

Idioma: Inglés

TÍTULO

Tecnología de la información. Técnicas de seguridad. Directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas (ISO/IEC 27037:2012) (Ratificada por AENOR en diciembre de 2016.)

TÍTULO INGLÉS

Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012) (Endorsed by AENOR in December of 2016.)

TÍTULO FRANCÉS

Technologies de l'information - Techniques de sécurité - Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques (ISO/IEC 27037:2012) (Entérinée par l'AENOR en décembre 2016.)

OBSERVACIONES

En cumplimiento del punto 11.2.6.4 de las Reglas Internas de CEN/CENELEC Parte 2, se ha otorgado el rango de documento normativo español UNE al documento normativo europeo EN ISO/IEC 27037:2016 (Fecha de disponibilidad 2016-08-24)

Este documento está disponible en los idiomas oficiales de CEN/CENELEC/ETSI.

Este anuncio causará efecto a partir del primer día del mes siguiente al de su publicación en la revista AENOR.

La correspondiente versión oficial de este documento se encuentra disponible en AENOR (C/ Génova 6 28004 MADRID, www.aenor.es)

Information technology - Security techniques - Guidelines
for identification, collection, acquisition and preservation
of digital evidence (ISO/IEC 27037:2012)

Technologies de l'information - Techniques de sécurité
- Lignes directrices pour l'identification, la collecte,
l'acquisition et la préservation de preuves numériques
(ISO/IEC 27037:2012)

Informationstechnik - IT-Sicherheitsverfahren -
Leitfaden für die Identifikation, Sammlung, Erhebung
und Erhaltung der digitalen Beweissicherung (ISO/IEC
27037:2012)

This European Standard was approved by CEN on 19 June 2016.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Page

European foreword..... 3

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative reference	1
3 Terms and definitions	2
4 Abbreviated terms	4
5 Overview	6
5.1 Context for collecting digital evidence	6
5.2 Principles of digital evidence	6
5.3 Requirements for digital evidence handling	6
5.3.1 General	6
5.3.2 Auditability	7
5.3.3 Repeatability	7
5.3.4 Reproducibility	7
5.3.5 Justifiability	7
5.4 Digital evidence handling processes	8
5.4.1 Overview	8
5.4.2 Identification	8
5.4.3 Collection	9
5.4.4 Acquisition	9
5.4.5 Preservation	10
6 Key components of identification, collection, acquisition and preservation of digital evidence	10
6.1 Chain of custody	10
6.2 Precautions at the site of incident	11
6.2.1 General	11
6.2.2 Personnel	11
6.2.3 Potential digital evidence	12
6.3 Roles and responsibilities	12
6.4 Competency	13
6.5 Use reasonable care	13
6.6 Documentation	14
6.7 Briefing	14
6.7.1 General	14
6.7.2 Digital evidence specific	14
6.7.3 Personnel specific	15
6.7.4 Real-time incidents	15
6.7.5 Other briefing information	15
6.8 Prioritizing collection and acquisition	16
6.9 Preservation of potential digital evidence	17
6.9.1 Overview	17
6.9.2 Preserving potential digital evidence	17
6.9.3 Packaging digital devices and potential digital evidence	17
6.9.4 Transporting potential digital evidence	18
7 Instances of identification, collection, acquisition and preservation	19
7.1 Computers, peripheral devices and digital storage media	19
7.1.1 Identification	19
7.1.2 Collection	21

7.1.3	Acquisition	25
7.1.4	Preservation	29
7.2	Networked devices	29
7.2.1	Identification	29
7.2.2	Collection, acquisition and preservation	31
7.3	CCTV collection, acquisition and preservation	33
Annex A (informative) DEFR core skills and competency description		35
Annex B (informative) Minimum documentation requirements for evidence transfer		37
Bibliography		38

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27037 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.