Collecte de preuves

**1. Objet**

**1.1 Finalité**

**1.2 Domaine d'application**

**1.3 Glossaire**

**2. Responsabilité**

**3. Documents**

**4. Exigences de la norme ISO 27001 : 2022**

**5. Déroulement**

Historique

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Toutes | Création | 01/01/2022 |
| **Page** | **Changement** | **Date** |

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité d’assurer une gestion cohérente et efficace des preuves liées aux incidents de sécurité de l'information en vue d'actions disciplinaires et judiciaires.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Collecte de preuve » s’applique au personnel responsable des enregistrements dans notre organisation.

**1.3 Glossaire**

SMSI – système de management de la sécurité de l’information

RSI – responsable sécurité de l’information

Incident (de sécurité de l'information) - événement indésirable et inattendu en matière de sécurité de l'information qui peut compromettre des opérations de l’organisation

SI – sécurité de l’information

Vulnérabilité – faiblesse d’un actif pouvant conduire à un accès non autorisé

**2. Responsabilité**

Le responsable sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de cette procédure. Il est garant de son application. Il a l’appui du directeur.

**3. Documents**

Incidents

Liste de preuves

Vulnérabilités techniques

**4. Exigences de la norme ISO 27001 : 2022**

A.5.28 Collecte de preuves

L’organisation doit établir et appliquer des procédures pour l'identification, la collecte, l'acquisition et la préservation de preuves liées aux événements de sécurité de l'information.

**5. Déroulement**

La gestion des incidents de sécurité de l’information est réalisée selon la procédure Incidents.

Les preuves recueillies aussitôt que possible après l’incident sont conservées dans la Liste de preuves afin de servir pour des actions juridiques envisagées contre des personnes physiques ou morales. Des incidents de sécurité peuvent impliquer des mesures disciplinaires internes à l’organisation. Plus de détails dans le processus Appliquer la discipline.

Les activités de collecte de preuves liées à un incident incluent :

* l’identification
* le recueil
* l’acquisition et
* la préservation

Le recueil des preuves comprend :

* l’applicabilité de la preuve, c'est-à-dire si elles peuvent être utilisées, de manière fiable, pour de futures poursuites pénales
* le poids de la preuve :
  + qualité
  + exhaustivité
* les enregistrements sont complets et n'ont été modifiés d'aucune façon
* les copies des preuves électroniques sont vraisemblablement identiques aux originaux
* tout système d'information à partir duquel des preuves ont été recueillies fonctionnait correctement au moment où les preuves ont été enregistrées

Une certification ou d'autres moyens pertinents de qualification du personnel et des outils sont obtenus, afin de renforcer la valeur des preuves conservées.

Les preuves numériques peuvent dépasser les frontières organisationnelles ou juridictionnelles. Dans de tels cas, il convient de s'assurer que l'organisation est autorisée à collecter les informations requises en tant que preuves numériques.

Il est conseillé d'impliquer un conseil juridique dès le début de toute action en justice envisagée et de prendre conseil sur les preuves requises.