LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Agence nationale de la sécurité
des systèmes d'information

Glossaire Sécurité de l'Information

Mars 2026

1 Introduction

L'objectif de ce glossaire est de fournir un ensemble commun et clair de termes liés à la sécurité de l'information. Il vise à faciliter la compréhension des notions utilisées dans les documents de sécurité, afin d'aider les agents à mieux s'approprier les règles et bonnes pratiques associées.

Ce glossaire transversal, utilisable dans l'ensemble des documents relatifs à la sécurité de l'information, contribue à assurer la cohérence entre la *Politique Générale de Sécurité de l'Information* (PGSI), les politiques thématiques et les lignes directrices associées, ainsi qu'à une mise en œuvre cohérente et efficace des mesures de sécurité au sein des entités.

Il s'appuie sur les bonnes pratiques reconnues au niveau international, notamment celles issues de la série de normes ISO/IEC 27000, ainsi que sur les exigences européennes en matière de cybersécurité, comme la directive (UE) 2022/2555 (NIS2). Il tient également compte des recommandations de l'Agence de l'Union européenne pour la cybersécurité (ENISA), notamment les orientations publiées dans le *Guideline on Security Measures under the EECC* (4e édition).

Les définitions proposées ont été rédigées de manière à rester accessibles, tout en couvrant l'ensemble des domaines liés à la sécurité de l'information. Elles sont conçues pour s'adapter aux différents contextes, niveaux de maturité et enjeux des entités publiques, afin de soutenir une mise en œuvre efficace et cohérente des mesures de sécurité.

2 Définitions

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

A

Accès logique et physique :

- Accès logique : accès aux actifs via des moyens numériques (par exemple, authentification à un système).
- Accès physique : mécanisme permettant de limiter, surveiller et enregistrer l'entrée et la sortie des personnes dans des zones protégées, via badges, biométrie, surveillance humaine ou électronique.

Les deux types d'accès devraient être contrôlés, suivis et audités, qu'il s'agisse d'accès aux actifs par des moyens numériques ou d'accès matériel aux équipements ou locaux.

Accès privilégié : Accès accordé à un utilisateur, un système ou un service permettant d'effectuer des actions sensibles ou critiques (ex. : administration système, gestion des comptes, accès aux données confidentielles) qui nécessitent des contrôles renforcés.

Acteur tiers : Toute personne ou entité externe à l'entité (prestataire, sous-traitant, partenaire) ayant un rôle ou un accès aux systèmes d'information ou aux données de l'entité.

Actif (ou asset) : Tout élément, tangible ou intangible, ayant de la valeur pour l'entité. Cela inclut notamment les données et informations, les systèmes, les processus métier, les services (y compris externalisés), les logiciels, les équipements et infrastructures, ainsi que le personnel lorsqu'il détient des connaissances ou compétences essentielles. Un actif peut être matériel, numérique, organisationnel ou

humain, et contribue directement ou indirectement au fonctionnement, à la sécurité ou aux objectifs de l'entité.

Actif informationnel : Un actif informationnel est toute information ayant de la valeur pour l'entité, quel qu'en soit le format ou le support. Cela inclut notamment :

- Les données, contenus, documents, courriels, bases de données, enregistrements audio/visuels ou tout autre contenu informationnel ;
- Les supports, équipements, logiciels, services ou infrastructures associés au traitement, au stockage, à la transmission ou à l'exploitation de cette information, y compris lorsqu'ils sont numériques, physiques ou externalisés ;
- Les services métier et informations qui constituent la valeur primaire à protéger, car ils représentent le cœur des activités, connaissances ou savoir-faire de l'entité.

Un actif informationnel représente généralement l'élément central à protéger car il constitue la ressource informationnelle essentielle à la mission ou aux opérations de l'entité.

Actif informatique : Un actif informatique est un moyen technique ou organisationnel permettant de créer, traiter, stocker, transmettre ou protéger un actif informationnel. Cela inclut par exemple les systèmes, équipements, applications, logiciels, réseaux, infrastructures, supports de stockage, ainsi que les utilisateurs et prestataires qui en assurent le fonctionnement ou la sécurité. Ces actifs sont considérés comme des actifs de support : ils permettent le bon usage et la protection des actifs informationnels.

Actif primaire : Les actifs primaires sont les éléments ayant une valeur directe pour l'entité, généralement liés aux informations et aux processus métiers qui les manipulent.

Actif secondaire (ou de support) : Les actifs secondaires (ou de support) sont les éléments qui soutiennent, hébergent ou protègent les actifs primaires ; il s'agit le plus souvent d'actifs informatiques.

Actif vital : Un actif vital est un actif dont la compromission aurait un impact majeur sur la sécurité de l'information, la continuité des opérations ou la conformité réglementaire.

Appétit pour le risque : Seuil à partir duquel l'entité décide d'accepter un risque comme moyen de traitement, considérant qu'il est tolérable par rapport à ses objectifs stratégiques, opérationnels ou financiers, et qu'il ne nécessite pas d'autres actions pour être atténué.

Authentification : Processus permettant de vérifier l'identité d'un utilisateur, d'un système ou d'une entité avant de lui accorder l'accès à des ressources.

Autorisation : Processus consistant à accorder à un utilisateur, un système ou une entité des droits d'accès spécifiques à des ressources, en fonction de son identité et de ses privilèges.

B

Besoin d'en connaitre : Principe fondamental de sécurité selon lequel l'accès à une information n'est accordé à un agent que si cet accès est indispensable à l'exercice de ses fonctions et de ses missions.

C

Catégorisation du niveau de sensibilité d'un actif : Processus consistant à évaluer la sensibilité d'une information vis-à-vis de son besoin de confidentialité, et à lui attribuer un niveau (ex : « Sensible ») afin de déterminer les mesures de protection adéquates.

Chaîne d'approvisionnement TIC : Ensemble des acteurs ou entités externes (prestataires, sous-traitants, partenaires) impliqués dans la fourniture, le développement, la maintenance ou la mise à disposition de produits ou de services TIC à l'entité, et susceptibles d'avoir un impact sur la sécurité des systèmes d'information ou de l'information.

Chiffrement : procédé consistant à transformer des données en une forme illisible à l'aide d'un algorithme et d'une clé, afin d'en garantir la confidentialité.

Clause de confidentialité : Engagement contractuel imposant à un collaborateur ou un tiers de ne pas divulguer les informations sensibles ou confidentielles auxquelles il a eu accès dans le cadre de ses fonctions.

Clause de sécurité : Disposition contractuelle imposant au fournisseur des obligations spécifiques en matière de sécurité, telles que la notification d'incident, la capacité d'audit, la réversibilité, la suppression des données ou la désactivation des accès.

Confidentialité : Propriété d'une information qui garantit qu'elle n'est ni rendue disponible, ni divulguée à des personnes, des entités ou des processus non autorisés.

Compte d'urgence : Un compte réservé à l'accès rapide et sécurisé à des systèmes ou informations sensibles en cas de crise ou d'incident majeur, permettant de restaurer rapidement les services ou de gérer la situation d'urgence.

Continuité des opérations : Capacité de l'organisation à maintenir ou rétablir ses activités critiques en cas d'incident physique ou environnemental.

Cryptographie : ensemble des techniques permettant de protéger des informations en assurant leur confidentialité, leur intégrité et leur authenticité, notamment à l'aide de mécanismes tels que le chiffrement et les signatures numériques.

Culture de la sécurité de l'information : ensemble des valeurs, des comportements et des pratiques partagés au sein de l'entité visant à intégrer la sécurité de l'information dans les activités quotidiennes de tous les acteurs.

Cycle de vie des actifs : Succession des étapes qu'un actif traverse, depuis son acquisition ou sa création jusqu'à sa restitution, sa suppression ou sa destruction, incluant son utilisation, son stockage, sa maintenance et son transfert.

Cycle de vie RH : Ensemble des étapes encadrant la relation entre l'entité et une ressource humaine : recrutement, intégration, formation, gestion des accès, mobilité, changement de poste, sortie et obligations post-emploi.

D

Développement sécurisé (Secure SDLC) : Approche intégrant la sécurité dès les premières phases du cycle de vie d'un développement logiciel, incluant la conception, la codification, les tests et la mise en production.

Données à caractère personnel : Toute information permettant d'identifier, directement ou indirectement, une personne physique (un nom, un numéro, des données de localisation ou un identifiant en ligne).

E

Environnement à risque élevé : Zone ou contexte présentant une probabilité accrue d'incident (ex : locaux techniques, zones de stockage de données sensibles), nécessitant des mesures de sécurité renforcées.

Environnement de développement, test et production : Espaces techniques distincts dans lesquels les actifs sont utilisés à des fins différentes (développement, validation, exploitation), et devant faire l'objet de contrôles adaptés.

Entretien de sortie : Entretien réalisé lors du départ d'un collaborateur, permettant de rappeler les obligations de sécurité, de récupérer les actifs et d'identifier d'éventuels retours d'expérience.

Evènement de sécurité : un incident de sécurité correspond à une violation ou une menace imminente de violation des politiques de sécurité, des chartes d'utilisation ou des pratiques standards de sécurité.

F

Formation à la sécurité : Ensemble des actions de sensibilisation, d'information ou de formation visant à développer la culture de sécurité des collaborateurs et à leur permettre d'adopter les bons comportements.

Fournisseur : Toute entité externe (prestataire, éditeur, intégrateur, sous-traitant ou partenaire) intervenant dans l'acquisition, le développement, la maintenance ou la fourniture de biens, de services ou de traitements de données à l'entité, et pouvant avoir un impact sur la sécurité du système d'information ou de l'information.

Fournisseur critique : Fournisseur dont les services, prestations ou livrables sont essentiels au bon fonctionnement ou à la sécurité d'un système, d'un processus ou d'un service vital de l'entité, et dont la défaillance pourrait compromettre la confidentialité, l'intégrité ou la disponibilité des actifs vitaux.

G

Gestion des accès : Processus permettant d'attribuer, modifier, révoquer et auditer les droits d'accès physiques ou logiques aux ressources, systèmes, applications et données, en fonction du rôle et des responsabilités de l'utilisateur.

Gestion des actifs informationnels : Ensemble des processus permettant d'identifier, inventorier, classifier, protéger, surveiller, maintenir et supprimer les actifs informationnels tout au long de leur cycle de vie.

H

Aucun terme pour cette lettre.

I

Impact : Conséquence d'un risque sur l'entité, en termes, de confidentialité, d'intégrité, et de disponibilité.

Incident de sécurité de l'information : événement ou série d'événements non souhaités ayant un impact réel ou potentiel sur la confidentialité, l'intégrité ou la disponibilité des informations ou des systèmes d'information.

Infrastructure critique : Ensemble des installations, équipements et systèmes essentiels au fonctionnement de l'organisation (ex : alimentation électrique, réseaux, serveurs).

Inventaire des actifs : Liste structurée et tenue à jour des actifs informationnels de l'entité, incluant leur nature, leur localisation, leur propriétaire, leur classification et leur statut.

J

Journalisation : Enregistrement automatique, manuel ou systématique des événements liés à l'utilisation, à l'accès, à la modification ou aux entrées et sorties concernant un actif ou une zone protégée, incluant notamment l'identité, la date et l'heure, à des fins de traçabilité, d'audit ou de détection d'incidents.

K

KPI : Indicateur de performance clé est une mesure qui permet d'évaluer l'efficacité d'une équipe, d'un projet, d'un processus, etc... dans l'atteinte d'un objectif spécifique.

L

Aucun terme pour cette lettre.

M

Menace : Toute circonstance, situation, action ou événement susceptible de nuire ou de porter atteinte aux réseaux, systèmes d'information ou à la sécurité de l'information, pouvant notamment compromettre la confidentialité, l'intégrité ou la disponibilité, y compris lorsqu'elle provient d'un fournisseur ou d'une chaîne de sous-traitance.

Menace physique et environnementale : Tout événement susceptible de porter atteinte à l'intégrité, la disponibilité ou la confidentialité des actifs physiques (incendie, inondation, sabotage, etc.). Cela inclut notamment les catastrophes naturelles (incendie, inondation, tremblement de terre, tempête), les incidents d'origine humaine (sabotage, vandalisme, vol, actes de terrorisme, troubles civils), les accidents industriels (explosion, émission toxique), ainsi que les défaillances d'infrastructures (coupure d'électricité, panne de climatisation, défaillance des télécommunications, etc.).

Mesure de sécurité : Action, procédure, pratique ou dispositif technique, organisationnel, opérationnel ou contractuel mis en œuvre pour protéger les actifs de l'entité contre les menaces et vulnérabilités, et pour réduire le niveau d'un ou plusieurs risques liés à la sécurité de l'information, y compris dans le cadre de la relation avec les fournisseurs (ex. : tests, audits, clauses contractuelles, outils de contrôle).

Mobilité interne : Changement de poste, de périmètre ou de responsabilités d'un collaborateur au sein de l'entité, nécessitant une réévaluation des accès et des obligations de sécurité.

N

Niveaux de service (SLA) : Engagements contractuels mesurables définissant les performances attendues d'un fournisseur, notamment en matière de disponibilité, de temps de réponse, de traitement des incidents et de conformité aux exigences de sécurité.

Notification d'incident : Obligation pour un fournisseur d'informer l'entité, dans un délai défini, de tout incident de sécurité affectant un système, un service ou des données sous sa responsabilité ou confiés par l'entité.

O

Aucun terme pour cette lettre.

P

Périmètre de sécurité physique : Zone délimitée par des barrières physiques (murs, clôtures, portes sécurisées, etc.) destinée à protéger les actifs sensibles contre les accès non autorisés.

Personne autorisée : Individu ayant reçu une autorisation formelle d'accéder à une zone protégée, selon son rôle et ses responsabilités.

Plan de réversibilité : Ensemble de mesures prévues pour assurer la continuité des services et la protection des données lors de la fin d'un contrat ou de la fin de la relation contractuelle avec un fournisseur, notamment la restitution des données et la désactivation des accès.

Politique de sécurité RH : Document formalisant les exigences, les responsabilités et les mesures de sécurité applicables aux ressources humaines tout au long de leur cycle de vie.

Principe de moindre privilège : Principe selon lequel chaque utilisateur ou visiteur ne dispose que des droits d'accès strictement nécessaires à l'exercice de ses fonctions ou missions.

Principe de séparation des responsabilités : Principe visant à répartir les responsabilités entre plusieurs acteurs afin de limiter les risques d'erreur ou d'abus.

Probabilité : Estimation de la fréquence à laquelle une menace ou un incident est susceptible de survenir.

Procédure d'enregistrement des visiteurs : Processus documenté visant à identifier, enregistrer et accompagner toute personne extérieure accédant aux locaux, incluant la remise de badge temporaire et la consignation des horaires d'entrée/sortie.

Propriétaire d'actif : Personne, rôle ou fonction désigné(e) comme responsable de l'usage, de la protection et de la mise à jour des informations relatives à un actif tout au long de son cycle de vie. Cette responsabilité inclut notamment la définition de la catégorisation du niveau de sensibilité de l'information, l'autorisation des droits d'accès selon le besoin d'en connaître et la définition des exigences de protection appropriées.

Q

Aucun terme pour cette lettre.

R

Résilience : Capacité d'un système ou d'une organisation à résister à un incident, à s'en remettre et à poursuivre ses activités.

Restitution des actifs : Processus de retour, de désactivation ou de suppression des actifs lors de la fin d'un contrat, d'un changement de fonction ou de périmètre, ou de la sortie d'un utilisateur.

Ressource humaine : Toute personne physique (collaborateur, prestataire, consultant, stagiaire, etc.) ayant un rôle actif ou un accès aux systèmes d'information de l'entité.

Revue de sécurité : Évaluation formelle ou informelle des aspects de sécurité d'un projet ou d'un système, pouvant inclure des tests, des analyses de risques ou des contrôles documentaires.

Risques : Le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et de la probabilité qu'un tel incident se produise.

S

Site de secours / PRA / PCA : Site alternatif ou plan permettant de reprendre l'activité (Plan de Reprise d'Activité) ou de la maintenir (Plan de Continuité d'Activité) après un incident majeur.

Sécurité dès la conception : principe consistant à intégrer les exigences de sécurité de l'information dès les phases initiales de conception d'un système ou d'un projet, afin de réduire les risques tout au long de son cycle de vie.

Sensibilisation des agents : Actions visant à développer la connaissance des agents en matière de sécurité de l'information et des comportements attendus.

Sensibilisation fournisseur : Ensemble d'actions visant à informer les fournisseurs des exigences de sécurité de l'entité et à favoriser leur compréhension et leur application.

Stratégie de sortie du cloud : Stratégie définissant les modalités de sortie d'un service cloud, incluant la restitution ou la suppression des données, la continuité des opérations, la réversibilité technique et contractuelle, et la gestion des dépendances critiques.

Structure de gouvernance RH : Dispositif organisationnel (comité, référents, coordination interservices) chargé de piloter la mise en œuvre des mesures de sécurité liées aux ressources humaines.

Support amovible : Dispositif de stockage physique pouvant être connecté, transporté ou utilisé de manière temporaire (ex. : clé USB, disque dur externe), et nécessitant des mesures de sécurité spécifiques.

Système administratif : Un système informatique utilisé pour gérer les tâches administratives d'une organisation.

T

Test d'intrusion : Évaluation de la robustesse des dispositifs de sécurité physique par des tentatives contrôlées d'intrusion.

Traitement des risques : Processus de gestion des risques identifiés. Incluant l'acceptation, la réduction, le transfert, le partage, ou la suppression du risque.

U

Aucun terme pour cette lettre.

V

Vérification d'antécédents : Ensemble des contrôles réalisés avant l'embauche ou la contractualisation d'un individu, visant à s'assurer de sa fiabilité, dans le respect des lois applicables.

Vulnérabilité : Faiblesse, susceptibilité ou faille dans un actif, un produit TIC, un service TIC, un système, un service, un composant logiciel ou matériel, ou un processus (y compris ceux fournis par des tiers), pouvant être exploitée par une menace ou une cybermenace pour compromettre la sécurité de l'information, par exemple en raison d'un défaut de configuration, de l'absence de contrôle d'accès ou d'un code non sécurisé.

W

Aucun terme pour cette lettre.

X

Aucun terme pour cette lettre.

Y

Aucun terme pour cette lettre.

Z

Zone sécurisée : Espace protégé par des contrôles d'accès stricts, une surveillance accrue et/ou des procédures spécifiques pour limiter les risques d'intrusion ou de compromission.

Zone sensible / zone à haut niveau de criticité : Espace physique hébergeant des actifs critiques (ex : salle serveurs, locaux confidentiels) nécessitant des mesures de protection renforcées et des accès strictement contrôlés.