PREMIER MINISTRE

VIGIPIRATE

PARTIE PUBLIQUE

OBJECTIFS DE CYBERSÉCURITÉ

Édition du 27 février 2014

Introduction

*Le présent document est principalement destiné aux collectivités territoriales et aux opérateurs non-OIV * dans le cadre du plan VIGIPIRATE 2014. Il expose les objectifs de cybersécurité et les recommandations à respecter pour sécuriser les systèmes d'information d'une entité. Ces objectifs sont organisés selon sept familles d'activités propres à la sécurité des systèmes d'information : la gouvernance, la maîtrise des risques, la maîtrise des systèmes, la protection des systèmes, la gestion des incidents, l'évaluation et la relation avec les autorités. Chaque objectif est décliné suivant trois niveaux hiérarchiques (famille, sous-famille et rubrique).*

** OIV : opérateur d'importance vitale*

1 / PILOTER LA GOUVERNANCE DE LA CYBERSÉCURITÉ

FINALITÉ : l'entité traite au niveau stratégique la protection et la défense de ses systèmes sensibles.

RECOMMANDATION : une gouvernance de la sécurité est mise en place. Cette gouvernance doit permettre de définir une stratégie de sécurité validée au plus haut niveau de l'entité, de piloter la sécurité dans toute l'entité et de prendre en compte les aspects non techniques de la sécurité : communication, ressources humaines et aspects juridiques.

1.1 / DÉFINIR UNE STRATÉGIE DE LA CYBERSÉCURITÉ

■ **FINALITÉ : la direction de l'entité définit et pilote la stratégie cybersécurité de l'entité.**

☐ *RECOMMANDATION : la direction de l'entité s'engage à prendre en compte l'ensemble des enjeux de la cybersécurité.*

1.1.1 / Prendre en compte la cybersécurité au plus haut niveau

■ **FINALITÉ : les objectifs de cybersécurité et les risques sont portés et arbitrés au plus haut niveau de décision de l'entité.**

☐ *RECOMMANDATION : le responsable de la sécurité des systèmes d'information (RSSI) rend compte directement à la direction de l'entité, de manière régulière et à tout moment lorsque les circonstances l'exigent. La direction fixe la politique de cybersécurité de l'entité et s'engage à atteindre les objectifs de sécurité définis à l'issue des analyses de risques.*

1.1.2 / Définir les orientations de cybersécurité

■ **FINALITÉ : les choix relatifs à la cybersécurité sont effectués en cohérence avec la stratégie de l'entité et les risques auxquels elle est exposée.**

☐ *RECOMMANDATION : les orientations en termes de cybersécurité sont validées au moins annuellement par la direction de l'entité. Les arbitrages importants sont validés au niveau de la direction de l'entité, en particulier lorsque des mesures de cybersécurité ont un impact sur la réalisation des activités métier de l'entité. L'entité établit et entretient une vision à long terme de sa cybersécurité.*

1.1.3 / Définir des moyens alloués à la cybersécurité

■ **FINALITÉ : l'entité dispose des moyens financiers, techniques et humains nécessaires à la réalisation des objectifs de cybersécurité qu'elle a définis.**

☐ *RECOMMANDATION : la direction de l'entité s'engage à mettre en place les moyens nécessaires pour atteindre les objectifs de cybersécurité fixés à une échéance donnée.*

1.1.4 / Établir une cartographie fonctionnelle

■ **FINALITÉ : l'entité connaît les informations, activités, ressources et processus qui participent à la réalisation de ses missions.**

☐ *RECOMMANDATION : Une cartographie fonctionnelle de l'entité est établie et maintenue à jour. Cette cartographie doit notamment identifier les systèmes d'information sensibles et les exigences de sécurité (en confidentialité, disponibilité, intégrité) qui leur sont attachées.*

1.2 / PILOTER LA CYBERSÉCURITÉ

■ **FINALITÉ :** *l'entité dispose de l'organisation adéquate pour mettre en œuvre sa stratégie de cybersécurité.*

□ *RECOMMANDATION : l'entité met en place l'organisation et les processus permettant de répondre aux enjeux de cybersécurité ; elle est consciente de ses besoins et de son niveau réel de cybersécurité ; elle formalise sa politique de cybersécurité et les processus qui y participent ; elle identifie les problématiques de cybersécurité dans tous ses projets de systèmes d'information. Elle est capable de sélectionner et d'ajuster les mesures prises aux enjeux identifiés.*

1.2.1 / Définir l'organisation et les responsabilités en matière de cybersécurité

■ **FINALITÉ : l'entité définit et établit la chaîne de responsabilité cybersécurité et l'organisation adaptée pour répondre aux objectifs de cybersécurité.**

□ *RECOMMANDATION : l'ensemble des responsabilités est défini ; un responsable est en particulier identifié pour chaque bien sensible. L'organisation couvre l'ensemble des systèmes d'information de l'entité, y compris le système d'information de sûreté, les systèmes industriels, les systèmes support des systèmes sensibles et les systèmes sous-traités. L'organisation permet de réagir aux alertes et aux incidents de manière efficace. Les processus sont définis et respectés et permettent d'appliquer les recommandations des autorités. Autant que possible, un délégué chargé des relations avec les autorités est nommé et reconnu dans l'entité.*

1.2.2 / Établir la documentation de cybersécurité

■ **FINALITÉ : L'organisation, les politiques, les processus et les procédures de l'entité visant à répondre aux objectifs de cybersécurité sont formalisés dans des documents validés par la direction de l'entité. Ils sont ensuite appliqués par l'ensemble de l'entité.**

□ *RECOMMANDATION : l'entité établit le corpus documentaire qui définit l'organisation et les politiques de cybersécurité et le fait valider par la direction. Ce corpus comprend notamment :*

- *les politiques de sécurité (notamment PSSI) ;*
- *l'organisation, les rôles, les responsabilités et les procédures ;*
- *la gestion des situations exceptionnelles : les plans de continuité et de reprise d'activité ;*
- *les documents permettant la bonne mise en œuvre des politiques de sécurité (fiches réflexes, guides de configuration, etc.).*

Ces documents sont ensuite :

- *inclus dans un référentiel accessible à tout le personnel de l'entité. Le cas échéant, les éléments relevant d'un besoin d'en connaître restreint pourront être soustraits de la version du référentiel accessible à l'ensemble du personnel ;*
- *appliqués dans l'ensemble de l'entité, avec vérifications et audits réguliers ;*
- *mis à jour régulièrement et à chaque fois que cela est nécessaire.*

1.2.3 / Intégrer la cybersécurité dans les projets

■ **FINALITÉ : la cybersécurité est prise en compte dans l'ensemble du cycle de vie des projets.**

☐ *RECOMMANDATION : l'étude des enjeux et des risques est systématique dans tous les projets de systèmes d'information, et permet la prise en compte de la cybersécurité en fonction de la criticité et de l'exposition du système. Cette prise en compte des exigences de cybersécurité dans les projets est validée et contrôlée par la chaîne fonctionnelle de cybersécurité à toutes les étapes clés du cycle de vie du système. Les moyens nécessaires à cette prise en compte sont alloués. Une procédure permet de s'assurer qu'une évaluation des risques a été menée et que les risques résiduels ont été acceptés après traitement sur tous les systèmes mis en service puis régulièrement pendant leur exploitation*

1.2.4 / Définir et utiliser des indicateurs cybersécurité

■ **FINALITÉ : la direction de l'entité dispose d'une vision synthétique du niveau de prise en compte de la cybersécurité dans l'entité et de l'évolution de ce niveau, afin d'orienter l'évolution de sa stratégie.**

☐ *RECOMMANDATION : l'entité définit des indicateurs pour évaluer le niveau d'application et les résultats de la stratégie de cybersécurité et institue les modalités de collecte et d'analyse.*
La direction de l'entité examine régulièrement les tableaux de bord regroupant ces indicateurs et décide le cas échéant des actions à mener en conséquence.

1.2.5 / S'inscrire dans une démarche d'amélioration continue

■ **FINALITÉ : l'entité ajuste en permanence ses mesures de sécurité aux enjeux.**

☐ *RECOMMANDATION : l'entité exploite ses retours d'expériences, les résultats des audits et contrôles réalisés et les informations fournies par les autorités et la veille technique et juridique pour améliorer sa cybersécurité.*

1.3 / DÉFINIR UNE STRATÉGIE DE COMMUNICATION SUR LA CYBERSÉCURITÉ

■ **FINALITÉ : l'entité met en place une stratégie de communication de cybersécurité adaptée à ses enjeux.**

☐ *RECOMMANDATION : l'entité sensibilise son personnel aux enjeux de cybersécurité et prépare les communications internes et externes adaptées au quotidien et aux contextes de crises ou d'incidents majeurs.*

1.3.1 / Communiquer en interne et sensibiliser le personnel

■ **FINALITÉ : le personnel de l'entité est sensibilisé aux enjeux et bonnes pratiques de cybersécurité de manière à éviter les comportements à risque.**

☐ *RECOMMANDATION : tous les agents qui interviennent dans l'entité (y compris les stagiaires et les sous-traitants) sont périodiquement sensibilisés aux règles élémentaires d'hygiène informatique et aux bonnes pratiques de cybersécurité, et suivent des formations à la cybersécurité adaptées à leur fonction. La vigilance du personnel est régulièrement sollicitée afin d'éviter les comportements à risques. Des actions de communication interne sont mises en œuvre pour inciter le personnel à respecter les bonnes pratiques.*

1.3.2 / Communiquer vers l'extérieur lors des crises

■ **FINALITÉ : l'entité établit une stratégie de communication et la met en œuvre, en particulier lors des crises, de manière à maîtriser l'impact médiatique de l'événement.**

☐ *RECOMMANDATION : la stratégie de communication de crise de l'entité est validée par la direction. Elle définit les processus et l'organisation nécessaires pour communiquer lors des crises vers l'ensemble des interlocuteurs internes et externes de l'entité. Des éléments de langage sont préparés en amont, dans l'éventualité d'une communication de crise à destination des clients, de la presse ou des autorités. La direction désigne le personnel autorisé à communiquer pour chaque cas identifié.*

1.4 / DISPOSER DES RESSOURCES HUMAINES PERMETTANT LA CYBERSÉCURITÉ

■ **FINALITÉ : le personnel de l'entité contribue activement à la cybersécurité de l'entité.**

☐ *RECOMMANDATION : l'entité prend en compte les problématiques cybersécurité dans sa gestion des ressources humaines.*

1.4.1 / Responsabiliser le personnel

■ **FINALITÉ : le personnel de l'entité est individuellement responsabilisé quant aux risques liés à l'usage des systèmes d'information mis à sa disposition.**

☐ *RECOMMANDATION : le personnel s'engage par écrit, pour toute la durée de son contrat de travail, à respecter les règles de sécurité imposées par l'entité (charte, clauses de sécurité des contrats, règlement intérieur, engagement de confidentialité, etc.). Il est régulièrement informé des règles à respecter et de leurs évolutions. Des moyens sont mis en œuvre pour faire respecter ces règles (détection des négligences, rappels, sanctions, etc.).*

1.4.2 / Gérer les autorisations du personnel

■ **FINALITÉ : l'accès aux informations, documents ou systèmes les plus sensibles de l'entité est restreint au personnel ayant le besoin d'en connaître.**

☐ *RECOMMANDATION : le personnel accédant aux informations, documents ou systèmes les plus sensibles de l'entité est informé au préalable de leur caractère confidentiel et, par conséquent, des restrictions d'usage, de conservation et de diffusion au sein et à l'extérieur de l'entité. L'entité s'assure que le personnel accédant à des informations classifiées – au sens de l'instruction générale interministérielle sur la protection du secret de la défense nationale (IGI 1300) – est habilité.*

1.4.3 / Disposer des compétences de cybersécurité nécessaires dans la durée

■ **FINALITÉ : l'entité dispose dans la durée des compétences nécessaires à la réalisation des objectifs de cybersécurité.**

☐ *RECOMMANDATION : l'entité définit et met en place une stratégie d'acquisition et de maintien des compétences en cybersécurité.*
Cette stratégie définit les actions menées pour disposer des compétences nécessaires : recrutement, formation, emploi de compétences externes, etc.
L'entité décrit en particulier comment elle garantit qu'elle est toujours apte à remplir l'ensemble des fonctions en cas du départ d'un ou plusieurs de ses agents ainsi que les modalités d'évaluation des compétences en cybersécurité de son personnel.

1.5 / INCLURE LA CYBERSÉCURITÉ DANS LES CONTRATS

■ **FINALITÉ : la stratégie de cybersécurité est appliquée dans les relations avec les tiers. Elle inclut une veille portant sur les exigences réglementaires.**

☐ *RECOMMANDATION : l'entité intègre les exigences de cybersécurité dans les contrats et conventions (infogérance, relation avec les tiers) qu'elle signe, et connaît la réglementation applicable sur son périmètre.*

1.5.1 / Protéger les biens des clients et des partenaires

■ **FINALITÉ : l'entité garantit à ses clients et à ses partenaires la protection de leurs informations, biens et services, dans le respect des clauses contractuelles et de la réglementation applicable.**

☐ *RECOMMANDATION : le niveau de protection assuré par l'entité est conforme aux engagements pris auprès des clients ou des partenaires.*

1.5.2 / Maîtriser ses achats

■ **FINALITÉ : l'entité est capable d'imposer et d'évaluer le niveau de sécurité des services, prestations, équipements et systèmes d'information qu'elle acquiert, loue ou emprunte, et des informations ou systèmes d'information qu'elle confie à des prestataires.**

☐ *RECOMMANDATION : tout contrat relatif à un système d'information participant aux missions de l'entité comporte des clauses définissant les règles de sécurité que doit respecter le contractant afin de garantir le niveau de sécurité fixé pour ce système d'information. Ces règles sont cohérentes avec les enjeux du système, les objectifs de sécurité de l'entité et sont conformes à l'état de l'art.*
L'entité a les moyens de vérifier que les clauses sont correctement mises en œuvre, notamment par le biais de contrôles.
L'entité s'assure que ses sous-traitants et prestataires sont capables d'intervenir dans les délais requis lors des exercices, des incidents ou des crises.

1.5.3 / Choisir des prestataires de confiance

■ **FINALITÉ : l'entité recourt à des prestataires de confiance lorsqu'elle veut contractualiser des services ou des prestations liées à la cybersécurité.**

☐ *RECOMMANDATION : pour les domaines de prestations et services liés à la cybersécurité couverts par des schémas de labellisation existants, l'entité sélectionne des prestataires labellisés par l'autorité nationale de la sécurité des systèmes d'information.*

1.5.4 / Maîtriser ses interfaces

■ **FINALITÉ : l'entité maîtrise les interconnexions avec des tiers, aussi bien au niveau juridique que technique.**

☐ *RECOMMANDATION : l'entité définit dans ses contrats et conventions le niveau de sécurité des systèmes d'information externes avec lesquels s'interfacent ses propres systèmes. Elle insère des clauses dans les contrats et met en œuvre les moyens de vérifier leur application effective. De même l'entité sécurise les interfaces de ses SI avec des réseaux moins protégés que ses propres systèmes (par exemple Internet).*

1.5.5 / Connaître ses obligations légales et réglementaires

■ **FINALITÉ : l'entité réalise une veille juridique régulière sur ses obligations légales et réglementaires ayant trait à la cybersécurité et la protection des données. Dès lors qu'elle dispose d'implantations à l'étranger, l'entité connaît les contraintes légales et réglementaires propres à tous les pays concernés.**

☐ *RECOMMANDATION : l'entité s'assure que son personnel connaît les obligations légales et réglementaires qu'il doit respecter dans le cadre de ses activités.*

2 / MAÎTRISER LES RISQUES

FINALITÉ : la maîtrise des risques est au centre de la stratégie de protection et de défense des systèmes d'information de l'entité.

RECOMMANDATION : les risques sont évalués sur tous les systèmes d'information de l'entité. A travers la démarche d'homologation, les risques résiduels sont portés à la connaissance de la direction de l'entité qui les accepte ou les refuse après traitement.

2.1 / ANALYSER LES RISQUES CYBER RELATIFS À SES SYSTÈMES

■ **FINALITÉ : les risques sont évalués sur tous les systèmes d'information de l'entité, pendant toutes les phases de leur cycle de vie, afin de les sécuriser de manière adaptée aux risques et enjeux.**

□ *RECOMMANDATION : l'entité réalise une analyse de risques pour tous ses systèmes d'information, dès les phases amont des projets, en employant une méthodologie adaptée. L'entité planifie l'analyse de risques de tous ses systèmes existants. L'entité met à jour régulièrement cette analyse de risques (au minimum tous les ans, et à chaque fois qu'une nouvelle menace ou vulnérabilité importante est portée à sa connaissance ou à l'occasion de chaque évolution technique ou fonctionnelle du système considéré). A partir des résultats d'analyse de risques, l'entité est en mesure d'apprécier les conséquences d'un incident ou d'une défaillance sur ses éléments sensibles. L'entité déploie les mesures pertinentes sur ou autour de ses systèmes pour que ne subsistent que des risques résiduels acceptables. L'analyse de risque suit une méthode reconnue et systématique (par exemple la méthode EBIOS).*

2.2 / HOMOLOGUER SES SYSTÈMES D'INFORMATION

■ **FINALITÉ : l'entité a connaissance des risques résiduels des systèmes d'information qu'elle a sous sa responsabilité et elle les accepte formellement.**

□ *RECOMMANDATION : une évaluation des risques résiduels est menée pour chaque système et présentée dans un dossier de sécurité. L'acceptation des risques résiduels est validée par l'autorité responsable de l'entité. Lorsque le périmètre fonctionnel, technique ou physique est modifié ou que de nouvelles vulnérabilités apparaissent, l'entité réévalue les risques résiduels et se prononce sur l'opportunité d'entreprendre une nouvelle validation de l'acceptation de ces risques*

3 / MAÎTRISER LES SYSTÈMES D'INFORMATION

FINALITÉ : l'entité maîtrise les systèmes d'information qu'elle utilise ou dont elle est responsable.

RECOMMANDATION : l'entité élabore ou fait élaborer ses systèmes d'information conformément à ses besoins, connaît leur fonctionnement, les maîtrise pendant tout leur cycle de vie et en maîtrise les accès.

3.1 / CONNAÎTRE SES SYSTÈMES

■ **FINALITÉ : l'entité connaît les systèmes d'information qu'elle utilise ou dont elle est responsable.**

□ *RECOMMANDATION : l'entité dispose d'une cartographie et une documentation complètes de ses systèmes d'information, et maîtrise les règles de manipulation des informations sensibles.*

3.1.1 / Cartographier ses systèmes

■ **FINALITÉ : l'entité établit et tient à jour une cartographie de ses systèmes d'information, de manière à connaître ce qu'elle doit protéger.**

□ *RECOMMANDATION : l'entité établit et maintient à jour annuellement :*

- *une cartographie technique macroscopique de tous ses systèmes d'information, cohérente avec la cartographie fonctionnelle;*
- *une cartographie détaillée de tous les systèmes d'information rénovés, remplacés ou mis en service.*

L'entité maîtrise les flux entrants et sortants de ses systèmes, y compris ceux provenant ou à destination de territoires étrangers, ainsi que la localisation géographique de ses réseaux.

3.1.2 / Disposer de la documentation de ses systèmes et composants

■ **FINALITÉ : l'entité dispose de la documentation à jour de tous les systèmes d'information et composants dont elle est responsable, de manière à pouvoir intervenir plus facilement sur ses systèmes en cas d'incident.**

□ *RECOMMANDATION : la documentation des systèmes d'information et composants de l'entité est complète, organisée et accessible aux seuls acteurs concernés. Elle permet la compréhension, l'administration, la maintenance et l'utilisation correcte des systèmes. Elle détaille les procédures d'exploitation de la sécurité des systèmes ou composants le nécessitant.*

3.1.3 / Sécuriser la manipulation des informations sensibles

■ **FINALITÉ : l'entité assure la sécurité de ses informations et documents sensibles en confidentialité, intégrité et disponibilité.**

□ *RECOMMANDATION : les informations sensibles sont identifiées, marquées et manipulées de manière à préserver leur confidentialité et leur accès est restreint aux seules personnes ayant le besoin d'en connaître.*

3.2 / MAÎTRISER SES SYSTÈMES TOUT AU LONG DE LEUR CYCLE DE VIE

■ **FINALITÉ : l'entité maîtrise ses systèmes d'information sur tout leur cycle de vie.**

□ *RECOMMANDATION : lorsqu'elle construit, acquiert ou modifie ses systèmes d'information, l'entité s'assure que les principes de maîtrise de ses systèmes sont bien pris en compte.*

3.2.1 / Concevoir et développer des systèmes sûrs

■ **FINALITÉ : Les systèmes d'information sont conçus et développés selon une architecture sécurisée.**

□ *RECOMMANDATION : la conception d'un système d'information respecte, autant que possible, les règles suivantes :*

- *En début de projet, identifier les besoins de sécurité relatifs au système et son environnement pour évaluer l'effort nécessaire de prise en compte de la cybersécurité dans le projet ;*
- *Réduire la complexité du système de manière à en faciliter la maîtrise, l'analyse et la maintenance ;*
- *Réduire les dépendances entre les composants afin de réduire les impacts de l'évolution d'un composant sur l'ensemble du système ;*
- *Confiner les fonctions de sécurité et les traitements de données sensibles dans des zones de confiance, séparées des traitements de moindre niveau de confiance ;*
- *Placer les fonctions non sûres dans des environnements dédiés afin de limiter leurs impacts sur le système ;*
- *Contrôler les données d'entrée du système pour préserver son intégrité et sa disponibilité et les données de sortie du système pour préserver leur confidentialité ;*
- *Définir le comportement du système de manière déterministe : il ne doit pas être possible de détourner le système de ses fonctions prévues ;*
- *Gérer les erreurs et les exceptions pour faire revenir le système dans un état stable et maîtrisé ;*
- *Ne réutiliser un composant que s'il a fait la démonstration de son niveau de sécurité ;*
- *Construire le système de manière à ce qu'il ne fasse pas d'erreur par lui-même, qu'il résiste aux erreurs et qu'il soit disponible et capable de revenir à un état stable après un incident majeur ;*
- *Construire le système de manière à ce que la sécurité ne réduise pas ses performances au-delà d'un seuil acceptable ;*
- *Construire le système afin de permettre de passer d'un environnement à un autre de manière simple ;*
- *Construire le système afin qu'il soit conforme aux besoins fonctionnels, pertinent, interopérable et conforme aux standards spécifiés.*
- *Concevoir le système avec un contrôle d'accès et une administration sécurisée ;*
- *Concevoir le système afin qu'il soit simple de comprendre son utilisation, son exploitation et son administration ;*
- *Concevoir le système afin qu'il soit simple de l'analyser, de le modifier et de le tester.*

3.2.2 / Maîtriser les chaînes d'approvisionnement

■ **FINALITÉ : l'approvisionnement ne doit pas constituer un vecteur de fragilisation des systèmes.**

☐ *RECOMMANDATION : l'entité maîtrise l'intégrité de sa chaîne d'approvisionnement, que cela soit pour la réalisation initiale de ses systèmes, leur maintenance ou leur évolution.*

3.2.3 / Valider la cybersécurité lors de la recette

■ **FINALITÉ : la sécurité des systèmes d'information est validée lors des phases de recette.**

☐ *RECOMMANDATION : le niveau de sécurité des systèmes d'information est évalué par rapport à l'état de l'art et est conforme aux clauses contractuelles de cybersécurité. Une évaluation du niveau de sécurité du système d'information est menée lors de la phase de recette. Les tests des exigences de sécurité sont intégrés aux tests de validation du système. Les éléments utilisés lors des tests sont protégés en fonction de leur sensibilité.*

3.2.4 / Exploiter de manière sécurisée

■ **FINALITÉ : les conditions d'exploitation de chaque système de l'entité permettent d'assurer un niveau de sécurité de l'environnement du système d'information compatible, voire complémentaire de la sécurité intrinsèque du système.**

☐ *RECOMMANDATION : l'utilisation et l'administration d'un système d'information en exploitation sont conformes aux politiques de sécurité de l'entité et s'accompagnent des mesures organisationnelles et techniques décidées lors de l'homologation du système.*

3.2.5 / Maîtriser la maintenance et le maintien en condition de sécurité

■ **FINALITÉ : les systèmes d'information conservent un niveau de sécurité satisfaisant tout au long de leur exploitation, correspondant au niveau de risque accepté lors de l'homologation.**

☐ *RECOMMANDATION : l'entité assure une veille sur les vulnérabilités des systèmes et de leurs composants (en particulier les composants sur étagère) et identifie les moyens de corriger ces vulnérabilités.*
Une stratégie est définie et mise en place pour limiter la dégradation du niveau de sécurité, consécutif à l'évolution de l'environnement et aux incidents auxquels les systèmes d'information ne sont pas préparés. Cette stratégie définit notamment les règles de mise à jour des composants des systèmes de l'entité et de déploiement des politiques de sécurité.

3.2.6 / Encadrer l'évolution des systèmes

■ **FINALITÉ : l'entité encadre l'évolution des systèmes d'information de manière à satisfaire les évolutions des besoins métiers tout en maintenant les niveaux de sécurité attribués aux systèmes.**

☐ *RECOMMANDATION : l'entité établit et suit :*

- *une politique de développement de ses systèmes d'information qui définit les étapes du cycle de vie de chaque système ou évolutions d'un système (par exemple : spécifications, maquettage, test en pré-production, production, retrait). Des jalons sont spécifiés à chacune des étapes avec leurs conditions de franchissement (par exemple : validation formelle des spécifications, succès des tests) ;*
- *une politique de migration de ses systèmes d'information, qui définit et applique des critères déclenchant la migration d'un système d'une version à une autre, ou d'un système à un autre (suite à obsolescence ou perte d'interopérabilité, etc.), et guidant la migration du système vers un niveau de sécurité au moins égal à son niveau actuel.*

Toute évolution d'un système entraîne une révision de son homologation, examinant au minimum les écarts entre les deux versions du système.

3.2.7 / Garantir la sécurité lors du retrait de service

■ **FINALITÉ : le retrait du service de tout ou partie du système ne diminue pas le niveau de cybersécurité de l'entité**

☐ *RECOMMANDATION : l'entité garantit la sécurité du système et des données qu'il contient ou auxquelles il accède, lors du retrait du service de tout ou partie de ce système.*

3.3 / MAÎTRISER LES ACCÈS À SES SYSTÈMES

■ **FINALITÉ : l'entité maîtrise l'accès à ses systèmes d'information.**

☐ *RECOMMANDATION : l'entité définit les principes de maîtrise des accès, en fonction des systèmes d'information, et en tenant compte du cycle de vie des utilisateurs.*

3.3.1 / Définir les principes de maîtrise des droits d'accès

■ **FINALITÉ : l'entité maîtrise les droits d'accès accordés aux acteurs ou aux équipements pour accéder aux systèmes d'information.**

☐ *RECOMMANDATION : l'entité définit les principes de gestion des droits d'accès aux systèmes dont elle est responsable, en particulier lorsque ces droits concernent des comptes privilégiés ou des accès à des informations sensibles. L'entité garantit que les droits octroyés sur les systèmes d'information sont appliqués selon le principe du moindre privilège et du juste besoin. L'entité définit les procédures et les moyens permettant de filtrer les accès et les fonctionnalités des systèmes d'information traitant ou concernant des éléments sensibles.*

3.3.2 / Définir les principes d'identification et d'authentification

■ **FINALITÉ : l'utilisation de moyens d'identification et d'authentification permet la traçabilité et la non-répudiation des opérations réalisées sur les systèmes, ainsi que la sécurisation des accès.**

☐ *RECOMMANDATION : les principes d'identification et d'authentification (vérification / preuve de l'identité présentée au système) des accès à l'ensemble des systèmes de l'entité, par les acteurs et les équipements, sont définis au regard de la criticité des informations traitées.*

3.3.3 / Définir les rôles et les profils

■ **FINALITÉ : l'entité fixe pour chaque catégorie d'acteur des règles d'accès à ses systèmes de manière à limiter le risque d'usage non autorisé.**

☐ *RECOMMANDATION : l'entité détermine, pour chaque catégorie d'acteurs, le juste besoin d'accès aux systèmes en s'appuyant sur les exigences réglementaires et les principes fondamentaux. Les règles ainsi définies sont régulièrement révisées. Des principes de cloisonnement des droits, de ségrégation des responsabilités, et de gestion du besoin d'en connaître, d'origine réglementaire ou non, sont appliqués.*

3.3.4 / Limiter l'accès selon des principes d'habilitation

■ **FINALITÉ : l'entité limite l'accès aux systèmes ou informations sensibles aux seules personnes habilitées à y accéder.**

☐ *RECOMMANDATION : l'entité définit les types de systèmes qui requièrent une habilitation préalable des agents, ainsi que les modalités d'habilitation. L'entité définit et applique les procédures d'habilitation associées.*

3.3.5 / Gérer les droits utilisateurs selon leur cycle de vie

■ **FINALITÉ : les droits accordés aux utilisateurs correspondent aux fonctions et rôles qu'ils occupent.**

☐ *RECOMMANDATION : des principes de mise à jour des droits tout au long du cycle de vie des utilisateurs (arrivée, mutation, mission, départ, …) sont définis et appliqués. Notamment, il est indispensable que l'ensemble des droits affectés à une personne soient révoqués lors du départ ou du changement de fonction de cette dernière (pour éviter le cumul de droits menant à des abus). L'entité dispose d'un inventaire exhaustif des comptes privilégiés qu'elle maintient à jour. L'entité identifie nominativement chaque acteur ayant accès au système.*

3.3.6 / Contrôler les droits d'accès

■ **FINALITÉ : les droits accordés correspondent aux règles définies.**

☐ *RECOMMANDATION : l'entité contrôle régulièrement les droits accordés aux utilisateurs et aux différents composants de ses systèmes de manière à vérifier leur conformité aux règles qu'elle a définies.*

4 / PROTÉGER LES SYSTÈMES

FINALITÉ : l'entité protège ses systèmes d'information.

RECOMMANDATION : l'entité protège ses systèmes d'information physiquement et logiquement contre les scénarios de menaces identifiés à l'aide de composants à l'état de l'art du point de vue de la sécurité.

4.1 / UTILISER DES COMPOSANTS SÉCURISÉS

■ **FINALITÉ :** **Les composants constituant les systèmes d'information offrent des garanties de sécurité en complément de leurs fonctionnalités, en particulier lorsque des fonctions de sécurité dépendent de ces composants.**

□ *RECOMMANDATION : l'entité choisit des composants de confiance pour supporter les fonctions sensibles et les fonctions de sécurité de ses systèmes d'information. Ces composants sont configurés de manière à limiter leur exposition aux menaces.*

4.1.1 / S'assurer du développement de confiance de ses composants

■ **FINALITÉ : l'entité a confiance dans le niveau de sécurité et les performances des composants qu'elle utilise et met en œuvre dans ses systèmes d'information.**

□ *RECOMMANDATION : les composants sensibles ou comportant des fonctions de sécurité importantes sont développés dans un environnement de confiance, selon les bonnes pratiques de développement matériel et logiciel.*

4.1.2 / Utiliser des composants qualifiés

■ **FINALITÉ : l'entité a l'assurance du niveau de sécurité des composants de sécurité qu'elle utilise.**

□ *RECOMMANDATION : l'entité utilise, lorsqu'ils existent, des composants qualifiés par l'autorité nationale de la sécurité des systèmes d'information pour les fonctions de sécurité de ses systèmes sensibles.*

4.1.3 / Configurer correctement ses composants

■ **FINALITÉ : les composants utilisés dans les systèmes d'information sont configurés de manière à limiter leur exposition aux menaces.**

□ *RECOMMANDATION : l'entité définit et fait appliquer les règles de configuration de ses composants, en se basant sur les bonnes pratiques permettant de limiter leur surface d'attaque. Ce sont notamment :*

- *la désactivation ou suppression des fonctions et services inutiles ;*
- *la restriction des privilèges des utilisateurs ;*
- *le choix des fonctions sécurisées ;*
- *la personnalisation des mots de passe et des éléments secrets ;*
- *la sécurisation des fonctions d'administration du composant.*

4.1.4 / Utiliser des services cryptographiques à l'état de l'art et protéger ses clés

■ **FINALITÉ : les composants ayant des fonctions de sécurité utilisent des services cryptographiques adaptés basés sur une implémenta-**

tion, des algorithmes, des protocoles et une gestion des clés à l'état de l'art de manière à garantir la robustesse des services utilisés.

☐ *RECOMMANDATION : l'entité utilise des composants faisant appel à des services cryptographiques à l'état de l'art pour protéger en confidentialité, intégrité, authenticité les données qu'ils manipulent, stockent et échangent et pour garantir l'imputabilité des actions réalisées par les acteurs.*
Des procédures sont définies pour l'ensemble du cycle de vie des clés (génération, distribution, utilisation, effacement et révocation) de manière à assurer leur confidentialité, intégrité et authenticité. Elles permettent de réaliser rapidement en cas de compromission de clés ou de certificats :
- *l'alerte des utilisateurs,*
- *la révocation technique des éléments compromis,*
- *le renouvellement des clés compromises par des méthodes sécurisées.*

4.1.5 / Garantir la robustesse des authentifiants et mots de passe

■ **FINALITÉ : les éléments d'authentification sont robustes.**

☐ *RECOMMANDATION : L'utilisation de moyens d'authentification forte à l'état de l'art est préférée à l'emploi de mots de passe. Lorsque l'authentification par mot de passe est choisie, l'entité exige et s'assure par des moyens techniques que la politique de mots de passe est appliquée (mots de passe robustes, renouvelés régulièrement). L'entité ne conserve pas en clair les mots de passe dans des fichiers stockés sur ses systèmes informatiques. Les fichiers ou les documents papier contenant les mots de passe sont protégés par des moyens en cohérence avec les enjeux. L'entité supprime ou modifie les éléments d'authentification installés par défaut sur les équipements (mots de passe constructeur).*

4.2 / PROTÉGER PHYSIQUEMENT SES SYSTÈMES D'INFORMATION

■ **FINALITÉ : les systèmes d'information sont protégés contre les incidents et menaces physiques auxquels ils pourraient être exposés.**

☐ *RECOMMANDATION : l'entité protège les systèmes d'information contre les accès physiques illégitimes, les agressions physiques et les événements naturels.*

4.2.1 / Garantir la disponibilité des servitudes

■ **FINALITÉ : l'entité garantit l'approvisionnement de ses systèmes d'information sensibles en flux nécessaires : énergie, refroidissement et réseaux de communication.**

☐ *RECOMMANDATION : l'approvisionnement en énergie et en refroidissement des systèmes d'information est dimensionné de façon à assurer la continuité de fonctionnement, y compris lorsque l'entité est confrontée aux scénarios de menaces identifiés.*

4.2.2 / Résister aux événements naturels, incidents et attaques physiques

■ **FINALITÉ : l'entité garantit la disponibilité et l'intégrité de ses systèmes d'information sensibles face aux événements naturels, incidents et attaques physiques auxquels ils peuvent être confrontés.**

☐ *RECOMMANDATION : l'entité assure la disponibilité et l'intégrité de ses systèmes d'information face aux scénarios d'événements redoutés (dont notamment l'incendie, les dégâts des eaux, les phénomènes climatiques exceptionnels, les malveillances, etc.).*

4.2.3 / Protéger les accès physiques

■ **FINALITÉ : l'entité retarde ou empêche l'accès physique aux locaux, aux systèmes et aux informations par des acteurs non autorisés, tout en maintenant la disponibilité des accès pour les acteurs légitimes.**

☐ *RECOMMANDATION : l'entité définit les zones contenant ses systèmes d'information sensibles. La protection des accès physiques aux systèmes d'information de l'entité est suffisante pour répondre aux scénarios de menaces identifiés, en particulier dans les zones sensibles. Il n'est pas possible d'accéder sans contrôle d'accès à des systèmes d'information sensibles depuis les zones publiques de l'entité. Les réseaux de gestion technique des bâtiments (GTB) et les systèmes d'information de sûreté peuvent contribuer à cette protection et doivent, à ce titre, être spécifiquement protégés.*

4.2.4 / Contrôler l'accès physique des personnes

■ **FINALITÉ : l'entité contrôle l'accès physique des personnes et matériels aux différentes zones dans lesquelles sont implantés l'entité ou des systèmes d'information dont elle est responsable, en fonction de la sensibilité de ses zones.**

☐ *RECOMMANDATION : seules les personnes autorisées peuvent accéder aux zones sensibles. Le contournement du contrôle d'accès par une personne non autorisée est détecté. Les accès temporaires aux zones sensibles sont tracés.*

4.2.5 / Se prémunir contre les risques électromagnétiques

■ **FINALITÉ : l'entité protège ses informations sensibles d'une fuite par canaux auxiliaires et se protège des attaques électromagnétiques.**

☐ *RECOMMANDATION : l'entité prend en compte les risques de fuite d'informations sensibles par l'émission de signaux parasites compromettants lors de ses analyses de risques et s'assure que les écrans susceptibles d'afficher des informations sensibles en confidentialité ne sont pas visibles depuis une zone ouverte au public.*

4.3 / PROTÉGER LOGIQUEMENT SES SYSTÈMES D'INFORMATION

■ **FINALITÉ : l'entité protège ses systèmes d'information des utilisations malveillantes.**

□ *RECOMMANDATION : l'entité définit et met en place une défense en profondeur de ses systèmes d'information. Elle contrôle les accès logiques à ses systèmes d'information, se protège contre les applications malveillantes, sécurise ses réseaux, ses équipements, ses données et ses supports de données.*

4.3.1 / Se prémunir contre les codes malveillants

■ **FINALITÉ : l'entité se prémunit contre les effets des codes malveillants susceptibles de pénétrer ses systèmes.**

□ *RECOMMANDATION : l'entité identifie les chemins et scénarios par lesquels des codes malveillants peuvent pénétrer ses systèmes d'information. Elle met en place, notamment par filtrage des contenus, des moyens permettant de détecter, de bloquer et de supprimer de tels codes.*

4.3.2 / Protéger les réseaux

■ **FINALITÉ : les échanges sur les réseaux de l'entité sont sécurisés et maîtrisés, en particulier au niveau des interconnexions entre systèmes d'information ou avec des réseaux extérieurs à l'entité, afin d'éviter les attaques et d'en limiter la propagation.**

□ *RECOMMANDATION : L'entité filtre et contrôle les flux de données (contenus, types de fichiers, sources, protocoles, groupes d'utilisateurs, …) au niveau des interconnexions entre réseaux. Les réseaux sont segmentés en zones de sensibilité homogène. Les équipements contenant des informations sensibles en confidentialité, intégrité ou disponibilité pour l'entité sont placés dans une zone protégée par une passerelle d'interconnexion spécifique. L'usage d'infrastructure sans fil (notamment WiFi) est limité aux cas où il ne peut être évité et des mesures de protection complémentaires doivent être étudiées. En particulier, les réseaux d'accès sans fil doivent être cloisonnés des autres systèmes d'information.*
Le nombre de points d'accès des systèmes d'information de l'entité à Internet est limité au strict nécessaire. Les passerelles d'interconnexion avec Internet sont sécurisées.
Les équipements réseaux et les équipements de sécurité sont configurés suivant l'état de l'art. L'entité privilégie des applications et protocoles d'échanges sécurisés, en particulier pour l'administration à distance, les accès distants ou nomades.

4.3.3 / Protéger les équipements

■ **FINALITÉ : les équipements connectés aux systèmes d'information de l'entité sont maîtrisés et sécurisés.**

☐ RECOMMANDATION : *l'entité maîtrise tous les équipements qui se connectent à ses systèmes d'information et elle maîtrise leur configuration. Ces équipements sont sécurisés. Des procédures basées sur l'analyse de risques et l'homologation autorisent ou interdisent la connexion des équipements aux systèmes de l'entité. Les conditions dans lesquelles les équipements peuvent être connectés (configuration, restriction d'emploi, …) sont définies. La connexion d'équipements personnels aux systèmes d'information de l'entité est interdite. Les terminaux mobiles sont gérés selon une politique de sécurité au moins aussi stricte que celle des postes fixes.*

Les connexions à distance sont :

- *interdites dans tous les cas où cela est possible ;*
- *autorisées uniquement depuis des postes professionnels mettant en œuvre des mécanismes d'authentification forte et protégeant l'intégrité et la confidentialité des échanges à l'aide de moyens robustes.*

4.3.4 / Protéger les données

■ **FINALITÉ : la sécurité (disponibilité, confidentialité, intégrité, traçabilité) des données de l'entité est garantie sur tout leur cycle de vie en fonction de leur sensibilité.**

☐ RECOMMANDATION : *l'entité définit et met en place les politiques de sécurisation de ses données. Elle protège ses données lors de leur traitement, échange sur des réseaux, stockage et effacement. Elle définit le niveau de disponibilité dont doivent bénéficier les données et met en œuvre les moyens permettant d'atteindre ce niveau (sauvegardes distribuées, redondances hétérogènes de systèmes, etc.).*

4.3.5 / Protéger les supports de données

■ **FINALITÉ : les données sont protégées lors de leur stockage sur un support de données.**

☐ RECOMMANDATION : *l'entité définit et met en place des procédures d'utilisation et des moyens de protection des supports de données sur tout leur cycle de vie. Elle s'assure que les sauvegardes sont protégées en confidentialité et en intégrité.*

L'entité définit des règles d'utilisation des imprimantes, des photocopieuses et des documents imprimés.

Elle veille à la protection en confidentialité des postes nomades et des supports de données amovibles. Elle définit et fait appliquer des règles relatives à la connexion des supports amovibles aux systèmes d'information de l'entité, de manière à éviter la fuite d'informations sensibles ou l'introduction d'applications malveillantes.

4.3.6 / Contrôler les accès logiques

■ **FINALITÉ : les acteurs et les équipements ne peuvent accéder logiquement aux systèmes d'information que pour y réaliser les opérations pour lesquelles ils sont autorisés.**

☐ RECOMMANDATION : *toutes les fonctions de contrôle d'accès aux systèmes sont réalisées conformément aux objectifs de maîtrise des accès aux systèmes. Les annuaires sont maîtrisés et correctement configurés.*

4.3.7 / Protéger l'administration des systèmes

■ **FINALITÉ : les bonnes pratiques d'administration des systèmes d'information contribuent à renforcer leur niveau de sécurité.**

☐ *RECOMMANDATION : les modalités d'administration des systèmes d'information sont définies en accord avec les enjeux de cybersécurité et diffusées aux acteurs concernés. La navigation sur Internet est interdite depuis les comptes administrateurs. L'administration des équipements est réalisée sur un réseau cloisonné de celui des utilisateurs et l'entité vérifie qu'aucun équipement ne comporte d'interface d'administration accessible depuis Internet. Les utilisateurs n'ont pas de privilèges d'administration et le nombre de comptes administrateurs doit être réduit à son strict minimum.*

4.3.8 / Garantir la non-répudiation des actions

■ **FINALITÉ : l'entité est capable d'imputer les actions pouvant avoir un impact sur la sécurité de ses systèmes d'information, afin de reconstituer les événements et responsabilités lors d'un incident.**

☐ *RECOMMANDATION : l'entité est capable d'assurer l'authentification et la journalisation des actions pouvant avoir un impact sur la sécurité de ses systèmes d'information, notamment les actions concernant l'administration, la journalisation, les opérations sur les applications ou données sensibles. L'entité est capable d'imputer les actions critiques réalisées par des tiers sur ses systèmes d'information.*

4.4 / RENFORCER LA VIGILANCE ET LA PROTECTION

■ **FINALITÉ : l'entité renforce les mesures de vigilance et de protection en cas d'élévation du niveau de menace VIGIPIRATE.**

☐ *RECOMMANDATIONS : l'entité augmente sa vigilance et sa protection de manière à détecter et limiter l'impact d'attaques informatiques, notamment par la vérification de ses dispositifs de sécurité, l'analyse de ses journaux d'événements et le changement de ses mots de passe administrateurs.*

5 / GÉRER LES INCIDENTS DE CYBERSÉCURITÉ

FINALITÉ : l'entité réduit l'impact des attaques et incidents qu'elle subit.

RECOMMANDATION : l'entité dispose d'une réelle capacité de gestion des incidents, permettant de surveiller ses systèmes d'information, détecter et analyser des incidents, réagir face aux attaques, et garantir la continuité de ses missions sensibles.

5.1 / PRÉPARER LE DISPOSITIF DE GESTION DES INCIDENTS

■ **FINALITÉ : l'entité limite l'impact des incidents dont elle est la cible, facilite la remontée d'information et l'analyse.**

□ *RECOMMANDATION : l'entité est capable de détecter les incidents qu'elle subit et de remonter rapidement les alertes dans sa chaîne interne de traitement des incidents, et auprès des autorités concernées.*

5.1.1 / Disposer d'une chaîne opérationnelle de gestion des incidents

■ **FINALITÉ : l'entité dispose de l'organisation et des moyens de gestion des incidents permettant la prise en compte des alertes dans un délai qui permet leur traitement efficace.**

□ *RECOMMANDATION : l'entité est dotée d'une chaîne opérationnelle de traitement des incidents, permettant de détecter et limiter l'impact des incidents touchant ses systèmes d'information. Les procédures de remontée des incidents sont définies et mises en œuvre. Elles utilisent les différents canaux de remontée d'incident (système de détection, personnel, externe). Elles sont connues de tous les intervenants. Elles incluent une phase de qualification des incidents, et une phase de traitement de leurs causes et de leurs conséquences.*
L'opérateur peut sous-traiter certaines parties de la chaîne opérationnelle de gestion des incidents à des partenaires de confiance labellisés par l'ANSSI.

5.1.2 / Collecter les événements de sécurité

■ **FINALITÉ : l'entité dispose des traces et des éléments clés des systèmes d'information permettant l'analyse des comportements suspects et la détection d'incident ayant eu lieu sur les systèmes d'information ou sur les sites de l'entité.**

□ *RECOMMANDATION : les traces et les éléments clés des systèmes d'information (notamment les journaux) couvrent les systèmes d'information de l'entité avec un niveau de granularité adapté aux enjeux. Leur remontée est centralisée. Les évènements de sécurité liés aux sites de l'entité sont centralisés par site ou par regroupement de sites et conservés, si possible pendant un an. L'entité vérifie périodiquement le bon fonctionnement de la surveillance des évènements de sécurité.*

5.1.3 / Détecter les événements anormaux

■ **FINALITÉ : l'entité identifie les incidents et attaques potentielles par analyse automatique et/ou humaine des informations collectées.**

□ *RECOMMANDATION : l'entité définit, valide et exploite les règles et moyens d'analyse permettant d'identifier les incidents, les comportements malveillants et les attaques potentielles, sur les éléments actuels et passés. L'opérateur peut sous-traiter certaines parties de la chaîne opérationnelle de gestion des incidents à des partenaires de confiance labellisés par l'ANSSI.*

5.2 / ANALYSER ET QUALIFIER LES INCIDENTS

■ **FINALITÉ : l'entité connaît les caractéristiques des incidents et en déduit les impacts sur son métier.**

☐ *RECOMMANDATION : l'entité est capable de déterminer les caractéristiques des incidents (scénario, vecteur, périmètre).*

5.2.1 / Reconstituer le scénario des incidents, les vecteurs et leur périmètre

■ **FINALITÉ : l'entité connaît le scénario des incidents, les vecteurs utilisés et l'étendue sur les systèmes d'information de l'entité.**

☐ *RECOMMANDATION : l'entité est capable de reconstituer le scénario d'un incident, d'en déterminer les vecteurs et de connaître les zones, informations et équipements touchés. L'entité ne se contente pas de traiter l'infection d'une machine sans tenter de déterminer le scénario de l'incident.*

5.2.2 / Évaluer l'impact et le périmètre de l'incident sur l'activité

■ **FINALITÉ : l'entité évalue le périmètre et l'impact de chaque attaque ou de chaque incident sur son métier.**

☐ *RECOMMANDATION : l'entité est capable de déterminer le lien entre les opérations réalisées par les attaquants (exploitation de vulnérabilités, choix d'un chemin d'attaque), et l'impact sur son métier (exfiltration d'informations, modification de données, sabotage, etc.). Pour affiner son analyse, l'entité déploie si nécessaire des moyens de supervision et de détection complémentaires.*

5.3 / RÉAGIR AUX INCIDENTS

■ **FINALITÉ : l'entité prépare et organise sa réaction aux incidents et aux alertes.**

☐ *RECOMMANDATION : l'entité organise et conduit la réaction, avec pour objectif de supprimer les causes de l'incident afin d'éviter qu'il ne se reproduise et d'en limiter les conséquences ; l'entité effectue un retour d'expérience sur sa gestion des incidents.*

5.3.1 / Organiser la réaction

■ **FINALITÉ : l'entité organise la réaction à un incident ou à une attaque.**

☐ *RECOMMANDATION : l'entité dispose de capacités de réaction et d'une organisation adaptée pour les mettre en œuvre lorsque cela s'avère nécessaire.*

5.3.2 / Préparer des mesures de réaction

■ **FINALITÉ : l'entité prépare les mesures de réaction pour rétablir un niveau de sécurité en cas d'incident ou d'attaque.**

☐ *RECOMMANDATION : suite à un incident ou une attaque, l'entité augmente le niveau de sécurité, de manière à limiter les conséquences ou l'étendue de l'incident ou de l'attaque. L'entité prépare les personnes compétentes et les outils nécessaires afin de pouvoir mener de manière efficace la réaction à l'incident ou l'attaque. Les impacts métier de la réaction sont anticipés ; l'entité prépare une stratégie de communication interne et externe sur l'incident.*

5.3.3 / Conduire la réaction

■ **FINALITÉ : l'entité bloque l'attaquant ou stoppe l'incident, reprend la maîtrise de ses sites et de ses réseaux et durcit ses systèmes d'information pour éviter une nouvelle occurrence de l'incident.**

☐ *RECOMMANDATION : suite à un incident ou une attaque, l'entité est capable d'exécuter les opérations nécessaires pour supprimer les causes de l'incident ou de l'attaque et pour éviter qu'il se reproduise ou se prolonge. Ces opérations sont faites de manière à limiter les conséquences de l'incident ou de l'attaque.*
L'entité met en œuvre les mesures techniques d'isolation, de configuration et de renforcement de la sécurité nécessaires pour remplir cet objectif. Ces mesures peuvent être complétées si nécessaire par le déclenchement de tout ou partie du PCA ou du PRA.

5.3.4 / Réaliser un retour d'expérience

■ **FINALITÉ : l'entité tire les enseignements des incidents et attaques qu'elle subit pour limiter l'impact de futurs incidents.**

☐ *RECOMMANDATION : l'entité réalise un bilan ponctuel immédiat après tout incident. Elle établit régulièrement le retour d'expérience sur ses incidents et attaques, afin d'identifier les succès, les dysfonctionnements et les pistes d'amélioration.*

5.4 / GARANTIR LA CONTINUITÉ DE SERVICE

■ **FINALITÉ : l'entité assure la continuité de service de ses missions sensibles. L'entité est capable de reprendre ses activités dans un délai défini, à la suite d'un incident ou d'une attaque.**

☐ *RECOMMANDATION : l'entité prépare et met en œuvre l'ensemble des actions préventives ou curatives, ainsi que les moyens correspondants, permettant d'assurer la continuité de l'activité de l'entité suite à une attaque ou à un incident. L'entité prépare et met en œuvre l'ensemble des actions permettant de passer en mode dégradé, voire de suspendre temporairement son activité puis de la reprendre en mode nominal après un incident.*

5.4.1 / Se préparer à un sinistre

■ **FINALITÉ : l'entité est préparée à la survenue d'un incident ou d'un sinistre. Elle planifie le renforcement de la cybersécurité lorsque le niveau de menace augmente.**

☐ *RECOMMANDATION : l'entité a identifié les informations sensibles et les systèmes d'information à protéger. Ses plans de continuité d'activité et de reprise d'activité comportent :*

- *les procédures à mettre en œuvre, la planification et la conduite à tenir pour maintenir les missions sensibles ou reprendre les activités suite à un sinistre,*
- *les scénarios techniques de gestion de crise ou d'incident adaptés à l'entité et aux SI concernés, notamment les procédures permettant de diffuser les solutions de contournement ou les correctifs, y compris en cas d'indisponibilité des réseaux habituellement utilisés,*
- *les scénarios de renforcement de la cybersécurité, qui renforcent la vigilance et la protection des systèmes lorsque le niveau de menace augmente et qui identifient les impacts métiers consécutifs de leur mise en œuvre.*

L'entité établit et met à jour des fiches réflexes permettant aux opérateurs de réagir rapidement face aux incidents et dysfonctionnements. Elle met à jour ses plans de continuité d'activité en fonction de son expérience des incidents qu'elle a subis.

5.4.2 / Garantir la résilience des systèmes

■ **FINALITÉ : les systèmes d'information sensibles sont résilients.**

☐ *RECOMMANDATION : l'entité construit ses systèmes d'information sensibles de manière à garantir leur résilience aux scénarios d'incidents identifiés, de manière à permettre la continuité ou la reprise des missions sensibles de l'entité.*
Elle sauvegarde régulièrement ses journaux, ses données métier et système, et protège ses sauvegardes au même niveau que les données sauvegardées (intégrité, disponibilité et confidentialité). Elle est capable de contrôler ses sauvegardes avant leur restauration pour y détecter d'éventuelles menaces résiduelles (codes malveillants sauvegardés, fichiers détruits, etc.). Elle teste régulièrement la restauration des données sauvegardées.
La fréquence de journalisation doit être adaptée au niveau de criticité du système d'information concerné.

5.4.3 / Réagir face à un sinistre

■ **FINALITÉ : l'entité est en mesure de réagir efficacement face à un sinistre de manière à garantir ses missions sensibles.**

☐ *RECOMMANDATION : l'entité vérifie régulièrement sa capacité à réagir face à un sinistre et à mettre en œuvre ses plans de continuité et de reprise de l'activité, par des tests, des exercices et des entraînements réguliers. Elle est capable d'activer son centre de gestion de crise. Elle prévoit la capacité de mobiliser le personnel nécessaire pour la gestion des crises et anticipe les contraintes de disponibilité associées (astreintes, permanences). Elle s'assure que les moyens qui permettent la gestion de crise et la résilience de ses systèmes d'information sont opérationnels. Elle met en place et maintient les moyens de communication sécurisés (disponibilité, confidentialité, intégrité, non-répudiation) nécessaires à la gestion de crise, et parmi eux des moyens indépendants des systèmes d'information de l'entité.*

6 / ÉVALUER LE NIVEAU DE SÉCURITÉ

FINALITÉ : l'entité connaît le niveau de sécurité de ses systèmes d'information et les vulnérabilités résiduelles réelles de ses systèmes d'information. Elle est entraînée à la gestion de crise.

RECOMMANDATION : l'entité réalise régulièrement des vérifications et audits de la sécurité de ses systèmes d'information, et valide régulièrement ses procédures de gestion de crise par des exercices réguliers.

6.1 / PROCÉDER À DES AUDITS ET DES VÉRIFICATIONS

■ **FINALITÉ : les audits et les vérifications fournissent une évaluation du fonctionnement organisationnel de l'entité et du niveau de sécurité de ses systèmes.**

□ *RECOMMANDATION : l'entité définit et met en œuvre une politique de vérification récurrente et systématique des processus organisationnels de sécurité et des configurations de sécurité de ses systèmes d'information. En complément elle réalise des audits permettant d'évaluer le plus objectivement possible ses processus et ses systèmes d'information, par rapport à son référentiel et à l'état de l'art, et d'identifier d'éventuelles traces d'attaques antérieures. L'entité corrige aussi vite que possible les défauts remontés par les audits et les vérifications. L'entité fait appel à des prestataires d'audit labellisés par l'ANSSI pour réaliser ses audits.*

6.1.1 / Identifier les écarts au référentiel

■ **FINALITÉ : l'entité identifie l'écart entre le niveau de sécurité théorique de son référentiel et le niveau réel de ses systèmes.**

□ *RECOMMANDATION : l'entité établit des référentiels correspondant au niveau de sécurité qu'elle cherche à atteindre et réalise régulièrement des vérifications et des audits pour constater l'écart entre ces référentiels et l'état de ses processus et de ses systèmes. En particulier elle audite ou fait auditer fréquemment la configuration de ses annuaires centraux (par exemple Active Directory en environnement Windows ou annuaire LDAP).*

6.1.2 / Évaluer par rapport à l'état de l'art

■ **FINALITÉ : l'audit détermine si le système ou l'entité comporte des vulnérabilités exploitables par un attaquant.**

□ *RECOMMANDATION : l'entité évalue régulièrement la sécurité de ses systèmes par rapport à l'état de l'art à l'aide d'audits pouvant notamment porter sur la configuration et l'architecture du système d'information, des tests de pénétration du système ou la prise en compte organisationnelle de la cybersécurité dans l'entité.*

6.1.3 / Rechercher des traces de compromission

■ **FINALITÉ : au cours de l'audit ou de la vérification l'entité cherche à déceler tout marqueur évident d'une compromission du système.**

☐ *RECOMMANDATION : lors des audits ou des vérifications sur des systèmes d'information, des traces visibles d'intrusion sont recherchées dans les journaux (antivirus, pare-feu, serveurs, postes de travail, DNS, proxy, etc.), dans les programmes s'exécutant sur les postes de travail et les serveurs ou à l'aide de marqueurs spécifiques (noms de fichiers, domaines DNS malveillants, etc.). De manière plus générale, l'entité recherche des indices d'intrusion ou de compromission lors de ses audits et vérifications.*

6.1.4 / Corriger les problèmes identifiés

■ **FINALITÉ : la vulnérabilité de l'entité est diminuée en corrigeant les problèmes de sécurité identifiés lors des vérifications et des audits.**

☐ *RECOMMANDATION : suite aux audits et aux vérifications, l'entité rédige et met en œuvre des plans d'actions de correction des problèmes identifiés.*

6.1.5 / Mener des audits de sites internationaux

■ **FINALITÉ : l'entité, si elle en dispose, est capable de vérifier le niveau de sécurité de toutes ses implantations placées l'étranger ou de ses interconnexions avec des partenaires étrangers.**

☐ *RECOMMANDATION : l'entité, notamment si elle dispose d'implantations à l'extérieur du territoire national, est capable de mener des audits de ses infrastructures multinationales. Par ailleurs, l'entité inscrit dans ses contrats sa capacité de mener, de faire mener ou de demander les résultats des audits des systèmes d'information de partenaires étrangers situés en France, qui sont interconnectés avec ses propres systèmes d'information.*

6.2 / ORGANISER DES EXERCICES ET DES ENTRAÎNEMENTS

■ **FINALITÉ : les acteurs de l'entité et les acteurs externes concernés par la cybersécurité de l'entité (prestataires, clients, autorités, etc.) réagissent correctement, selon les procédures définies préalablement, lors d'un incident ayant un impact sur les missions sensibles de l'entité.**

☐ *RECOMMANDATION : l'entité organise des entraînements et des exercices, ou participe à des exercices, afin d'entraîner son personnel et de vérifier que des procédures adaptées aux crises sont correctement mises en place et opérationnelles. Les prestataires externes sont inclus dans le périmètre des entraînements et des exercices.*

7 / GÉRER LES RELATIONS AVEC LES AUTORITÉS

FINALITÉ : l'État et l'entité collaborent pour garantir la cybersécurité des systèmes d'information.

RECOMMANDATION : l'entité répond aux sollicitations étatiques et utilise avec efficacité l'expertise étatique qui lui est apportée.

7.1 / SE COORDONNER AVEC LES AUTORITÉS

■ **FINALITÉ : l'État collabore avec l'entité pour augmenter le niveau de cybersécurité de l'entité et de ses systèmes.**

☐ *RECOMMANDATION : l'entité exploite efficacement les informations, conseils et préconisations étatiques pour renforcer sa cybersécurité et celles de ses systèmes d'information sensibles.*

7.1.1 / Être sensibilisé aux risques

■ **FINALITÉ : l'entité prend en considération les risques auxquels l'État la sensibilise.**

☐ *RECOMMANDATION : l'entité prend en compte dans ses analyses de risques les risques qui sont identifiés par les autorités. L'entité consulte les guides publiés par l'ANSSI et les prend en considération dans la sélection des mesures à mettre en œuvre pour réduire les risques précédemment identifiés.*

7.1.2 / Informer les autorités

■ **FINALITÉ : les autorités disposent des informations nécessaires pour coordonner la défense des systèmes d'information.**

☐ *RECOMMANDATION : l'entité communique son annuaire de gestion de crise à l'ANSSI à sa demande.*

7.1.3 / Activer des mesures spécifiques

■ **FINALITÉ : l'entité est capable d'adapter son niveau de protection à la menace en appliquant les mesures préconisées par l'ANSSI.**

☐ *RECOMMANDATION : l'entité est capable d'appliquer à ses systèmes d'information les recommandations des avis et alertes émis par l'ANSSI et identifie l'impact de leur mise en œuvre sur ses activités.*

7.2 / PERMETTRE L'IMPLICATION ÉTATIQUE LORS DE LA GESTION DES INCIDENTS

■ **FINALITÉ : l'aide de l'État permet à l'entité de mieux gérer ses incidents.**

☐ *RECOMMANDATION : l'entité collabore pleinement avec l'État.*

7.2.1 / Mettre en œuvre les plans gouvernementaux

■ **FINALITÉ : l'entité contribue à la mise en œuvre du plan VIGIPIRATE lorsqu'il est activé.**

☐ *RECOMMANDATION : l'entité connaît le plan VIGIPIRATE et s'assure de sa capacité à mettre en œuvre les mesures contenues dans le présent référentiel. Elle maintient à jour les informations contenues dans ses annuaires de crise.*

7.2.2 / Partager les informations sur les incidents

■ **FINALITÉ : l'entité dispose des informations nécessaires pour traiter ses incidents en lien avec la réponse nationale pilotée par l'ANSSI.**

☐ *RECOMMANDATION : l'entité prend en compte les informations relatives aux incidents diffusées par l'ANSSI. Elle met en œuvre l'organisation et les moyens nécessaires pour traiter ces incidents.*

ANSSI - SGDSN - 51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP
Tél : 01 71 75 82 65 - Fax : 01 71 75 82 60