MINISTÈRE
DE L'AGRICULTURE,
DE L'AGRO-ALIMENTAIRE
ET DE LA SOUVERAINETÉ
ALIMENTAIRE

Liberté
Égalité
Fraternité

Service de la Statistique et de la Prospective

Détail des critères et niveaux d'expression des besoins de sécurité

Le MAASA a standardisé l'expression des besoins de sécurité comme suit :

QUEL EST LE BESOIN DE DISPONIBILITE DU SYSTEME CIBLE ?

AUCUN (D0)	Ce niveau traduit un délai maximal d'interruption autorisée illimité.
FAIBLE (D1)	Ce niveau traduit un délai maximal d'interruption autorisée entre une semaine et un mois.
MOYEN (D2)	Ce niveau traduit un délai maximal d'interruption autorisée de 5 jours consécutifs ouvrés.
FORT (D3)	Ce niveau traduit un délai maximal d'interruption autorisée de 2 jours consécutifs ouvrés.
TRES FORT (D4)	Ce niveau traduit un délai maximal d'interruption autorisée de 8 heures consécutives ouvrées.
VITAL (D5)	Ce niveau traduit une tolérance inférieure à 4h.

QUEL EST LE BESOIN D'INTEGRITE DES INFORMATIONS GEREES ?

AUCUN (I0)	Ce niveau traduit qu'une perte ou modification non prévue, volontaire ou non volontaire, n'affecte en rien les activités d'un service ou d'une direction du ministère.
FAIBLE (I1)	L'exactitude des informations est avérée mais sans garantie particulière d'exhaustivité. Une sauvegarde mensuelle suffit à la récupération des données perdues. La modification illicite des informations traitées ne doit

	pas provoquer de gêne significative pour un service ou direction du ministère. Le contrôle visuel est suffisant pour détecter toute modification illicite.
MOYEN (I2)	L'exactitude des informations est avérée et garantie par un scellement. L'authenticité des transactions est avérée mais sans garantie particulière d'exhaustivité. Une sauvegarde hebdomadaire suffit à la récupération des données perdues. La modification illicite des informations traitées ne doit pas provoquer de gêne significative pour un service ou direction critique du ministère. Le contrôle d'intégrité est automatique et porte sur quelques éléments clés d'un traitement.
FORT (I3)	L'exactitude des informations est garantie par dispositif de scellement protégé. L'authenticité des transactions est garantie par scellement sur toutes les transactions. Une sauvegarde quotidienne suffit à la récupération des données perdues. La modification illicite n'est pas tolérée et doit être détectée sous 24H.
VITAL (I4)	L'exactitude des informations et l'authenticité des transactions est garantie par dispositif de scellement protégé sur l'ensemble des traitements. La modification illicite n'est pas tolérée et doit être détectée le plus rapidement possible.

QUEL EST LE BESOIN DE CONFIDENTIALITE DES INFORMATIONS GEREES ?

AUCUN (C0)	Ce niveau traduit que la diffusion d'une information dans le domaine public n'affecte en rien les activités d'un service, d'une direction du ministère ou le service public en général. Il s'agit en particulier des informations publiées sur les sites Internet institutionnels du ministère.
RESERVE INTERNE (C1)	Ce niveau traduit que la diffusion est seulement possible en interne du ministère tout service et direction confondus.
RESTREINT (C2)	Ce niveau restreint la diffusion d'information à une direction ou un service concerné ou projet transverse. Un directeur ou chef de service non concerné peut avoir accès à ce niveau de connaissance sans habilitation particulière.
CONFIDENTIEL (C3)	Ce niveau restreint la diffusion d'informations sensibles telles que des données nominatives du personnel ou d'usagers aux seuls personnels ayant le droit d'en connaître. Ces personnels doivent être listés nominativement. Un directeur ou chef de service non concerné ne

	peut pas avoir accès à ce niveau de connaissance sans habilitation particulière.
TRES CONFIDENTIEL (C4)	Ce niveau restreint la diffusion d'information à quelques agents pour un sujet donné. Ce niveau d'information ne devrait sortir en aucun cas du ministère.

QUEL EST LE BESOIN DE PREUVE OPPOSABLE VIA A VIS DES INFORMATIONS GEREES ?

AUCUN (P0)	Ce niveau traduit que l'absence de toute trace sur les systèmes ou applications n'affectent en rien les activités d'un service ou d'une direction du ministère. Le besoin de preuve des opérations ou des transactions effectuées sur le système est nul.
FAIBLE (P1)	Ce niveau traduit un besoin de journalisation standard des principaux événements d'un système ou d'une application. L'élément de preuve est suffisant, il ne sera pas nécessaire de l'opposer dans le cadre d'une procédure en contentieux.
MOYEN (P2)	Ce niveau traduit un besoin de journalisation systématique des accès et des entrées-sorties de données d'un système ou d'une application. L'élément de preuve est suffisant, il ne sera pas nécessaire de l'opposer dans le cadre d'une procédure en contentieux.
IMPORTANT (P3)	Ce niveau traduit la nécessité une journalisation des événements systèmes ou applicatifs dont l'intégrité des journaux est garantie. L'élément de preuve doit pouvoir être produit lors d'une procédure en contentieux.
VITAL (P4)	Ce niveau garantit un niveau de preuve opposable sur les événements système ou applicatifs.