiques qui seront identifiés.

## 1.3. **Niveaux de préconisation.**

Les règles définies dans ce document ont différents niveaux de préconisation et sont conformes au référentiel général d'intéropérabilité (RGI) et à la RFC2119 :

- 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.

## 1.4. **Gestion des dérogations.**

Les dérogations envisagées par les autorités qualifiées doivent être instruites (circonstances, durée, justification).

La direction générale des systèmes d'information et de communication (DGSIC) en est informée pour les règles recommandées et déconseillées.

Une approbation formelle de la DGSIC est demandée pour les règles obligatoires et interdites.

2. CADRE DOCUMENTAIRE.

2.1. **Documents applicables.**

IGI 1300 : instruction générale interministérielle n° 1300/SGDN/PSE/SSD du 23 juillet 2010 (1) sur la protection du secret de la défense nationale.
http://www.ssi.gouv.fr/IMG/pdf/igi1300.pdf

PSSI : instruction n° 133/DEF/SEC/DIR/SIC du 18 mars 2002 relative à la politique de sécurité des systèmes d'information du ministère de la défense.
http://www.ssi.defense.gouv.fr/ dirsic/textes/mis sec dir sic/secur sys info/textes base/ref regl/textes ministere/politique generale/im n 133 def sec.dir.sic du 18 mars 2002.pdf

SYVIT : méthode pour identifier et caractériser les systèmes vitaux du 5 décembre 2007, réalisée par l'ANSSI.
http://www.ssi.defense.gouv.fr/ dirsic/textes/mis sec dir sic/secur sys info/textes base/ref regl/textes nationaux europeens/textes intermin guides/SYVIT-Methode-2007-12-05.pdf

IM2004 : instruction n° 2004/DEF/DGSIC du 14 décembre 2009 relative à la fonction d'administrateur de systèmes d'information et de communication au sein du ministère de la défense.
http://www.dgsic.defense.gouv.fr/IMG/pdf/20091215_IM_administrateurs_V1.6.pdf

GM005 : guide ministériel n° 5 du 10 décembre 2010 (1) relatif aux dispositions pratiques et techniques de continuité informatique.
http:www.dgsic.defense.gouv.fr/IMG/pdf/20101210 Guide dispositions pratiques techniques continuite informatique vla.pdf

GM006 : guide ministériel n° 6 du 27 avril 2011 (1) relatif à la valorisation des données de caractérisation d'un système d'information.

RFC2119 : mots-clés pour niveaux d'obligation.

2.2. **Sites de référence.**

Site DGSIC : site DGSIC à l'adresse intradef : www.dgsic.defense.gouv.fr

Sites SSI :

- site des sécurités des systèmes d'information (SSI) à l'adresse intradef : www.ssi.defense.gouv.fr ;

- site SSI de l'agence nationale de sécurité des systèmes d'information à l'adresse internet : www.ssi.gouv.fr

Documentation SSI : http://www.ssi.defense.gouv.fr/ dirsic/textes/mis sec dir sic/secur sys info/textes base/ref regl/ref regl.htm

3. DOMAINE COUVERT ET EMPLOI.

La directive vise à définir les principes et les procédures à suivre pour identifier et caractériser les systèmes critiques relevant des autorités qualifiées du ministère de la défense, des établissements ou organismes sous tutelle.

3.1. **Principes.**

Un système d'information est dit critique dès lors qu'il remplit ou supporte une ou plusieurs mission(s) essentielle(s) du ministère.

Les autorités métiers décident du caractère critique et du niveau de criticité des systèmes qu'elles utilisent et évaluent les impacts possibles en cas d'atteinte aux besoins de sécurité (cf. annexe I.). Les systèmes critiques doivent faire l'objet d'une attention particulière et bénéficier de mesures de sécurité adaptées pour assurer leur protection et leur continuité.

La DGSIC tient à jour un répertoire des systèmes critiques et de leur état de préparation et le met à la disposition du fonctionnaire de sécurité des systèmes d'information (FSSI), des autorités du ministère et des responsables des sécurités des systèmes d'information [(RSSI) (cf. annexe I.)] des systèmes critiques identifiés afin d'en permettre la tenue à jour.

Le premier objectif est de cartographier les systèmes critiques du ministère, de les caractériser et de maintenir à jour la cartographie ainsi réalisée.

Il s'agit ensuite d'établir des plans d'action et calendriers de progrès vers les objectifs de sécurité retenus et de suivre leur application.

Il s'agit d'une démarche d'amélioration continue et il est donc impératif de réviser régulièrement les résultats. Pour les systèmes ayant fait l'objet d'une démarche de sécurisation, une partie de la démarche a déjà été réalisée et les conclusions peuvent être directement reprises.

3.2. **Périmètre et limites.**

La directive est applicable aux systèmes utilisés par le ministère de la défense et des anciens combattants, ainsi que par les établissements ou organismes sous tutelle. Elle fait partie du référentiel documentaire sur lequel s'appuie la politique de sécurité de leurs SI.

La directive établit des règles communes à tous les systèmes indépendamment du fait qu'ils soient nationaux, de l'Organisation du traité de l'Atlantique Nord (OTAN), de l'Union européenne (UE), de coalition ou autre.

4. LES RÈGLES.

La directive est déclinée sous 2 angles : organisationnel (RO) et technique (RT). Les règles sont numérotées séquentiellement par catégorie.

RO 1 : il est obligatoire que chaque autorité qualifiée fasse mener une démarche pour identifier et caractériser les systèmes critiques de son autorité.

RO 2 : il est obligatoire que chaque autorité qualifiée définisse la liste des entités placées sous son autorité qui devront appliquer la méthode.

À noter : la précision à laquelle descendra cette liste est laissée à la libre appréciation des autorités qualifiées. Par exemple, une entité de niveau n peut désigner une entité de niveau n-1.

RO 3 : il est obligatoire que les autorités qualifiées mandatent un responsable appartenant aux entités qu'elles auront identifiées pour mener une démarche d'identification et de caractérisation des systèmes critiques employés sous leur autorité.

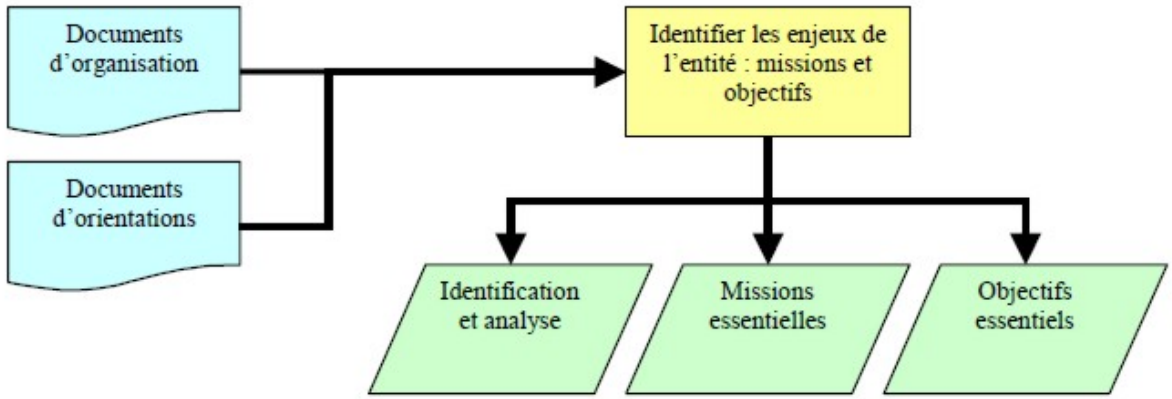
RO 4 : il est obligatoire que les autorités qualifiées mandatent un ou plusieurs responsables pour mener une démarche permettant d'identifier et de caractériser les systèmes critiques employés par les établissements ou organismes sous tutelle (2).

4.1. **L’identification des systèmes critiques.**

L'identification des enjeux d'une entité.

Cette étape a pour but de décrire et de délimiter le périmètre de l'étude. Une analyse succincte de l'entité ou du service considéré est réalisée, et ses missions essentielles et objectifs essentiels (enjeux) participant ou supportant les missions essentielles du ministère sont identifiés.

Identification des enjeux.




RO 5 : il est obligatoire, si elle n'a pas été conduite par ailleurs, que chaque responsable mandaté mène une démarche pour identifier les missions et objectifs essentiels de son entité, remplissant ou supportant les missions essentielles du ministère.

À noter : les missions et objectifs essentiels d'une entité sont constitués par la déclinaison des missions essentielles du ministère au niveau de l'entité. Il est possible qu'une entité n'en possède pas.

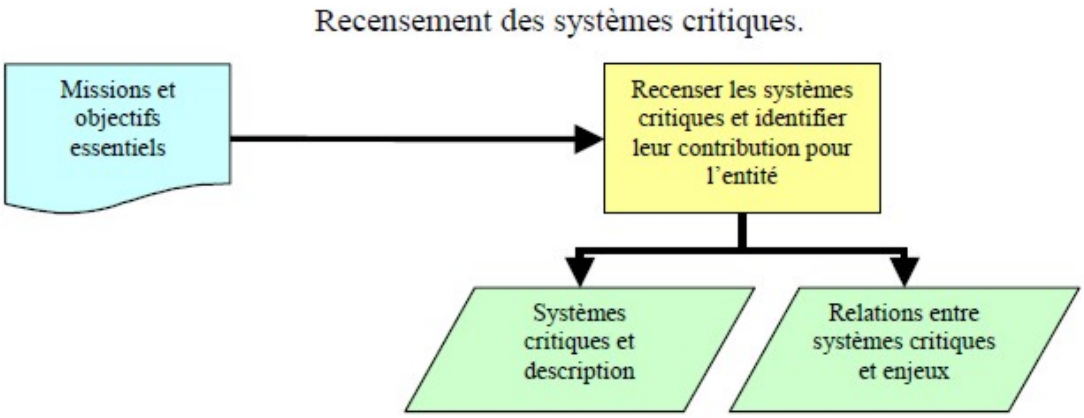
À noter : les missions et objectifs essentiels sont extraits des documents d'organisation (décrets relatifs à l'entité, directive de fonctionnement opérationnelle, etc.) et d'orientation (schéma directeur, notes d'orientation, etc.).

RO 6 : il est obligatoire que ces missions et objectifs essentiels soient validés par l'autorité d'emploi de l'entité.

RO 7 : il est obligatoire que les missions et objectifs essentiels de chaque entité soient communiqués à l'autorité qualifiée, ou que l'autorité d'emploi de l'entité atteste à l'autorité qualifiée ne pas avoir de mission ou d'objectif essentiel supportant ou participant aux missions essentielles du ministère.

Le recensement des systèmes critiques.

Cette étape a pour but de justifier de l'importance des systèmes dans l'accomplissement des missions et objectifs essentiels de l'entité. Les données en entrée sont celles obtenues précédemment (missions et objectifs essentiels).




RO 8 : il est obligatoire que les responsables mandatés identifient les systèmes sur lesquels reposent les missions et objectifs essentiels de leur entité.

À noter : un système est jugé critique si sa défaillance empêche la réalisation d'une mission essentielle ou d'un objectif essentiel de l'entité. Une démarche cohérente consiste à identifier les applications ou les informations particulièrement sensibles, et donc les réseaux qui les portent. Il s'agit notamment de celles dont la destruction, l'altération ou la compromission est de nature à nuire aux missions essentielles du ministère.

À noter : il convient de ne retenir que les systèmes véritablement critiques pour l'entité, et non de recenser tous les systèmes ou toutes les applications.

À noter : relier un système critique à une mission ou un objectif essentiel permet de vérifier qu'il est bien critique ou qu'il ne manque pas de mission ou d'objectif.

RO 9 : il est obligatoire de préciser en quoi chaque système est critique vis-à-vis des missions ou des objectifs essentiels.

RO 10 : il est obligatoire que les responsables mandatés identifient l'autorité d'emploi de ces systèmes.

RO 11 : il est obligatoire que les responsables mandatés formalisent et communiquent à leur autorité qualifiée les relations entre les systèmes critiques et les missions et objectifs essentiels de leur entité.

RO 12 : il est obligatoire que les autorités qualifiées informent l'autorité qualifiée d'un système jugé critique lors qu'elle n'en est pas elle-même responsable.

RO 13 : il est obligatoire que les autorités qualifiées ou leurs représentants communiquent un bilan des relations entre les systèmes critiques et les missions essentielles et objectifs essentiels de leur organisme au FSSI et au comité directeur des intranets.

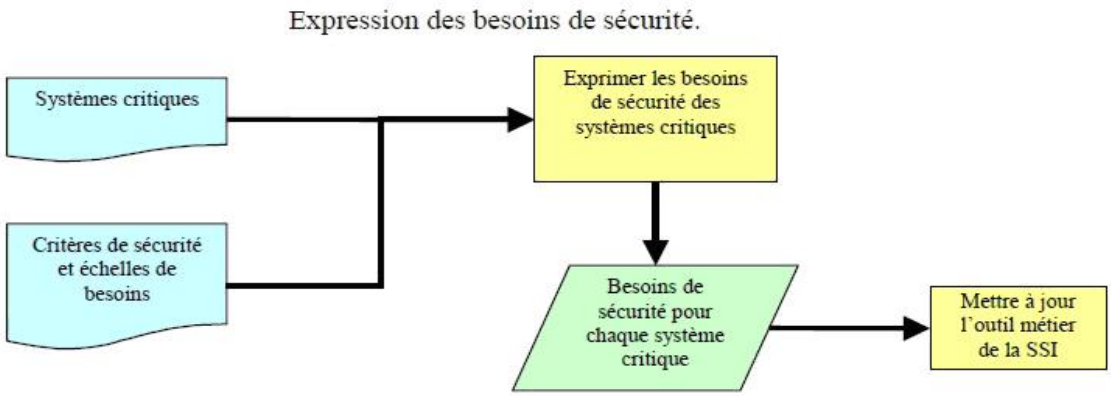
À noter : les résultats de cette étape peuvent être renseignés dans un tableau ayant la forme suivante.

Tableau r&eacu

4.2. **Caractérisation des systèmes critiques.**

L'expression des besoins de sécurité.

Cette étape a pour but de fixer les objectifs mesurables des systèmes critiques, en les caractérisant en termes de disponibilité (cf. annexe I.), d'intégrité (cf. annexe I.), de confidentialité (cf. annexe I.), et de perte de données maximale autorisée [(PDMA) (cf. annexe I.)]. La PDMA est exprimée en jours et en heures de travail perdues.




RT 2 : il est obligatoire, d'utiliser les échelles de besoins des critères de sécurité « disponibilité », « intégrité » et « confidentialité » issues du guide relatif à la valorisation des données de caractérisation d'un système d'information (GM006).

RT 3 : il est obligatoire, d'utiliser l'échelle suivante pour la perte de données maximale autorisée (PMDA) :

| NIVEAUX DE L'ÉCHELLE. | PERTE DE DONNÉES MAXIMALE AUTORISÉE. | DESCRIPTION. |
|---|---|---|
| TOLÉRABLE. | PDMA > 2 jours. | Toute perte de données consécutive à une indisponibilité de plus de deux jours du système est considérée comme sans impact sur le fonctionnement des services du ministère de la défense. |
| GÊNANTE. | 6 h < PDMA < 2 jours. | Toute perte de données consécutive à une indisponibilité du système est considérée comme gênante pour le fonctionnement des services du ministère de la défense et par voie de conséquence de l'État. |
| GRAVE. | 1 h < PDMA < 6 h. | Toute perte de données consécutive à une indisponibilité du système est considérée comme grave pour le fonctionnement des services du ministère de la défense et par voie de conséquence de l'État. |
| INACCEPTABLE. | PDMA < 1 h. | Toute perte de données consécutive à une indisponibilité du système est considérée comme inacceptable pour le fonctionnement des services du ministère de la défense et par voie de conséquence de l'État. |

RO 14 : il est obligatoire que les autorités d'emplois expriment les besoins de sécurité sur chaque système critique utilisé, en s'appuyant éventuellement sur la FEROS.

RO 15 : il est obligatoire d'exprimer les besoins de sécurité vis-à-vis de chaque mission ou objectif essentiel.

RT 4 : il est obligatoire de décliner les besoins de sécurité en termes de confidentialité, de disponibilité, d'intégrité et de perte de données maximale autorisée.

À noter : le besoin de sécurité du système est égal au maximum des besoins de chaque mission pour les critères de disponibilité, d'intégrité, de confidentialité et de PDMA.

À noter : si les besoins de sécurité varient dans le temps, on s'intéressera à la situation qui requiert les besoins les plus importants.

RO 16 : il est obligatoire de mettre à jour l'outil métier de la SSI [3] avec les besoins de sécurité des systèmes critiques.

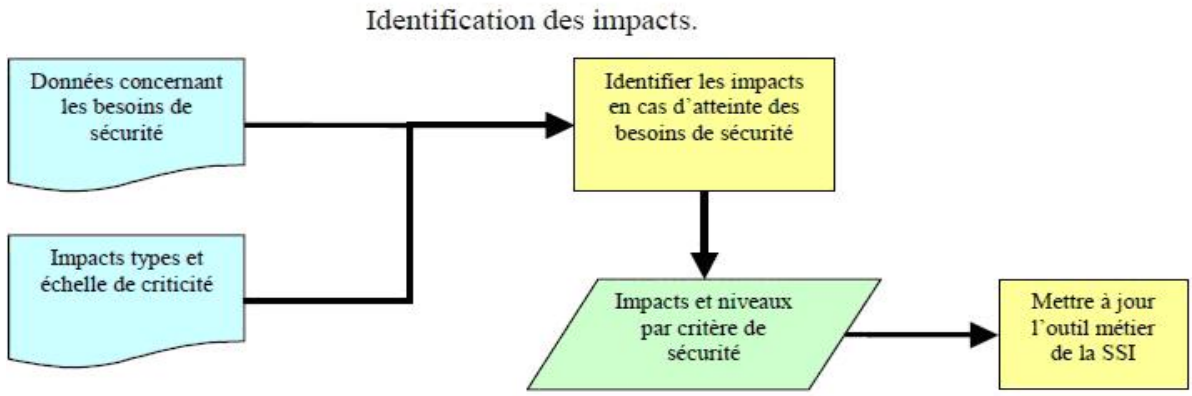
À noter : pour chaque système critique, les résultats de cette étape peuvent être consignés dans un tableau ayant la forme suivante.

Tableau récapitulatif des besoins de sécurité des systèmes critiques d'une entité.

| SYSTÉME CRITIQUE NOM DU SYSTEME. | NIVEAUX. | MISSION ESSENTIELLE 1. | MISSION ESSENTIELLE 2. | OBJECTIF ESSENTIEL 1. | ... | BESOIN MAX. |
|---|---|---|---|---|---|---|
| DISPONIBILITÉ. | Faible (24h HO). | | | | | Forte (1h H24). |
| | Standard (6h HO). | | | | | |
| | Élevée (6h H24). | | x | x | | |
| | Forte (1h H24). | x | | | | |
| INTÉGRITÉ. | Altérable. | | | | | Maîtrisé. |
| | Détectable. | | x | x | | |
| | Maîtrisé. | x | | | | |
| | Intègre. | | | | | |
| CONFIDENTIALITÉ. | Non protégé. | | | | | Secret. |
| | Restreint. | | x | x | | |
| | Confidentiel. | | | | | |
| | Secret. | x | | | | |
| | Très secret. | | | | | |
| PDMA. | > 2 jours. | | | x | | < 1h. |
| | 6h à 2 jours. | | x | | | |
| | 1h à 6h. | | | | | |
| | < 1h. | x | | | | |

L'identification des impacts.

Cette étape a pour but d'estimer les conséquences d'incidents ou de sinistres. Ainsi, pour chaque système critique, et chaque type d'impact, le niveau de criticité doit être estimé.




RT 5 : il est recommandé d'utiliser les types d'impacts suivants :

- impacts sur les missions ;
- impact sur la sécurité de l'État ;
- impact sur la sécurité des personnes ;
- impacts financiers ;
- impact juridiques ;
- impacts sur l'image ;
- impact sur l'environnement ;
- impact sur les tiers.

RO 17 : il est obligatoire que les autorités d'emploi identifient les impacts en cas d'atteinte des besoins de sécurité, en s'appuyant éventuellement sur la FEROS.

RO 18 : il est obligatoire que les autorités d'emploi évaluent le niveau potentiel des impacts.

RT 6 : il est obligatoire, pour évaluer la criticité d'un impact, d'utiliser l'échelle criticité issue du guide relatif à la valorisation des données de caractérisation d'un système d'information (GM006).

RT 7 : il est obligatoire de mettre à jour l'outil métier de la SSI avec l'identification des impacts potentiels et de leur niveau sur les systèmes critiques.

À noter : un système dont les impacts sont tous limités ou nuls ne devrait pas être jugé comme critique.

RO 19 : il est obligatoire de communiquer les besoins de sécurité et les impacts potentiels en cas d'atteinte de ces besoins aux autorités qualifiées.

RO 20 : il est obligatoire que les autorités qualifiées (AQ) communiquent au FSSI un bilan des besoins de sécurité et des impacts potentiels en cas d'atteinte des besoins de sécurité des systèmes critiques.

À noter : pour chaque système critique, les résultats de cette étape peuvent être consignés dans un tableau ayant la forme de celui présenté au point 4.3.

4.3. **Caractérisation des systèmes critiques.**

RO 21 : il est obligatoire que pour chaque système critique, un plan de continuité informatique (PCI) soit rédigé en liaison avec l'autorité d'exploitation (cf. annexe I.).

RO 22 : il est obligatoire que ce PCI soit validé par l'autorité d'emploi.

RO 23 : il est obligatoire de mettre en place des règles d'administration strictes :

- exploitation des journaux ;
- respect des différents types d'administrateurs - sécurité, réseau, système ;
- ...

RO 24 : il est interdit de mener une procédure d'homologation simplifiée pour ces systèmes.

RO 25 : il est recommandé de réviser au moins annuellement les résultats afin de prendre en compte les évolutions du contexte (nouveaux objectifs, systèmes, besoins et impacts, nouvelles mission, menaces, etc.) et les retours d'expérience.

RO 26 : il est obligatoire, pour les nouveaux systèmes, d'identifier leur criticité potentielle en phase d'initialisation du projet ou du programme.

RO 27 : il est interdit de prononcer une homologation pour une durée supérieure à 2 ans pour un système critique.

Tableau récapitulatif des impacts.

| SYSTÉMES VITAUX. | CRITÈRES DE SECURITÉ. | BESOINS DE SÉCURITÉ. | EXEMPLES D'IMPACTS POSSIBLE EN CAS D'ATTEINTE DU BESOIN DE SÉCURITÉ. | | | | | | | | ESTIMATION DU NIVEAU DES IMPACTS. |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | SUR LES MISSIONS. | SUR LA SÉCURITÉ DE L'ÉTAT. | SUR LA SÉCURITÉ PERSONNES. | FINANCIERS. | JURIDIQUES. | SUR L'IMAGE. | SUR L'ENVIRONNEMENT. | SUR LES TIERS. | |
| SYSTÈME A. | Disponibilité. | Élevée (6h H 24) | Frein à la conduite de crise. | Atteinte à l'exercice de l'autorité de l'État. | Perte de maîtrise d'une crise sanitaire. | | | Le ministère est ridiculisé par les médias. | | | Critique. |
| | Intégrité. | Intègre. | Conduite de crise faussée. | Mauvaise posture de défense. | Envoi de faux ordres. | | | Perte de fiabilité du service. | | | Critique. |
| | Confidentialité. | Secret. | La protection des données n'est plus assurée. | Fuite de données classifiées. | | | Procédure pénale engagée. | Un document clasifié est diffusé sur Internet. | | | Critique. |
| | PDMA. | < 1h | Des données de missions sont perdues. | | | | | | | | Critique. |
| SYSTÈME B. | Disponibilité. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. |
| | Intégrité. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. |
| | Confidentialité. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. |
| | PDMA. | Etc. | Etc. | Etc | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. | Etc. |

Pour le ministre de la défense et des anciens combattants et par délégation :

*L'amiral,*
*directeur général des systèmes d'information et de communication,*

Christian PÉNILLARD.

---

(1) n.i. BO.

(2) Par exemple l'état-major de la marine devra désigner un responsable de la démarche au sein du service hydrographique et océanographique de la marine (SHOM).

(3) L'outil métier de la SSI est le tableau de bord des homologations de la sécurité des systèmes d'informations (TBHSSI). Ce dernier devrait être remplacé par PROMÉTEC.

ANNEXE I.

## GLOSSAIRE ET ACRONYMES.

Autorité d'emploi : autorité qui est à l'origine du besoin du système d'information (SI). Elle est également responsable de la mise en œuvre du SI. C'est l'autorité d'emploi, qui après avoir défini les finalités du traitement en pilote l'emploi et les évolutions. Elle est le garant de la bonne utilisation du SI.

Autorité d'exploitation : autorité qui assure les fonctions techniques d'exploitation du système d'information [exemple : la direction interarmées des réseaux d'infrastructures et des systèmes d'information (DIRISI)].

Autorité qualifiée en matière de SSI : responsable de la sécurité des systèmes d'information dans les administrations centrales et les services déconcentrés de l'État, dans les établissements publics, placé sous l'autorité d'un ministre ainsi que dans les organismes et établissements relevant de ses attributions.

Besoin de sécurité : définition précise et non ambigüe des niveaux correspondant aux critères de sécurité (disponibilité, confidentialité, intégrité, preuve, etc.) qu'il convient d'assurer à un élément essentiel.

Confidentialité : caractère réservé d'une information dont l'accès est limité aux seules personnes admises à la connaître pour les besoins du service.

Disponibilité : aptitude du système à remplir une fonction dans des conditions définies d'horaires, de délais et de performances.

Information : tout renseignement ou tout élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, à un enregistrement ou à un traitement.

Information ou support classifié : procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier présentant un caractère de secret de la défense nationale [art. 413-9. du code pénal (1)].

Information sensible : désigne une information dont la confidentialité, la disponibilité et l'intégrité ne procèdent pas du secret de la défense nationale tel que défini par les articles 413-9. à 413-12. du code pénal (1). Une information sensible est néanmoins protégée par des dispositions telles que l'obligation de discrétion professionnelle, le secret professionnel, les textes sur les données à caractère personnel et les obligations contractuelles.

Intégrité : garantie que le système et les informations traitées ne sont modifiés que par une action volontaire et légitime. Lorsque l'information est échangée, l'intégrité s'étend à l'authentification du message, c'est-à-dire à la garantie de son origine et de sa destination.

Objectif de sécurité : expression de la décision de traiter un risque selon des modalités prescrites. On distingue notamment la réduction, le transfert (partage des pertes), le refus (changements structurels pour éviter une situation à risque) et la prise de risque.

Perte de données maximale autorisée : durée au-delà de laquelle la perte des données traitées par un système ne permet plus de remplir une mission.

Programme métier au profit des équipes de cybersécurité (PROMÉTEC) : dénomination retenue pour la version 2 de TBHSSI (voir TBHSSI).

Responsable SSI : personne chargée de faire appliquer la politique SSI interne du système, en conformité avec la politique SSI du ministère.

Système critique : un système d'information est dit critique dès lors qu'il remplit ou supporte une ou plusieurs missions(s) essentielles du ministère (connaissance et anticipation, prévention, dissuasion, protection et intervention).

Système d'information (SI) : ensemble des moyens humains et matériels ayant pour finalité d'élaborer, de traiter, de stocker, d'acheminer, de présenter ou de détruire des informations.

Tableau de bord des homologations SSI (TBHSSI) : outil de suivi de la démarche de sécurisation d'un système d'information.

ANNEXE II.

**PROCESSUS ET CYCLE DE VIE.**