RÉFÉRENTIEL DE MATURITÉ CYBER FONDAMENTAL

-

Comprendre et appliquer

-

15/07/2026

MINISTÈRE
DES ARMÉES
ET DES ANCIENS
COMBATTANTS

Liberté
Égalité
Fraternité

DGA
DIRECTION
GÉNÉRALE
DE L'ARMEMENT

PARTIE 1

-

Principes généraux

Ce document est la propriété exclusive du ministère des armées et des anciens combattants. Il ne peut être reproduit sans son accord direct.

Processus d'élaboration des référentiels

1

L'état et les maîtres d'œuvre industriels de défense se mobilisent dans le contexte **d'économie de guerre**

2

Constitution de plusieurs groupes de travail réunissant acteurs étatiques et industriels de défense

3

Création en 2023 de deux référentiels fondamentaux : sûreté et cyber *

4

Réalisations de guides associés * permettant une montée en maturité progressive

* Référentiels fondamentaux de protection et guides disponibles sur le site armement.gouv.fr

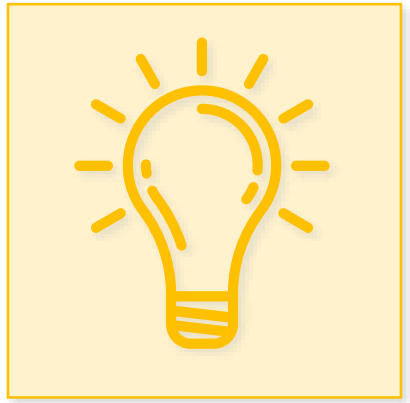
Présentation du référentiel de maturité cyber fondamental

Référentiel conjointement élaboré par la DGA, les experts cyber et services achats des 8 MOI de la convention cyber, en concertation avec l'ANSSI

Objectifs :

1. Augmenter significativement le niveau cyber des entreprises de la défense
2. Leur éviter d'être exclues des marchés internationaux
3. Eviter les **risques d'ingérence** économique

Conçu avec un souci de pragmatisme en proposant des mesures simples et applicables par toute entreprise, quelle que soit sa taille et la nature de ses activités



Référentiel qui devient contractuel et qui anticipe la **mise en œuvre de la directive** européenne NIS 2

Présentation du référentiel de maturité cyber fondamental (2)

Mesures organisationnelles

- Prise en compte du risque cyber
- Identification des informations et actifs sensibles
- Organisation de la cybersécurité
- Sensibilisation des utilisateurs
- Gestion des incidents cyber

Mesures de protection

- Filtrage des points de connexion
- Sécurisation des réseaux sans fil
- Stockage sécurisé des supports
- Protection des équipements mobiles et contre les logiciels malveillants
- Sécurisation des accès aux systèmes d'information
- Contrôle d'accès aux locaux
- Sauvegarde et restauration

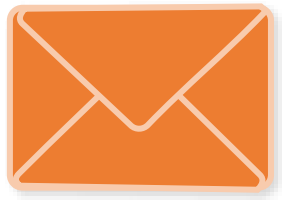
Montée en maturité

1

Évaluer son niveau de sécurité et constater les écarts entre les mesures mises en œuvre et les exigences du référentiel

Mettre en place un plan **d'action** listant les mesures proposées et les jalons calendaires associés

2



3

Contacter si nécessaire les acteurs étatiques (DRSD, DGA) pour être accompagné

Protéger le résultat de l'évaluation par un moyen de chiffrement adapté au contexte

4

Vos contacts étatiques

La DGA est à l'écoute et accompagne les entreprises, notamment via le portail : https://armement.defense.gouv.fr/
La DRSD propose gratuitement et sur simple demande des missions de conseil aux entreprises de la BITD.

MINISTÈRE DES ARMÉES ET DES ANCIENS COMBATTANTS
Liberté
Égalité
Fraternité

DGA
DIRECTION GÉNÉRALE DE L'ARMEMENT

Incident cyber : dga-ext.olid.fct@intradef.gouv.fr

Accompagnement des petites et moyennes entreprises dans leur montée en maturité cyber : dga-did-pme-cyber.contact.fct@intradef.gouv.fr

Conseil cyber et homologations : Contacts de sécurité numérique

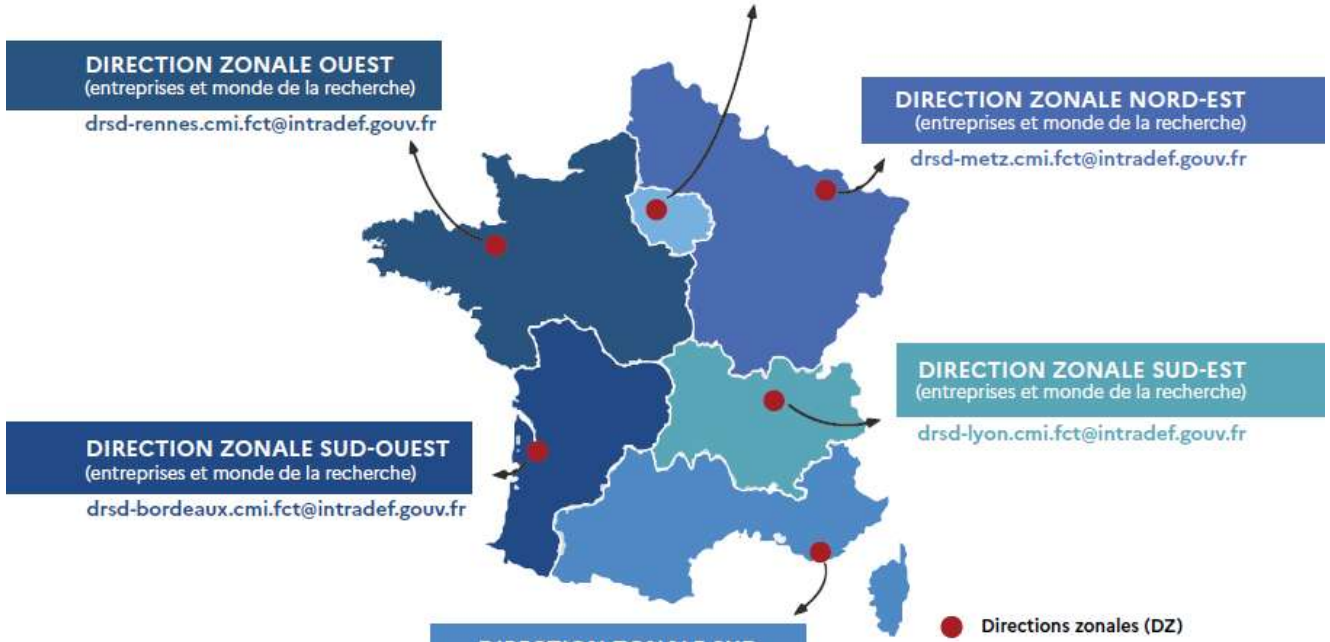
MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Pour contacter la DGSI : securite-economique@interieur.gouv.fr

DIRECTION CENTRALE
Section Sensibilisation
drsd-cie-sensibilisation.contact.fct@intradef.gouv.fr

DIRECTION ZONALE HORS MÉTROPOLE
drsd-dzhm.cmi.fct@intradef.gouv.fr

DIRECTION ZONALE ILE-DE-FRANCE
Entreprises : drsd-dsezp.cmi.fct@intradef.gouv.fr
Écoles et instituts de recherche : prsd-villacoublay.cmi.fct@intradef.gouv.fr



PARTIE 2

-

Présentation des exigences

Ce document est la propriété exclusive du ministère des armées et des anciens combattants. Il ne peut être reproduit sans son accord direct.

Décryptage du questionnaire

Gouvernance (6 exigences)

Gestion du risque	RH / Responsable	Cartographie	Information sensible
1-GOUV-1 « Le risque cyber existe »	3-GOUV-3 « Un responsable cyber »	5-GOUV-5 « Bien Support : de quoi parle-t-on ? »	8-GOUV-6 « Bien Support : Stockage, Chiffrement, Destruction »
2-GOUV-2 « Valeur Métier : lieux, stockage traitement de l'information »	4-GOUV-4 « Sensibilisation des utilisateurs »		

Protection (13 exigences)

Gestion des droits	Contrôle des accès	Durcissement	Accès au site	Equipements
7-PROT-2 « Accès WIFI »	6-PROT-1 « Filtrage Internet »	12-PROT-6 « Mises à jour »	17-PROT-11 « Salles serveurs »	9-PROT-3 « Bien support : antivol et chiffrement »
16-PROT-10 « Les secrets ou les mots de passe »	10-PROT-4 « Accès distant »	13-PROT-7 « Malwares & Autres »	18-PROT-12 « Les visiteurs »	11-PROT-5 « Shadow IT »
19-PROT-13 « Les administrateurs »	15-PROT-9 « Accès gérés par personnes physiques »	14-PROT-8 « Messagerie »		

Défense

Incidents
20-DEF-1 « Plan de gestion des incidents »

Résilience

Sauvegardes
21-RES-1 « Indépendantes »

GOUV

Comprendre l'exigence

1-GOUV-1

L'entreprise intègre le risque cyber dans ses risques et le traite comme un risque majeur tel que l'incendie, le risque financier…

Bénéfices / Risques couverts

- L'entreprise prend conscience de ses potentielles vulnérabilités, s'organise en conséquence.
- Une gestion globalisée des risques permet d'assurer la cohérence du traitement des risques Cyber avec les autres domaines.
- L'identification des acteurs internes ou externes qui peuvent aider l'entreprise en cas de crise cyber permet une plus grande réactivité.
- La prise en compte du risque cyber peut constituer un avantage concurrentiel et permet de rassurer les clients.
- L'évaluation des risques contribue à adapter les investissements au juste niveau et à maîtriser les coûts.

Facilités de mise en œuvre

- De la documentation est disponible : référentiel de maturité cyber DGA, guide d'hygiène informatique et cybersécurité pour les TPE/PME (ANSSI).
- Des spécialistes du domaine peuvent accompagner les TPE/PME.

“ **Le coût de votre sécurisation afin d'éviter une cyberattaque sera toujours inférieur** au coût que pourra représenter une telle attaque pour votre entreprise. ”

GOUV

1-GOUV-1

Appliquer l'exigence

L'entreprise intègre le risque cyber dans ses risques et le traite comme un risque majeur tel que l'incendie, le risque financier…

MonAide Cyber

DIAG CYBERSÉCURITÉ

La démarche à suivre

Le guide AMRAE-ANSSI « maîtrise du risque numérique » propose une démarche type, que chaque entreprise peut adapter simplement à ses spécificités :

- Prendre la mesure du risque numérique ;
- Comprendre le risque numérique et s'organiser ;
- Bâtir son socle de sécurité ;
- Piloter son risque numérique et valoriser sa cybersécurité.

Mettre en place le premier niveau de gouvernance

- La gouvernance mise en place doit être formellement endossée par l'entreprise, au même niveau de responsabilité que la gestion des autres risques majeurs (incendie, finances, sécurité des personnes…).
- Un écosystème existe et peut accompagner les TPE/PME (MonAideCyber, Cybermalveillance.fr, compagnies d'assurance, dispositifs d'aide régionaux ou nationaux…).
- Le recours à un prestataire spécialisé permet une approche professionnelle de la gestion des risques numériques. Il est recommandé de faire appel à des PACS (Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information) qualifiés par l'ANSSI.

GOUV

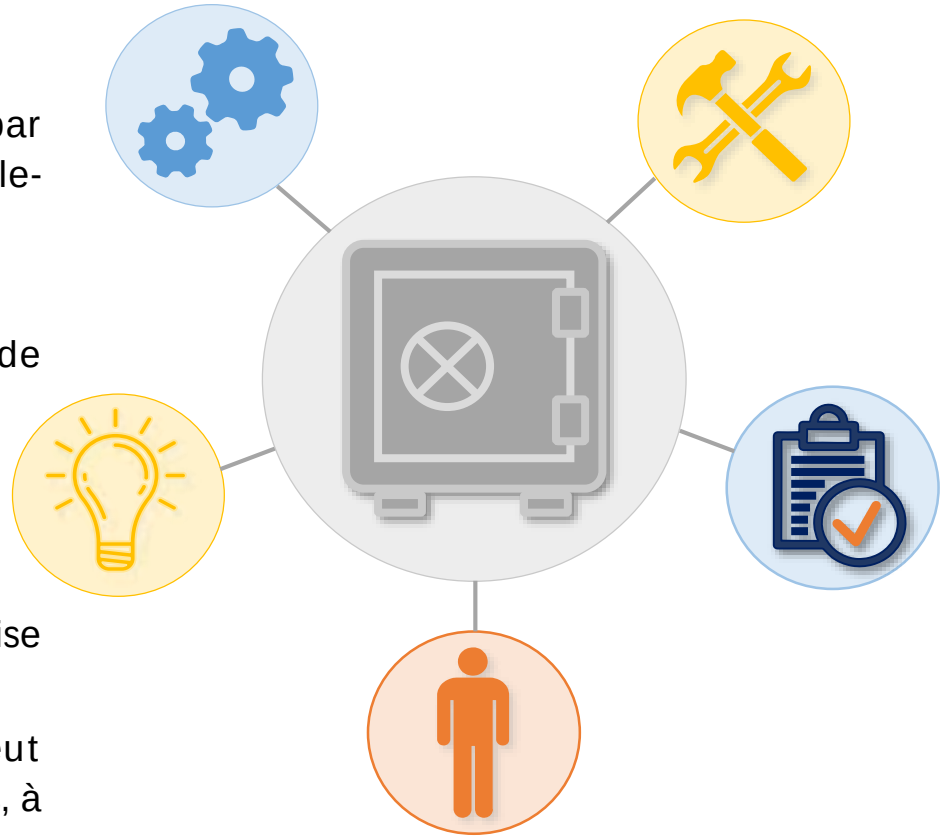
Comprendre l'exigence

2-GOUV-2

L'entreprise effectue une analyse de la sensibilité de ses informations et maintient une liste des informations sensibles, de leurs lieux de stockage et de traitement.

Bénéfices / Risques couverts

- L'entreprise prend conscience des données stratégiques dont l'accès par un tiers hostile pourrait nuire à ses clients, à ses fournisseurs ou à elle-même.
- Identifier ses propres faiblesses permet de mieux se défendre.
- Ce travail d'identification contribue à l'élaboration d'une politique de sécurité adaptée.



Facilités de mise en œuvre

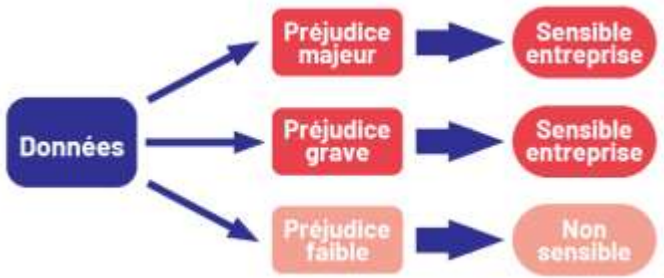
- Ce travail est à la portée des acteurs métier, il n'exige pas une expertise en cybersécurité.
- Il ne nécessite pas le recours obligatoire à des outils complexes et peut consister dans les cas les plus simples à réaliser des évaluations rapides, à l'aide de moyens légers.

> **La connaissance des informations sensibles et de leur localisation permet d'adapter** les mesures de protection au juste niveau.

Appliquer l'exigence

L'entreprise effectue une analyse de la sensibilité de ses informations et maintient une liste des informations sensibles, de leurs lieux de stockage et de traitement.

Détermination de vos données sensibles



La sensibilité de ses données peut être caractérisée en fonction du préjudice potentiel qui pourrait résulter de leur divulgation, indisponibilité ou altération.

Vous pouvez vous référer au guide à usage des entreprises d'identification des données sensibles visées à l'article 1er de la loi dite de blocage.

N'oubliez pas de respecter la réglementation en matière d'information protégée :

Reportez-vous à la fiche réflexe Chiffrement de la DGA pour l'envoi de données sensibles ou DR.

Modalités de mise en œuvre

Adaptez, par exemple, l'atelier 1 d'EBIOS-RM pour hiérarchiser vos informations sensibles :

- Définissez le périmètre de l'analyse en identifiant les processus ou activités métiers qui manipulent des fichiers critiques et autres bases de données en tant que valeurs métiers ;
- Établissez une liste exhaustive des documents comme des biens supports associés à ces valeurs métiers ;
- Identifiez les événements redoutés spécifiques à ces documents.

EBIOS RISK MANAGER

https://cyber.gouv.fr/securisation/analyse-des-risques/methode-ebios-rm/
https://club-ebios.org/site/approche-flash-de-la-methode-ebios-risk-manager/

Comprendre **l'exigence**

Un responsable des sujets cybersécurité est désigné par la direction de l'entreprise et lui rend compte directement. Il dispose des moyens permettant de couvrir les risques cyber.

Bénéfices / Risques couverts

- Cette nomination permet d'assurer la cohérence et la constance de l'effort dans la définition et la mise en œuvre de plans d'action satisfaisant à la couverture des risques cyber.
- Elle permet de faciliter et d'accélérer les échanges avec les services étatiques susceptibles d'apporter leur soutien en cas d'incident.
- Elle rend la communication interne et externe plus cohérente sur les sujets cyber.

Facilités de mise en œuvre

- Ce rôle ne doit pas nécessairement être attribué à un spécialiste technique.
- L'impact RH peut être très faible si le rôle est détenu par le responsable informatique ou le responsable d'organisme.

“ **Disposer d'un responsable pour les sujets cyber est une mesure organisationnelle** qui évite la dispersion des efforts et tient la direction informée au juste niveau. ”

3-GOUV-3

Appliquer l'exigence

Un responsable des sujets cybersécurité est désigné par la direction de l'entreprise et lui rend compte directement. Il dispose des moyens permettant de couvrir les risques cyber.

Choisir le bon profil

- La désignation du responsable cyber est prise formellement au niveau du dirigeant de l'organisme, et doit être accompagnée d'une description de ses missions.
- Sans être nécessairement un spécialiste de la sécurité numérique, le responsable désigné doit présenter une certaine appétence pour ce domaine, et être en mesure de communiquer avec les spécialistes correspondant.
- Dans les petites structures, le chef d'organisme peut assumer cette fonction.

S'inspirer d'exemples

Les missions du responsable cyber peuvent être établies en s'inspirant des sources suivantes, en les adaptant aux enjeux et obligations réglementaires de l'entité :

- L'IM 900 – Fiche 2.6 ;
- Le « Panorama des métiers de la cybersécurité » (Syntec Numérique – ANSSI) – Fiche RSSI (responsable de la sécurité des systèmes d'Information) et sa déclinaison en PME / TPE.

GOUV

4-GOUV-4

Comprendre **l'exigence**

Chaque utilisateur des systèmes d'information reçoit une sensibilisation aux risques cyber et aux bons comportements à adopter.

Bénéfices / Risques couverts

- Le facteur humain est un enjeu majeur de la cybersécurité, vecteur important pour les intrusions numériques.
- La sensibilisation aux menaces et bonnes pratiques permet de réduire significativement le risque, notamment vis-à-vis de la cybercriminalité opportuniste.

Facilités de mise en œuvre

- Le format est laissé à l'appréciation de la société concernant le document précisant les consignes (note, guide, affiche, etc.).
- Il existe des supports disponibles, comme le Guide d'hygiène de l'ANSSI ou la Lettre d'information économique de la DRSD.

“ **La sensibilisation permet de transformer l'utilisateur réputé maillon faible, en un acteur de** la cybersécurité. ”

4-GOUV-4

Appliquer l'exigence

Chaque utilisateur des systèmes d'information reçoit une sensibilisation aux risques cyber et aux bons comportements à adopter.

Ressources accessibles

- Le site cybermalveillance.gouv.fr met à disposition SensCyber : un dispositif de e-sensibilisation à la cybersécurité gratuit et accessible à tous, conçu pour adopter les bonnes pratiques cyber et les partager avec son entourage, composé de définitions illustrées, de quiz ou de séquences interactives (modules de 25 à 45 minutes).
- Des solutions globales de sensibilisation existent dans le commerce qui peuvent être adaptées à votre environnement avec des campagnes d'hameçonnage sur mesure.

Mises en œuvre possibles

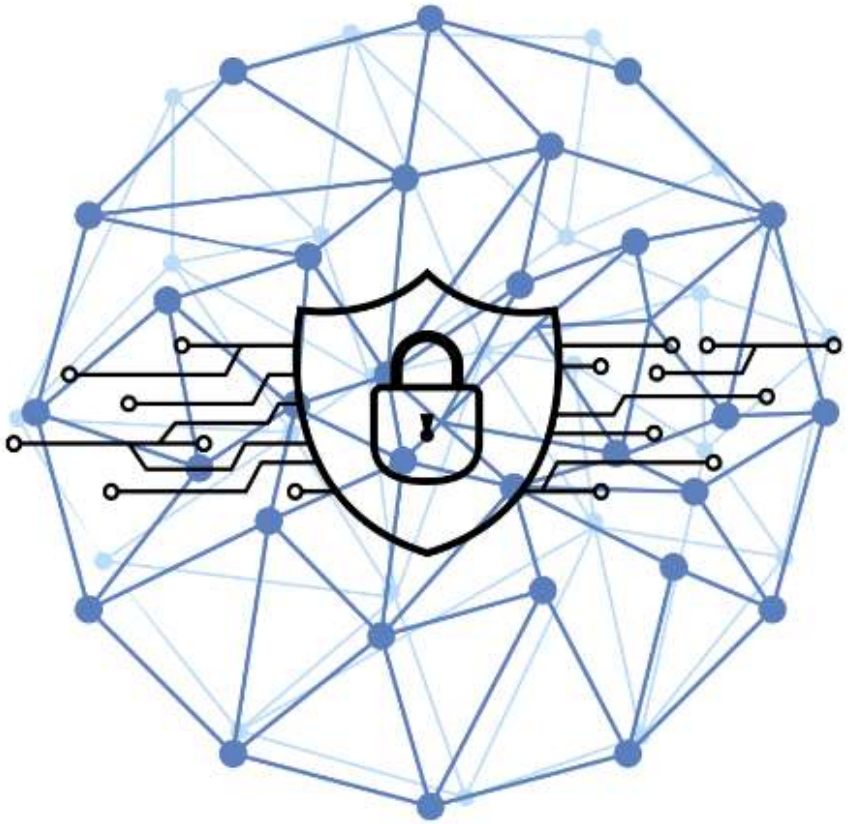
- Mettre à disposition de tous les salariés des vidéos de e-learning et terminer la sensibilisation avec un questionnaire qui aboutira à la délivrance d'un certificat ;
- Organiser des campagnes de simulation d'hameçonnage tout au long de l'année pour garder les salariés attentifs aux messages qu'ils reçoivent ;
- Effectuer des prestations récurrentes de sensibilisation en faisant appel à un organisme étatique ou à un prestataire extérieur. Le recours à un prestataire d'accompagnement et de conseil en sécurité des systèmes d'information (PACS) qualifié par l'ANSSI offre des garanties de compétences en protection des systèmes d'information.

GOUV

Comprendre **l'exigence**

5-GOUV-5

L'entreprise identifie les actifs support (postes de travail, serveurs, machines-outils, connexions réseaux...) et maintient à jour cet inventaire. Elle entretient une cartographie orientée sécurité numérique.



Bénéfices / Risques couverts

- La connaissance à jour du système d'information de l'entreprise est un préalable à toutes les actions de sécurité.
- Elle permet d'identifier les besoins de sécurité au juste niveau.
- Elle permet une plus grande réactivité dans la prise en compte des vulnérabilités nouvelles et dans le déploiement de correctifs adaptés pour maintenir le niveau de sécurité.

Facilités de mise en œuvre

- Identification simple des supports (étiquette autocollante, numérotation unique, etc.).
- Format laissé à l'appréciation de la société concernant le document Inventaire (Tableur, etc.).
- Contrôle facilité du parc numérique par certains logiciels spécialisés.

“On ne peut sécuriser au bon niveau que ce que l'on connaît.”

GOUV

Appliquer l'exigence

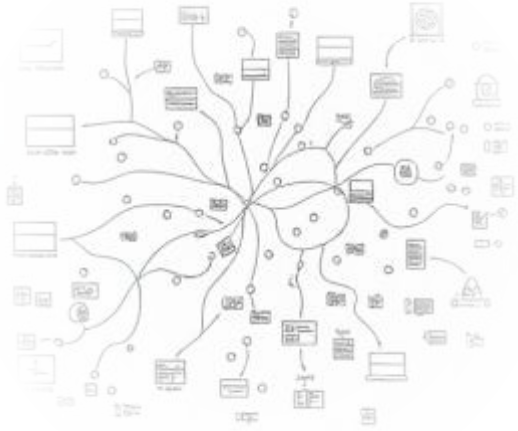
5-GOUV-5

L'entreprise identifie les actifs support (postes de travail, serveurs, machines-outils, connexions réseaux...) et maintient à jour cet inventaire. Elle entretient une cartographie orientée sécurité numérique.

Ressources disponibles

L'exigence s'appuie sur le guide « Cartographie » de l'ANSSI qui prévoit 3 niveaux de granularité.
https://messervices.cyber.gouv.fr/documents-guides/20181213_anssi_guide_cartographie_v1b.pdf
Le RMC-F vise les informations correspondant à la granularité minimale de niveau 1 (annexe 1 du guide).

Modalités de mise en œuvre



Principaux objectifs :

- Identifier les informations et serveurs les plus sensibles et maintenir un schéma des réseaux ;
- Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour ;
- Inclure les schémas des réseaux, avec les connexions internes et externes.

Une cartographie pourra s'appuyer sur un outil qui doit satisfaire les besoins suivants :

- Constituer l'inventaire ;
- Réaliser les vues et représenter les liens entre elles ;
- Mettre en œuvre et contrôler le processus de maintien à jour de la cartographie.

L'entreprise peut se faire aider par un professionnel, en particulier un prestataire d'aide à la cybersécurité (liste des PACS disponible : https://cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/services-de-securite-evalue/decouvrir-les-solutions-certifiees-qualifiees/).

GOUV

Comprendre **l'exigence**

8-GOUV-6

Les supports contenant des informations sensibles sont soit chiffrés soit stockés en lieu sûr. En fin de vie, ces supports sont effacés de manière définitive, ou mis au rebut avec destruction physique.

Bénéfices / Risques couverts

- La maîtrise des supports permet de garantir la confidentialité des informations sensibles pour l'entreprise et limite le risque d'espionnage industriel.
- Elle apporte une garantie à l'intégrité des données et évite qu'un acteur hostile ne modifie des paramètres de réglage d'une ligne de production ou les données chiffrées d'une offre commerciale.
- Enfin, elle garantit la disponibilité des données essentielles au fonctionnement de l'entreprise (éléments de paie, prises de commandes, facturation…).

Facilités de mise en œuvre

- Des armoires fermant à clé constituent une première barrière efficace contre la malveillance ou le vol.
- Des conteneurs numériques gratuits permettent de chiffrer les informations sensibles.

> **La maîtrise des supports d'information est une réponse nécessaire à la dépendance de l'entreprise au numérique.**

GOUV

Appliquer l'exigence

8-GOUV-6

Les supports contenant des informations sensibles sont soit chiffrés soit stockés en lieu sûr. En fin de vie, ces supports sont effacés de manière définitive, ou mis au rebut avec destruction physique.

Chiffrement du support

Les systèmes d'exploitation peuvent proposer nativement leurs propres services de chiffrement. D'autres solutions sont recommandées par l'ANSSI :

CRYHOD
FOR DISKS AND LAPTOPS

DATALOCKER
SIMPLY SECURE

Solutions techniques

Effacement de données

blancco

coreutils shred
HDparm

Destruction physique de supports

Suivre la norme ISO 21964, pour les données internes :

		Classe 1		
	Papier	P-1	P-2	P-3
	Taille max. de coupe	Bandes 12 mm	Bandes 6 mm	320 mm²
	Film	F-1	F-2	F-3
	Taille max. de coupe	160 mm²	30 mm²	10 mm²
	Optique	O-1	O-2	O-3
	Taille max. de coupe	2000 mm²	800 mm²	160 mm²
	Magnétique	T-1	T-2	T-3
	Taille max. de coupe	Hors d'état de fonctionner	2000 mm²	320 mm²
	Numérique	H-1	H-2	H-3
	Taille max. de coupe	Hors d'état de fonctionner	Endommagé	Déformé
	Electronique	E-1	E-2	E-3
	Taille max. de coupe	Hors d'état de fonctionner	Divisé	160 mm²

Modalités de mise en œuvre

- Identifier les données sensibles (2-GOUV-2) et rédiger les processus de manipulation, de marquage et de traçabilité des supports physiques et logiques.
- Le chiffrement du support est à privilégier, avec les solutions techniques recommandées, pour faciliter l'effacement ultérieur des données.
- Guide ANSSI – Recommandations relatives au reconditionnement des ordinateurs de bureau ou portables, chapitre 3 « Recommandations concernant la cession d'ordinateurs » : anssi-guide-reconditionnement_ordinateurs_bureau_portables_v1-0.pdf.

Recommandations s'appuyant sur le catalogue de produits et services certifiés, qualifiés, agréés par l'ANSSI, version du 26/06/2026

PROT

6-PROT-1

Comprendre **l'exigence**

Les points de connexion entre le SI et l'internet sont identifiés et maîtrisés. Des dispositifs de sécurité y sont déployés pour se prémunir des attaques.

Bénéfices / Risques couverts

- Internet est un canal principal d'attaques cyber.
- La gestion des flux entrants et sortants contribue à la protection de l'entreprise contre les tentatives d'intrusion et les fuites d'informations.
- Les menaces cyber étant de plus en plus furtives, la maitrise des interconnexions permet de remonter des alertes et de conserver les traces nécessaires pour mettre fin à une attaque ou en réduire les effets.

Facilités de mise en œuvre

- La mise en place et la configuration d'un pare-feu suffit à limiter les flux réseau entrant et sortant au strict nécessaire entre vos équipements et Internet.
- Le routeur Internet peut aussi être sécurisé en le plaçant dans un local ou armoire fermant à clé.
- Des dispositifs de scan existent et permettent de vérifier rapidement votre exposition sur Internet.
- Des solutions complémentaires tels que VPN ou détecteur d'intrusion existent.

> **L'interconnexion est une nécessité mais elle augmente la surface d'attaque. La maîtriser** est donc essentiel pour en tirer tous les bénéfices attendus.

PROT

6-PROT-1

Appliquer **l'exigence**

Les points de connexion entre le SI et l'internet sont identifiés et maîtrisés. Des dispositifs de sécurité y sont déployés pour se prémunir des attaques.

Solution technique

Le recours à un pare-feu qualifié ou certifié par l'ANSSI, offre des garanties de robustesse (en juin 2026, la gamme de firewalls *Stormshield Network Security* est la seule à disposer d'une qualification standard accordée par l'ANSSI).

STORMSHIELD

Modalités de mise en œuvre

- Identifier les flux (entrants et sortants) nécessaires à l'activité de votre entreprise ;
- Configurer le pare-feu pour n'autoriser que les flux utiles entre votre réseau d'entreprise (considéré comme maîtrisé) et Internet (considéré comme hostile). Cette configuration peut aussi être réalisée par un prestataire (ex : PACS qualifié par l'ANSSI) ;
- S'inscrire au service SILENE de l'ANSSI afin de cartographier son exposition à Internet : https://messervices.cyber.gouv.fr/services/silene.html.

PROT

Comprendre l'exigence

Les accès sans fil sont sécurisés.

Seuls les terminaux identifiés sont autorisés sur le réseau sans fil de l'entreprise.

Bénéfices / Risques couverts

- Eviter le piratage de votre réseau Wifi interne.
- Les accès sans fil (Wifi) rendent possible l'accès au réseau interne de l'entreprise depuis l'extérieur des locaux, y compris à des distances importantes moyennant des antennes adaptées.
- Eviter le vol d'informations ou de données sensibles pour votre activité.

Facilités de mise en œuvre

- Changement facile de nom et de mot de passe par défaut de votre routeur Wifi.
- Masquage facile de votre SSID (permet de rendre son réseau invisible).
- Un guide ANSSI est disponible et présente des recommandations relativement simples pour sécuriser votre Wifi.

“Ne facilitez pas l'accès à vos informations et à vos réseaux par des moyens sans fil qui contourneraient les mesures de sécurité que vous avez mises en place en interne de l'entreprise.”

PROT

7-PROT-2

Appliquer l'exigence

Les accès sans fil sont sécurisés.

Seuls les terminaux identifiés sont autorisés sur le réseau sans fil de l'entreprise.

Modalités de mise en œuvre

- Configuration de sécurité : les équipements et systèmes Wifi disposent d'interfaces de configuration permettant un durcissement de la connexion sans fil : activation du chiffrement WPA3, supervision / filtrage des équipements connectés, désactivation en dehors des horaires de bureau… L'accès à l'interface de configuration doit être également sécurisé (mot de passe fort).
- Cloisonnement réseau : si des accès Wifi doivent être mis à la disposition de personnels extérieurs, privilégier un réseau Wifi dédié à cet usage, avec une isolation vis-à-vis des infrastructures de l'entreprise (VLAN, accès internet dédié).
- Contrôle de portée : même si la portée du réseau Wifi dépend du matériel utilisé, une vérification élémentaire de la portée d'un réseau déployé est possible (test de la connectivité depuis l'extérieur). Elle permet d'éviter une couverture trop large, notamment en modifiant l'emplacement des antennes réseau.

Guide

Le guide ANSSI dédié au Wifi de 2013 peut être utilisé comme source d'information, en prenant soin d'utiliser un chiffrement à l'état de l'art : https://messervices.cyber.gouv.fr/documents-guides/NP_Wifi_NoteTech.pdf.

PROT

Comprendre l'exigence

L'entreprise met en place des mesures de sécurisation des équipements mobiles contre le vol physique et le vol de données.

Bénéfices / Risques couverts

- En cas de vol, les données chiffrées et les informations chiffrées permettant l'accès aux systèmes de l'entreprise sont inexploitables par un voleur.
- La mise en place des mesures de sécurité retarde l'intrusion sur l'équipement ou sur les réseaux et permet de disposer de temps pour désactiver les accès au système de l'entreprise.

Facilités de mise en œuvre

- Des solutions automatisables permettent de sécuriser les postes en limitant l'intervention nécessaire de l'utilisateur.
- Des solutions organisationnelles permettent de limiter le risque, comme le recours à des postes dédiés aux réunions externes, dépourvus d'accès à distance et ne comprenant que les données strictement indispensables à la mission.

> La virtualisation ne doit pas faire oublier que les données sensibles, et celles permettant une **connexion à l'entreprise, résident nécessairement sur des supports physiques dont la perte ou le** vol constituent des risques de compromission.

Appliquer **l'exigence**

L'entreprise met en place des mesures de sécurisation des équipements mobiles contre le vol physique et le vol de données.

Consulter les guides et les fiches pratiques

- Des supports synthétiques peuvent être consultés pour comprendre rapidement ce qu'il convient de faire :

  La fiche de la CNIL sur la sécurisation de l'informatique mobile :
  https://www.cnil.fr/fr/securite-securiser-linformatique-mobile

  La fiche réflexe de Cybermalveillance sur la sécurité des appareils mobiles :
  https://www.cybermalveillance.gouv.fr/medias/2020/04/fiche_s%C3%A9curit%C3%A9_appareils_mobiles.pdf

- Leur lecture peut être approfondie en consultant le guide plus complet de l'ANSSI sur le nomadisme numérique :
  https://messervices.cyber.gouv.fr/guides/recommandations-sur-le-nomadisme-numerique

Solutions techniques

Plusieurs produits sont disponibles, commerciaux ou libres, adaptés à des environnements Linux ou Windows, labellisés par l'ANSSI ou recommandés par le SILL (Socle interministériel de logiciels libres) :

PRIMX MAKE ENCRYPTION HAPPEN · DATALOCKER SIMPLY SECURE · VeraCrypt · Windows BitLocker · LUKS Linux Unified Key Setup

Recommandations s'appuyant sur le catalogue de produits et services certifiés, qualifiés, agréés par l'ANSSI, version du 26/06/2026

Comprendre **l'exigence**

Les accès distants au SI de l'entreprise sont sécurisés et nécessitent une authentification forte.

Bénéfices / Risques couverts

- L'authentification multi-facteurs empêche les connexions malveillantes.
- Le VPN rend les interceptions illisibles pour un attaquant.

Facilités de mise en œuvre

- Une partie de la solution est organisationnelle : élaborer une politique de sécurité prévoyant des restrictions de fonctionnalités aux accès distants.
- L'authentification forte représente un tel enjeu qu'il existe de nombreuses solutions disponibles sur le marché.

> Par définition un accès distant ne bénéficie pas des mesures de sécurisation mises en place **localement dans l'entreprise. Il convient donc d'en maitriser l'emploi et d'apporter une garantie supplémentaire à l'authentification des utilisateurs distants.**

Appliquer l'exigence

Les accès distants au SI de l'entreprise sont sécurisés et nécessitent une authentification forte.

Solutions techniques

Le recours à des solutions VPN qualifiées ou certifiées par l'ANSSI, libres ou commerciales, offre des garanties de robustesse :

THEGREENBOW OPENVPN CRYPTOSMART BY ERCOM

Modalités de mise en œuvre

L'authentification multi-facteurs* (Cf. 16-PROT-10) peut s'obtenir avec :

- l'emploi d'un dispositif physique (carte à puce ou *token*) ;
- la combinaison d'un facteur d'authentification complémentaire du mot de passe : clé enregistrée localement, code de validation transmis par SMS ou une application.

(*) MFA en anglais : *Multi-Factor Authentication*

PROT

Comprendre **l'exigence**

Tout équipement se connectant au réseau de l'entreprise doit être fourni ou maîtrisé par l'entreprise. Les utilisateurs n'ont pas de droit administrateur.

Bénéfices / Risques couverts

- La maîtrise de la cybersécurité est impossible sans maîtriser la configuration de tous les équipements se connectant au réseau d'entreprise.
- Un équipement non maîtrisé peut être porteur de code malveillant qui pourrait infecter le système de l'entreprise et établir des interconnexions non sécurisées susceptibles de provoquer la fuite de données sensibles.
- L'interdiction de connecter des équipements inconnus de l'entreprise limite le risque de compromission et d'atteinte à la disponibilité des systèmes d'information.

Facilités de mise en œuvre

- Une partie importante de la solution est organisationnelle, et consiste à définir et faire appliquer des consignes aux employés, aux visiteurs et aux sous-traitants.
- Il existe des mécanismes techniques permettant d'interdire ou de détecter des connexions d'équipements non maitrisés.

“L'entreprise ne peut évaluer le risque, et mettre en place des solutions de sécurisation adaptées, que sur ce qu'elle connaît et maîtrise techniquement.”

PROT

Appliquer l'exigence

Tout équipement se connectant au réseau de l'entreprise doit être fourni ou maîtrisé par l'entreprise. Les utilisateurs n'ont pas de droit administrateur.

Modalités de mise en œuvre

Pour maintenir le contrôle de son parc informatique, il est nécessaire de procéder aux actions suivantes :

- Sensibiliser, former et responsabiliser le personnel sur l'interdiction de connexion de tout équipement non maîtrisé par l'entreprise (4-GOUV-4) ;
- Mettre en place des solutions techniques de restriction et de surveillance (voir infra) ;
- Réaliser régulièrement l'inventaire du parc et les revues de comptes, et conduire des audits de parc (5-GOUV-5).

Solutions techniques

Plusieurs mesures techniques peuvent être prises :

- Verrouillage des ports d'accès au réseau local non affectés, à partir des outils de configuration des équipements réseau ;
- Utilisation d'un outil de suivi des adresses MAC. Des solutions sont disponibles, aucune actuellement ne bénéficiant d'un label de sécurité national ;
- Le recours à des produits de gestion automatisée de parc informatique, dont certains préconisés dans le SILL (Socle Interministériel des Logiciels Libres) :

NEDI

ZABBIX

OCS inventory

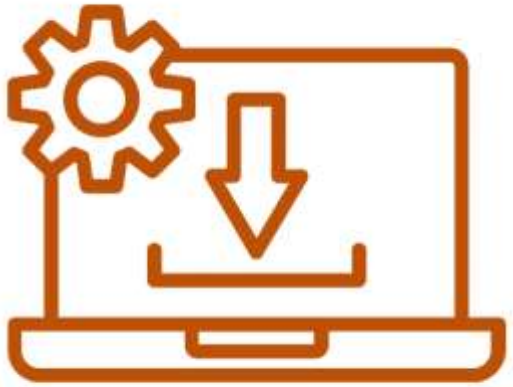
12-PROT-6

Comprendre l'exigence

L'entreprise met en œuvre sans délai les correctifs de sécurité publiés par les éditeurs.

Bénéfices / Risques couverts

Les attaquants exploitent régulièrement les vulnérabilités connues des produits logiciels. Etre à jour permet de se prémunir de ce type d'attaque.



Facilités de mise en œuvre

- La mise en œuvre sera d'autant plus facile que l'inventaire objet de l'exigence 5 sur la gouvernance aura été effectué.
- Les vulnérabilités connues sont publiées sans délai sur les sites spécialisés (CERT-FR, CERT territoriaux, CSIRT sectoriels…) et font l'objet de correctifs mis gratuitement à disposition par les éditeurs.
- Il existe des outils permettant de déployer des correctifs automatiquement sur un parc important (WSUS).

“ **Les attaquants ont généralement une longueur d'avance dans la connaissance des vulnérabilités** des produits et des logiciels. Fermez leur la porte au plus vite ! ”

PROT

Appliquer **l'exigence**

L'entreprise met en œuvre sans délai les correctifs de sécurité publiés par les éditeurs.

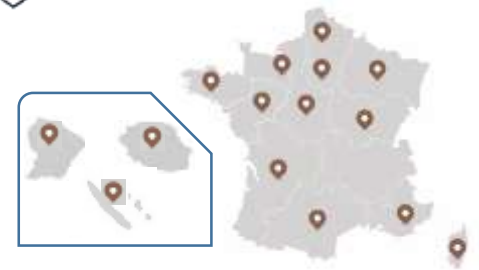
Modalités de mise en œuvre

- Suivre les vulnérabilités critiques, auprès d'un centre de veille et de réponse aux incidents Cyber (CERT-FR, CERT-ED, CERT régional) ;
- Confronter les vulnérabilités signalées avec la cartographie (5-GOUV-5) des systèmes et logiciels utilisés ;
- Adopter en continu les mises à jour disponibles auprès des éditeurs (authentifiées par signature numérique) et anticiper la fin de support des logiciels et systèmes.

Un prestataire externe, de préférence labellisé par l'ANSSI, peut contribuer ou assurer cette exigence (cartographie, identification des mises à jour, et des vulnérabilités critiques).

CERT-FR

CERT [ED]



Les CSIRT territoriaux

Ressources disponibles

Les systèmes d'exploitation se mettent à jour soit sur chaque poste avec une connexion internet, soit par téléchargement et distribution de fichiers de mise à jour certifiés *(Windows Server Update Services* sous *Windows, Content Caching* sous *MacOS,* dépôts *Linux).*

Pour les applications, les catalogues / stores du système d'exploitation permettent une mise à jour globale et efficace.

Une mise à jour systématique et régulière des bases antivirales est indispensable, soit via le logiciel antivirus, soit par téléchargement sur le site de l'éditeur (avec contrôle des signatures).

PROT

Comprendre l'exigence

Une solution de protection contre les logiciels malveillants correctement configurée est mise en œuvre et tenue à jour sur chaque poste de travail et serveur de l'entreprise.

Bénéfices / Risques couverts

- Détecter et neutraliser les intrusions sur votre système d'information.
- Eviter la destruction de votre système d'information, le vol de vos données…

Facilités de mise en œuvre

- Les solutions antivirales sont nombreuses et de mise à jour automatisable.
- Elles sont configurables et adaptables à vos besoins de sécurité : ciblées sur les éléments pertinents.
- Leur emploi s'est démocratisé et nécessite peu d'acculturation des utilisateurs de l'entreprise.

> Ne laissez pas les virus se répandre. **Les antivirus, c'est automatique !**

PROT

Appliquer l'exigence

Une solution de protection contre les logiciels malveillants correctement configurée est mise en œuvre et tenue à jour sur chaque poste de travail et serveur de l'entreprise.

Solutions techniques

Le recours à des solutions de type EDR* qualifiées ou certifiées par l'ANSSI, libres ou commerciales, offre des garanties de robustesse. Ces solutions détectent et endiguent les nouvelles cybermenaces comme les *ransomwares*, avec une efficacité supérieure à celle des antivirus traditionnels.

À défaut d'un EDR, le recours à un antivirus régulièrement mis à jour permet déjà d'éliminer une partie des menaces.

HarfangLab

Endpoint Detection & Response

STORMSHIELD

StormShield Endpoint Security

Modalités de mise en œuvre

L'EDR est une application à installer sur les postes utilisateur et les serveurs de votre entreprise qui permet la détection en temps réel de comportements numériques suspicieux, leur analyse et une réponse automatique adaptée.

(*) *Endpoint Detection and Response* ou service de détection et de réponse pour les terminaux

14-PROT-8

Comprendre **l'exigence**

La messagerie est sécurisée par des équipements ou des services permettant de réduire drastiquement le nombre et la portée des messages malveillants.

Bénéfices / Risques couverts

- La messagerie est le principal vecteur d'infection du poste de travail, qu'il s'agisse de l'ouverture de pièces jointes contenant un code malveillant ou du clic malencontreux sur un lien redirigeant vers un site lui-même malveillant.
- Un filtrage automatique et une analyse antivirus systématique sur les mails permet de prévenir la réception de fichiers infectés.
- Activer le chiffrement TLS permet de garantir la confidentialité et sécurise les échanges de mails sur Internet.

Facilités de mise en œuvre

- Les solutions de filtrage sont généralement intégrées dans les offres des opérateurs.
- Activer le chiffrement TLS entre serveurs de messagerie et entre les postes utilisateurs et le serveur de messagerie est à la portée des services informatiques ou des prestataires.

« La messagerie est une fenêtre utile sur le monde extérieur. Ne laisser pas n'importe qui ni n'importe quoi y passer ! »

Appliquer l'exigence

La messagerie est sécurisée par des équipements ou des services permettant de réduire drastiquement le nombre et la portée des messages malveillants.

Solutions techniques

Les spécifications techniques de l'Internet*, si elles sont respectées dans la mise en œuvre d'une messagerie, permettent de réduire efficacement le nombre et la portée des messages malveillants, grâce à des mécanismes standards d'authentification, de chiffrement et de filtrage éprouvés.

Modalités de mise en œuvre

La sécurisation de la messagerie électronique est présentée dans le chapitre 5 du guide suivant :
https://messervices.cyber.gouv.fr/guides/recommandations-relatives-linterconnexion-dun-si-internet
Le paragraphe 5.4 décrit en particulier le fonctionnement de la protection contre les courriels illégitimes.

Les services de messagerie les plus utilisés implémentent nativement des protections raisonnables, comme du filtrage antispam, mais peuvent nécessiter quelques configurations complémentaires, notamment la mise en place des mécanismes SPF, DKIM et DMARC.

(*) Appelées « RFC » pour *Request For Comments.*

PROT

Comprendre **l'exigence**

Chaque utilisateur est identifié et authentifié individuellement et ne peut accéder qu'aux seules informations, ressources et applications qui lui sont explicitement autorisées.

Bénéfices / Risques couverts

- Limiter le partage des données sensibles aux personnes ayant le droit d'en connaître.
- Limiter le champ d'action d'un éventuel collaborateur mécontent et vengeur ou d'un intervenant extérieur maladroit ou mal intentionné (stagiaire, prestataire externe, sous-traitant…).
- Permettre d'imputer les actions malveillantes internes et d'y mettre un terme plus rapidement.

Facilités de mise en œuvre

- Politique d'accès aux ressources partagées découlant logiquement de l'organisation de l'entreprise et de ses règles plus générales de gestion de projets.
- La plupart des progiciels intègrent la pratique des comptes individuels.
- Un annuaire technique d'entreprise permet de centraliser la gestion des droits sur la plupart des ressources, à condition qu'il soit lui-même sécurisé…

“Le facteur humain doit aussi être maîtrisé au travers de la gestion individuelle des droits d'accès aux ressources numériques de l'entreprise.”

PROT

Appliquer l'exigence

15-PROT-9

Chaque utilisateur est identifié et authentifié individuellement et ne peut accéder qu'aux seules informations, ressources et applications qui lui sont explicitement autorisées.

Solutions techniques

La gestion des droits des utilisateurs s'appuie généralement sur un ou plusieurs annuaire(s) LDAP (*Active Directory* pour Microsoft, *Open Directory* pour Apple, *Kerberos* ou *OpenLDAP* pour Linux).

L'ANSSI peut mettre en œuvre gratuitement le service ADS (*Active Directory Security*) d'audit des annuaires *Active Directory*, au bénéfice de certaines entreprises : https://messervices.cyber.gouv.fr/services/ads.html.

Modalités de mise en œuvre

- Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur (⇨ 19-PROT-13) ;
- Authentifier les utilisateurs avant tout accès au système d'information ;
- Configurer une politique différenciée de gestion d'accès aux données (lecture, écriture, suppression, etc.).
- Effectuer régulièrement une revue exhaustive des droits, en particulier ceux avec les privilèges les plus élevés.

PROT

16-PROT-10

Comprendre **l'exigence**

Pour assurer une authentification robuste, l'entreprise met en place une politique de gestion des secrets rendue techniquement d'application obligatoire.

Bénéfices / Risques couverts

- Les mots de passe robustes sont plus difficiles à deviner par ingénierie sociale.
- Leur complexité rallonge sensiblement le temps nécessaire pour les découvrir par méthode de recherche systématique, et apporte un niveau de confiance permettant de les changer moins souvent.
- Ces éléments permettent de garantir que l'élément secret d'un compte n'est connu, accessible en clair ou modifiable que des utilisateurs qui en ont la responsabilité.

Facilités de mise en œuvre

- La plupart des progiciels intègrent des mécanismes permettant d'imposer des règles de composition des mots de passe.
- Un générateur de mots de passe apporte une garantie de complexité. Couplé à un coffre fort numérique qualifié, il permet aux utilisateurs de limiter les efforts de mémorisation tout en conservant le recours à des mots de passe complexes.

> “Le mot de passe constitue la première barrière de sécurisation. Sa robustesse est donc essentielle dans le dispositif global de cybersécurité.”

16-PROT-10

Appliquer l'exigence

Pour assurer une authentification robuste, l'entreprise met en place une politique de gestion des secrets rendue techniquement d'application obligatoire.

Adopter un coffre-fort de mots de passe

Il existe plusieurs solutions de coffre-fort pour générer et stocker des mots de passe robustes, dont certaines font l'objet d'une qualification de sécurité par l'ANSSI.

Sensibiliser

- Au-delà des outils, les comportements restent essentiels, et les séances de sensibilisation doivent permettre de rappeler l'importance d'une gestion rigoureuse des secrets.
- On pourra par exemple s'appuyer sur les conseils de la CNIL en la matière : https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe

Pour aller plus loin…

Le guide de l'ANSSI *« Recommandations relatives à l'authentification multifacteur et aux mots de passe »* préconise une bonne utilisation des secrets, notamment au travers des recommandations R31 à R38 pour ce qui concerne les coffres-forts de mots de passe :

https://messervices.cyber.gouv.fr/guides/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe

PROT

Comprendre **l'exigence**

L'entreprise contrôle, trace et protège l'accès aux locaux, aux salles serveurs et aux locaux techniques.

Bénéfices / Risques couverts

- Ces mesures permettent de limiter l'atteinte à la confidentialité des données, et de réduire le risque de sabotage et de piégeage des équipements (serveurs d'applications ou de stockage, accès réseau, serveur de messagerie, systèmes de sauvegarde…).
- Le traçage des accès joue un rôle dissuasif, en même temps qu'il permet de détecter des actions malveillantes, ou de comprendre leurs mécanismes pour mieux y mettre fin et y remédier.

Facilités de mise en œuvre

- Cette exigence peut être remplie aux moyens de consignes, d'une organisation et de systèmes de protection physique ne nécessitant pas d'expertise cyber.
- Un certain nombre d'équipements sont pré équipés de dispositifs de protection ou de détection d'intrusion (baies informatiques par exemple).

> “Les accès physiques aux locaux offrent des opportunités aux attaquants. Ne leur facilitez pas la tâche.”

PROT

Appliquer **l'exigence**

L'entreprise contrôle, trace et protège l'accès aux locaux, aux salles serveurs et aux locaux techniques.

Cartographie

- Cartographier les locaux de l'entité ;
- Hiérarchiser les différents espaces selon leur niveau de sensibilité ;
- Identifier les vulnérabilités existantes.

Mesures adaptées

- Contrôler les accès aux différents espaces, via des badges à accès différenciés ;
- Badges dotés de codes-couleurs en fonction du statut (visiteur, prestataire, salarié) ;
- Accompagner les visiteurs : 18-PROT-12 ;
- Verrouiller les portes des bureaux et les salles hébergeant des données sensibles ;
- Effectuer des contrôles aléatoires ;
- Installer et sécuriser un système de détection d'intrusion pour protéger l'intérieur des locaux : détection d'ouverture, de choc ou encore de présence, couplés à un système de surveillance vidéo et/ou un système d'alarme, relié à un poste de sécurité.

Le système de surveillance doit être distinct du système d'information de l'entreprise.

PROT

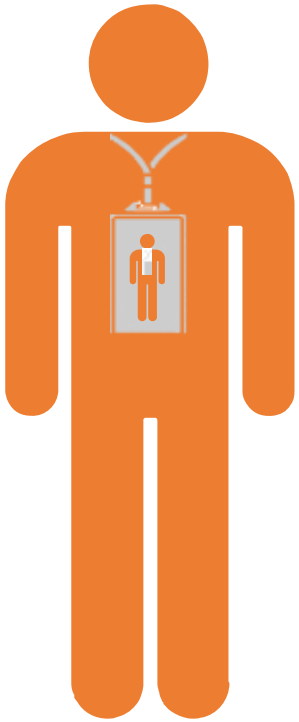
Comprendre **l'exigence**

18-PROT-12

Les visiteurs doivent être enregistrés lors de leur arrivée dans l'entreprise. Ils sont accompagnés, distingués (badge…) et surveillés dans tous les locaux où ils pourraient avoir accès aux SI de l'entreprise.

Bénéfices / Risques couverts

- Les visiteurs constituent une intrusion consentie. A ce titre, ils peuvent avoir accès à des ressources numériques soit mises à leur disposition, soit physiquement atteignable par proximité.
- Dès lors, il convient de prendre en compte les risques d'espionnage, de piégeage ou de sabotage dont ils pourraient être porteurs.
- Les connaître, les accompagner et les distinguer permet de limiter leurs capacités de nuisance ;
- Les visiteurs sont des alliés potentiels, les recevoir de manière maîtrisée c'est aussi leur donner confiance dans votre propre gestion de la sécurité !



Facilités de mise en œuvre

- Mesure essentiellement organisationnelle.
- Support libre pour le registre : il peut être papier ou numérique.
- Cette mesure peut être spécifiée simplement dans les consignes de cybersécurité de l'entreprise.

“ **Les visiteurs n'ont ni les mêmes responsabilités ni les mêmes intérêts que les employés. Dès lors** que vous les accueillez chez vous, démontrez leur votre maîtrise de la sécurité ! ”

PROT

Appliquer **l'exigence**

18-PROT-12

Les visiteurs doivent être enregistrés lors de leur arrivée dans l'entreprise. Ils sont accompagnés, distingués (badge…) et surveillés dans tous les locaux où ils pourraient avoir accès aux SI de l'entreprise.

Cette exigence correspond à l'exigence n°8 du référentiel de sûreté niveau fondamental.

Solutions techniques

Le parcours de notoriété est un circuit préétabli afin d'informer en amont les collaborateurs internes, d'assurer la sécurité de la visite de personnes étrangères à l'entité ainsi que de préparer le programme de cette visite.

Modalités de mise en œuvre

Suivre la fiche réflexe de la DRSD : « Savoir recevoir des visiteurs tout en protégeant son patrimoine ».

PROT

Comprendre **l'exigence**

19-PROT-13

Les comptes usuels des utilisateurs n'ont pas de droits d'administration.

L'administration des systèmes est réalisée avec des comptes individuels spécifiques permettant d'identifier de façon irrécusable l'administrateur.

Bénéfices / Risques couverts

- Les administrateurs sont des acteurs bénéficiant de privilèges particuliers leur permettant de gérer de nombreux droits d'accès à des ressources numériques de l'entreprise (applications, serveurs, messagerie, postes de travail, réseaux, moyens d'authentification…). Distinguer leurs comptes de ceux des utilisateurs est donc impératif pour éviter des élévations de privilèges non maîtrisées.
- Le fait de limiter les droits des utilisateurs au strict besoin permet de limiter l'impact d'une attaque ou d'erreurs de manipulation.
- L'attribution de comptes individuels aux administrateurs permet de les responsabiliser et de limiter les risques de compromission.

Facilités de mise en œuvre

- Les systèmes d'exploitation permettent de créer des comptes individuels et de faire de la ségrégation de droits.
- La répartition des droits d'administrateur découle d'une organisation du travail et d'un partage des attributions relevant d'une responsabilité managériale plus que d'un sujet cyber.

“Les administrateurs ont des privilèges techniques qui peuvent provoquer de nombreux dégâts. On ne protège pas une clé passe-**partout comme n'importe quel trousseau de clés !**”

PROT

Appliquer l'exigence

19-PROT-13

Les comptes usuels des utilisateurs n'ont pas de droits d'administration.

L'administration des systèmes est réalisée avec des comptes individuels spécifiques permettant d'identifier de façon irrécusable l'administrateur.

Modalités de mise en œuvre

- Sécuriser les comptes administrateur par des règles précises d'attribution, une traçabilité des activités et des audits réguliers.
- Découper le système d'information de l'entreprise en zones de confiance soumises à des administrateurs dédiés, auxquels seront attribués des droits selon le principe du moindre privilège.
- Identifier nominativement chaque compte administrateur en fonction du périmètre et des responsabilités associées (fichiers, postes de travail, serveurs…), pour simplifier la revue des droits et la détection d'anomalies.
- Décrire les différents types d'accès et autorisations correspondantes (authentification multifactorielle, audits réguliers, formation des administrateurs…), y compris dans un environnement virtualisé, dans une politique de gestion des comptes d'administration.
- Un compte d'administration doit être exclusivement utilisé à des tâches d'administration. Les autres tâches doivent être réalisées depuis un compte utilisateur sans privilège.

Ressources techniques

Consulter le guide de l'ANSSI « Recommandations relatives à l'administration sécurisée des systèmes d'information » pour :

- Comprendre le rôle clé des administrateurs (chapitre 2) et la notion de zone de confiance (chapitre 3) ;
- Restreindre les droits d'administration sur le poste de travail (recommandation R12) ;
- Identifier, authentifier et gérer les droits d'administration (recommandations R27 à R32).

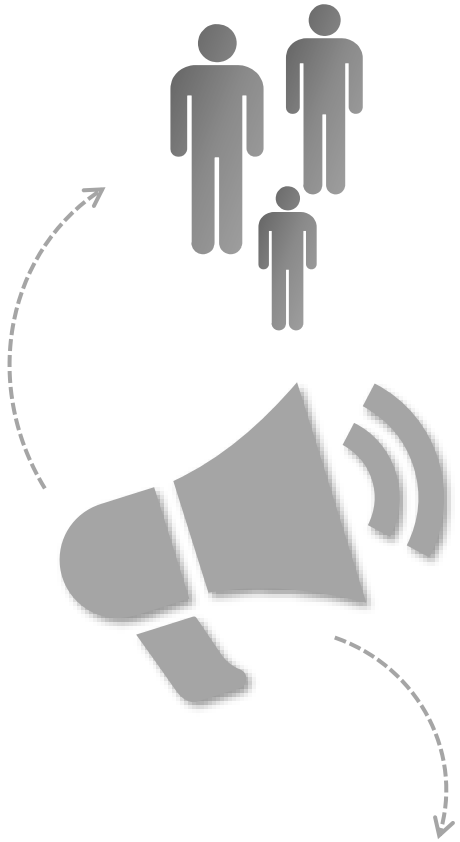
DEF

Comprendre **l'exigence**

20-DEF-1

En cas d'incident cyber sur le SI de l'entreprise, une alerte est envoyée à tous les clients (ou partenaires) potentiellement impactés, dans le respect du secret des affaires.

Les incidents doivent aussi être remontés à l'ANSSI par les fournisseurs français.



Bénéfices / Risques couverts

- Un incident cyber peut impacter directement ou indirectement les données ou les systèmes d'information des clients ou les activités réalisées pour ceux-ci : fuite de données, arrêt de production, problème d'intégrité dans les livraisons, propagation de rançongiciel…
- Prévenir ses partenaires, c'est leur permettre d'anticiper, de détecter la présence d'un attaquant tant qu'il est temps de s'en protéger.

Facilités de mise en œuvre

- Formalisme de compte-rendu relativement simple : date, localisation, type d'incident, description de l'incident, ses conséquences et les éventuelles mesures prises.
- Facilité de transmission : adresse fonctionnelle et plateforme de déclaration disponible sur Internet.

“ **Le partage d'informations relatives aux incidents cyber est une des armes défensives les plus** efficaces contre la cybercriminalité. ”

DEF

Appliquer l'exigence

En cas d'incident cyber sur le SI de l'entreprise, une alerte est envoyée à tous les clients (ou partenaires) potentiellement impactés, dans le respect du secret des affaires.

Les incidents doivent aussi être remontés à l'ANSSI par les fournisseurs français.

En amont de l'incident

- Se préparer à l'aide de la fiche réflexe « Gestion des incidents » ;
- Établir une liste des contacts à prévenir en cas d'incident.

Survenue de l'incident

Déclarer l'incident immédiatement

DGA Bureau LID

CERT [ED]

Traitement de l'incident

- Évaluer l'incident ;
- Le qualifier ;
- Mettre en place des mesures d'endiguement adaptées à l'incident…

… en s'aidant des fiches réflexes de l'InterCERT France

RESI

Comprendre l'exigence

L'entreprise met en place un système de sauvegarde et de restauration des systèmes d'information afin de pouvoir garantir le cas échéant une reprise rapide de son activité.

Bénéfices / Risques couverts

- Une entreprise victime d'un rançongiciel a très peu de chances de se relever de cette épreuve si elle ne dispose pas d'une sauvegarde disponible et fiable, hors ligne.
- Disposer d'une sauvegarde immune permet de recouvrer les données indispensables à la reprise d'activité, par exemple suite à une catastrophe naturelle (sauvegarde distante).

Facilités de mise en œuvre

- Il existe des solutions techniques adaptées aux besoins en capacité de stockage ou en disponibilité et rapidité de restauration.
- Certains hébergeurs proposent des niveaux de services intégrant des sauvegardes sécurisées.
- L'entreprise peut également mettre en place des procédures simples de gestion de supports de sauvegarde déconnectés.

**“La sauvegarde / restauration c'est la roue de secours numérique de l'entreprise.
Elle ne sert à rien tant que vous avez la chance de ne pas crever un pneu en rase campagne…”**

RESI

21-RES-1

Appliquer l'exigence

L'entreprise met en place un système de sauvegarde et de restauration des systèmes d'information afin de pouvoir garantir le cas échéant une reprise rapide de son activité.

Solutions techniques

De multiples solutions techniques de sauvegarde sont disponibles, avec des fonctionnalités variées.

Des solutions libres sont proposées sur le SILL : https://code.gouv.fr/sill/list?search=sauvegarde

Bareos

Duplicati

Modalités de mise en œuvre

- Une politique de sauvegarde définit la fréquence et la durée de conservation des sauvegardes.
- L'automatisation de la sauvegarde est essentielle pour garantir la permanence du service.
- Une sauvegarde régulière sur un support déconnecté est indispensable.
- Le chiffrement de la sauvegarde permet un hébergement distant préservant la confidentialité.
- Des tests de restauration fréquents sont indispensables pour vérifier le bon fonctionnement et mettre à jour les procédures associées.

Ce document est la propriété exclusive du ministère des armées et des anciens combattants. Il ne peut être reproduit sans son accord direct.