

NORME
INTERNATIONALE

ISO/IEC
27043

Première édition
2015-03-01

Technologies de l'information — Techniques de sécurité — Principes et processus d'investigation sur incident

*Information technology — Security techniques — Incident
investigation principles and processes*

ISO/IEC 27043:2015 - Preview only Copy via ILNAS e-Shop



Numéro de référence
ISO/IEC 27043:2015(F)

© ISO/IEC 2015



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2015, Publié en Suisse

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, l'affichage sur l'internet ou sur un Intranet, sans autorisation écrite préalable. Les demandes d'autorisation peuvent être adressées à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Sommaire

Page

Avant-propos.....	v
Introduction.....	vi
1 Domaine d'application	1
2 Références normatives	1
3 Termes et définitions	1
4 Symboles et abréviations	4
5 Investigations numériques	4
5.1 Principes généraux.....	4
5.2 Principes légaux.....	4
6 Processus d'investigation numérique	5
6.1 Vue d'ensemble des processus.....	5
6.2 Classes de processus d'investigation numérique.....	6
7 Processus de préparation	8
7.1 Vue d'ensemble des processus de préparation.....	8
7.2 Processus de définition du scénario.....	10
7.3 Processus d'identification des sources de preuves numériques éventuelles.....	10
7.4 Processus de planification de la collecte antérieure à l'incident, du stockage et du traitement des données représentant des preuves numériques éventuelles.....	12
7.5 Processus de planification de l'analyse des données antérieure à l'incident représentant des preuves numériques éventuelles.....	12
7.6 Processus de planification de la détection des incidents.....	12
7.7 Processus de définition de l'architecture du système.....	13
7.8 Processus de mise en œuvre de l'architecture du système.....	13
7.9 Processus de mise en œuvre de la collecte antérieure à l'incident, du stockage et du traitement des données représentant des preuves numériques éventuelle.....	13
7.10 Processus de mise en œuvre de l'analyse antérieure à l'incident des données représentant des preuves numériques éventuelles.....	13
7.11 Processus de mise en œuvre de la détection des incidents.....	14
7.12 Processus d'évaluation de la mise en œuvre.....	14
7.13 Processus de mise en œuvre des résultats d'évaluation.....	14
8 Processus d'initialisation	15
8.1 Vue d'ensemble des processus d'initialisation.....	15
8.2 Processus de détection des incidents.....	15
8.3 Processus de première réponse.....	16
8.4 Processus de planification.....	16
8.5 Processus de préparation.....	17
9 Processus d'acquisition	17
9.1 Vue d'ensemble des processus d'acquisition.....	17
9.2 Processus d'identification des preuves numériques éventuelles.....	18
9.3 Processus de collecte des preuves numériques éventuelles.....	19
9.4 Processus d'acquisition des preuves numériques éventuelles.....	19
9.5 Processus de transport des preuves numériques éventuelles.....	19
9.6 Processus de stockage et de préservation des preuves numériques éventuelles.....	19
10 Processus d'investigation	20
10.1 Vue d'ensemble des processus d'investigation.....	20
10.2 Processus d'acquisition des preuves numériques éventuelles.....	21
10.3 Processus d'examen et d'analyse des preuves numériques éventuelles.....	21
10.4 Processus d'interprétation des preuves numériques.....	22
10.5 Processus de consignation.....	22
10.6 Processus de présentation.....	23

10.7	Processus de clôture de l'investigation.....	23
11	Processus simultanés	23
11.1	Vue d'ensemble des processus simultanés.....	23
11.2	Processus d'obtention de l'autorisation.....	24
11.3	Processus de documentation.....	24
11.4	Processus de gestion du flux d'informations.....	24
11.5	Processus de préservation de la chaîne de contrôle.....	25
11.6	Processus de préservation des preuves numériques	25
11.7	Processus d'interaction avec l'investigation physique	25
12	Schéma du modèle du processus d'investigation numérique	25
Annexe A (informative) Processus d'investigation numérique: motif d'harmonisation.....		28
Bibliographie.....		31

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/iso/fr/foreword.html.

Le comité responsable de ce document est l'ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité*.

Introduction

À propos de la présente Norme internationale

La présente Norme internationale fournit des lignes directrices contenant des modèles idéalisés des processus d'investigation communs à travers divers scénarios d'investigation. Elle inclut des processus allant de la préparation antérieure à l'incident jusqu'au retour des preuves (inclus) pour stockage ou diffusion, de même que des conseils et mises en garde d'ordre général concernant les processus ainsi que l'identification, la collecte, l'acquisition, la préservation, l'analyse, l'interprétation et la présentation appropriées des preuves. L'un des principes de base des investigations numériques est la répétabilité, selon laquelle un investigateur doté du savoir-faire requis doit être en mesure d'obtenir le même résultat qu'un autre investigateur doté d'un savoir-faire similaire, travaillant dans des conditions similaires. Ce principe est extrêmement important pour toute investigation d'ordre général. Les lignes directrices de nombreux processus d'investigation sont fournies pour garantir clarté et transparence lors de l'obtention du résultat livré pour chaque processus donné. La raison motivant la fourniture de lignes directrices concernant les principes et processus d'investigation sur incident est indiquée ci-après.

Des lignes directrices établies couvrant les principes et processus d'investigation sur incident faciliteraient les investigations car elles fourniraient un ordre commun des événements composant une investigation. Le recours à des lignes directrices établies permet une transition en toute transparence d'un événement à l'autre au cours d'une investigation. De telles lignes directrices permettraient également une formation adéquate d'investigateurs inexpérimentés. De plus, les lignes directrices visent à garantir la flexibilité au sein d'une investigation en raison du fait que de nombreux types différents d'investigations numériques sont possibles. Des principes et processus d'investigation sur incident harmonisés sont spécifiés et des indications sont fournies concernant la façon dont les processus d'investigation peuvent être personnalisés selon des scénarios d'investigation différents.

Un modèle de processus d'investigation harmonisé est requis dans un contexte de poursuites pénales et civiles, ainsi que dans d'autres environnements, comme les atteintes à la sécurité des informations d'une entreprise et la récupération des informations numériques d'un dispositif de stockage défectueux. Les lignes directrices fournies donnent des préconisations succinctes concernant le processus exact à suivre pendant tout type d'investigation numérique de façon que, en cas de contestation, il convient qu'il ne subsiste aucun doute quant à l'adéquation du processus d'investigation suivi pendant une telle investigation.

Toute investigation numérique requiert un haut niveau d'expertise. Les personnes impliquées dans l'investigation doivent être compétentes, aptes à appliquer les processus utilisés et elles doivent utiliser des processus validés (voir l'ISO/IEC 27041) compatibles avec les politiques et/ou lois pertinentes dans les juridictions applicables.

Lorsqu'il est nécessaire d'affecter un processus à une personne, celle-ci assumera la responsabilité du processus. Par conséquent, une forte corrélation entre la responsabilité d'un processus et la contribution d'une personne déterminera le processus d'investigation exact requis conformément aux processus d'investigation harmonisés fournis en tant que lignes directrices dans la présente Norme internationale.

La présente Norme internationale est structurée selon une approche descendante. Cela signifie que les principes et processus d'investigation sont d'abord présentés de façon globale (abstraite) avant d'être affinés en détail. Par exemple, une présentation globale des principes et processus d'investigation est fournie et présentée dans les figures sous formes de «cases noires» dans un premier temps où chacun des processus globaux est ensuite divisés en processus détaillé (atomique). Par conséquent, une vue moins abstraite et plus détaillée de tous les principes et processus d'investigation est présentée vers la fin de la présente Norme internationale comme il est indiqué à la [Figure 8](#).

La présente Norme internationale est destinée à compléter d'autres normes et documents fournissant des préconisations concernant l'investigation, et la préparation à l'investigation, suite à des incidents de sécurité de l'information. Il ne s'agit pas là de préconisations détaillées, mais d'un guide fournissant plutôt un vaste aperçu de l'ensemble du processus d'investigation sur incident. Ce guide édicte également certains principes fondamentaux visant à garantir que les outils, les techniques et

les méthodes puissent être choisis de manière appropriée et que leur adéquation à l'application visée puisse être démontrée, le cas échéant.

Relation avec d'autres normes

La présente Norme internationale est destinée à compléter d'autres normes et documents donnant des préconisations concernant l'investigation, et la préparation à l'investigation, sur des incidents de sécurité de l'information. Elle ne constitue pas un guide exhaustif, mais édicte certains principes fondamentaux visant à garantir que les outils, les techniques et les méthodes soient choisis de manière appropriée et que leur adéquation avec l'application visée puisse être démontrée, le cas échéant.

La présente Norme internationale vise également à informer les décideurs devant déterminer la fiabilité des preuves numériques qui leur sont soumises. Elle s'applique aux organismes devant protéger, analyser et présenter des preuves numériques éventuelles. Elle est pertinente dans le contexte des organismes en charge de l'établissement de politiques, qui créent et évaluent des modes opératoires en rapport avec les preuves numériques, souvent dans le cadre d'un ensemble plus vaste de preuves.

La présente Norme internationale décrit une partie d'un processus d'investigation complet, portant sans s'y limiter sur les thématiques suivantes:

- gestion des incidents, comprenant la préparation et la planification des investigations;
- traitement des preuves numériques;
- utilisation de l'expurgation et problèmes en découlant;
- systèmes de prévention et de détection des intrusions, comprenant les informations pouvant être obtenues à partir de ces systèmes;
- sécurité du stockage, comprenant le nettoyage du stockage;
- vérification de l'adéquation avec l'application visée des méthodes d'investigation;
- analyse et interprétation des preuves numériques;
- connaissance des principes et processus liés à l'investigation des preuves numériques;
- gestion des événements d'incident de sécurité, comprenant l'établissement de preuve à partir de systèmes impliqués dans la gestion des événements d'incident de sécurité;
- relation entre la découverte électronique et les autres méthodes d'investigation, et utilisation des techniques de découverte électronique dans d'autres investigations;
- gouvernance des investigations, comprenant les investigations forensiques.

Ces thématiques sont couvertes partiellement dans les normes ISO/IEC suivantes:

- ISO/IEC 27037;

La présente Norme internationale décrit les moyens par lesquels les personnes impliquées dans les premières phases d'une investigation, comprenant la réponse initiale, peuvent s'assurer que des preuves numériques éventuelles suffisantes sont recueillies pour permettre de poursuivre l'investigation de manière appropriée.

- ISO/IEC 27038;

Certains documents peuvent contenir des informations dont il ne faut pas qu'elles soient divulguées auprès de certaines communautés. Des documents modifiés peuvent être diffusés auprès de ces communautés, après un traitement approprié du document d'origine. Le processus consistant à supprimer les informations à ne pas divulguer est intitulé l'«expurgation».

L'expurgation numérique des documents est un domaine relativement récent des pratiques de gestion documentaire, qui soulève des problèmes spécifiques et pose des risques potentiels. Lors

de l'expurgation de documents numériques, il faut que les informations supprimées ne soient pas récupérables. Dès lors, il est nécessaire de prendre des précautions pour que les informations expurgées soient supprimées définitivement du document numérique (par exemple il ne faut pas qu'elles soient simplement masquées dans des parties non affichables du document).

La norme ISO/IEC 27038 spécifie les méthodes d'expurgation numérique de documents numériques. Elle spécifie également les exigences concernant les logiciels utilisables pour l'expurgation.

— ISO/IEC 27040;

La présente Norme internationale fournit des préconisations techniques détaillées concernant la manière dont les organismes peuvent définir un niveau approprié d'atténuation des risques grâce à l'emploi d'une approche reconnue et cohérente de la planification, la conception, la documentation et la mise en œuvre de la sécurité de stockage des données. La sécurité du stockage s'applique à la protection (la sécurité) des informations là où elles sont stockées et à la sécurité des informations transférées au moyen des liaisons de communication associées au stockage. La sécurité du stockage comprend la sécurité des dispositifs et des supports, la sécurité des activités de management associées aux dispositifs et aux supports, la sécurité des applications et des services et la sécurité relative aux utilisateurs finaux pendant la durée de vie de leurs dispositifs et supports et après la fin de leur utilisation.

Les mécanismes de sécurité tels que le chiffrement et le nettoyage peuvent affecter la capacité d'investigation d'une personne en mettant en place des mécanismes d'obfuscation. Ils doivent être pris en compte en amont et au cours d'une investigation. Ils peuvent également être importants pour s'assurer que le stockage des matériaux probatoires, au cours et en aval d'une investigation, soit préparé et sécurisé de manière adéquate.

— ISO/IEC 27041;

Il est important de pouvoir démontrer que les méthodes et processus déployés au cours d'une investigation sont appropriés. Ce document fournit des préconisations concernant la façon de s'assurer que des méthodes et processus satisfont aux exigences de l'investigation et ont été soumises à essai de façon appropriée.

— ISO/IEC 27042;

La présente Norme internationale décrit les modes de conception et de mise en œuvre des méthodes et processus à utiliser au cours d'une investigation, afin de permettre une évaluation correcte des preuves numériques éventuelles, l'interprétation des preuves numériques et la consignation pertinente des découvertes.

Les projets ISO/IEC suivants couvrent également en partie les thématiques identifiées ci-dessus et peuvent conduire à la publication de normes pertinentes, suite à la publication de la présente Norme internationale.

— ISO/IEC 27035 (toutes les parties);

Cette norme en trois parties fournit aux organismes une approche structurée et planifiée de la gestion des incidents de sécurité. Elle se compose des parties suivantes:

— ISO/IEC 27035-1;

— ISO/IEC 27035-2;

— ISO/IEC 27035-3;

— ISO/IEC 27044;

— ISO/IEC 27050 (toutes les parties);

— ISO/IEC 30121.

La présente Norme internationale fournit un cadre pour les organes de gouvernance des organismes (comprenant les propriétaires, les membres du conseil d'administration, les directeurs, les partenaires, les cadres dirigeants ou des fonctions similaires), sur la meilleure façon de préparer un organisme aux investigations numériques avant leur occurrence. La présente Norme internationale s'applique au développement de processus (et de décisions) stratégiques concernant la conservation, la disponibilité, l'accès et l'efficacité économique de la divulgation de preuves numériques. Elle s'applique aux organismes de tous types et de toutes tailles. Elle concerne la préparation stratégique avisée d'un organisme à l'investigation numérique. La préparation à l'approche forensique garantit qu'un organisme a engagé une préparation stratégique appropriée et pertinente pour donner son aval concernant des événements potentiels de nature probatoire. Des actions peuvent se produire suite à d'inévitables violations de sécurité, fraudes et déclarations de réputation. Dans chaque situation, les technologies de l'information (TI) doivent être déployées de manière stratégique afin d'optimiser la disponibilité des preuves, leur accessibilité et leur efficacité économique.

La [Figure 1](#) représente les activités types liées à un incident et à l'investigation s'y rapportant. Les références représentées dans la figure (par exemple 27037) désignent les Normes internationales répertoriées ci-dessus; les barres grisées représentent les classes/activités auxquelles chacune d'elles est la plus susceptible d'être directement applicable ou sur lesquelles chacune d'elles exerce une certaine influence sur le processus d'investigation (par exemple en stipulant une politique ou en instaurant des contraintes). Il convient cependant qu'elles soient toutes consultées en amont et au cours des phases de planification et de préparation. Les classes du processus qui sont représentées font l'objet d'une définition complète dans cette Norme internationale et les activités identifiées correspondent à celles évoquées plus en détail dans l'ISO/IEC 27035-2, l'ISO/IEC 27037, et l'ISO/IEC 27042.