PERÚ Ministerio de la Producción

INACAL
Instituto Nacional de Calidad

Alcance general de las NTPs que contribuyen con la Seguridad de la Información (NTP-ISO/IEC 27001, 27002, 27003, 27004 y 27005)

GUSTAVO VALLEJO LA TORRE
Miembro del CTN Codificación e Intercambio Electrónico de Datos

BICENTENARIO PERÚ 2021

ÍNDICE / CONTENIDO

1

Ecosistema en la **SEGURIDAD DE LA INFORMACIÓN**

INSTITUTO NACIONAL DE CALIDAD

ECOSISTEMA SGSI

01

NTP-ISO/IEC 27001:2014
Sistemas de gestión de seguridad de la información. Requisitos

NTP-ISO/IEC 27002:2017
Código de prácticas para controles de seguridad de la información

02

NTP-ISO/IEC 27003:2019
SGSI. Orientación

NTP-ISO/IEC 27004:2018
SGSI. Seguimiento, medición, análisis y evaluación

NTP-ISO/IEC 27005:2018
Gestión de riesgos de la seguridad de la información

03

Privacidad / Cloud

Auditoría

Incidentes

Seguridad de red / aplicaciones

…

04

ISO/IEC 27032:2012
Directrices para ciberseguridad

PTS-ISO/IEC 27100:2021
Ciberseguridad – Revisión general y conceptos

ISO/IEC 27102:2019
Directrices para el ciber seguro

RTP-ISO/IEC TR 27103:2018
Ciberseguridad y normas ISO e IEC

ISO/IEC TS 27110:2021
Directrices de desarrollo del marco de ciberseguridad

ECOSISTEMA SGSI

NTP-ISO/IEC 27001:2014

ISO/IEC 27000:2018

- Privacidad
- Cloud
- Incidentes
- Seguridad de red
- Seguridad de aplicaciones
- Ciberseguridad
- …

NTP-ISO/IEC 31000:2018

NTP-ISO/IEC 27005:2018

NTP-ISO/IEC 27002:2017

NTP-ISO/IEC 27003:2019

NTP-ISO/IEC 27004:2018

2

NTP-ISO/IEC 27001:2014
SGSI. REQUISITOS

INSTITUTO NACIONAL DE CALIDAD

ESTRUCTURA NTP-ISO/IEC 27001:2014

1	Alcance
2	Referencias normativas
3	Términos y definiciones
4	Contexto de la organización
5	Liderazgo
6	Planificación
7	Soporte
8	Operación
9	Evaluación del desempeño
10	Mejoras
Anexo A	Objetivos de control y controles de referencia

SGSI

Características

- Confidencialidad
- Integridad
- Disponibilidad

Activos primarios

- INFORMACIÓN
- Datos personales (privacidad)

Uso de activos secundarios

- Reposo
- Transito
- Uso

3

NTP-ISO/IEC 27002:2017
CÓDIGO DE PRÁCTICAS PARA CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

INSTITUTO NACIONAL DE CALIDAD

ESTRUCTURA NTP-ISO/IEC 27002:2017

1	Alcance
2	Referencias normativas
3	Términos y definiciones
4	Estructura de este estándar
5	Políticas de seguridad de la información
6	Organización de la seguridad de la información
7	Seguridad de los recursos humanos
8	Gestión de activos
9	Control de acceso
10	Criptografía
11	Seguridad física y ambiental
12	Seguridad de las operaciones
13	Seguridad de las comunicaciones
14	Adquisición, desarrollo y mantenimiento de sistemas
15	Relaciones con los proveedores
16	Gestión de incidentes de seguridad de la información
17	Aspectos de seguridad de la información en la gestión de continuidad del negocio
18	Cumplimiento

4

NTP-ISO/IEC 27003:2019
SGSI. ORIENTACIÓN

INSTITUTO NACIONAL DE CALIDAD

ESTRUCTURA NTP-ISO/IEC 27003:2019

		Actividad requerida	Explicación	Guía	Otra información
1	Alcance				
2	Referencias normativas				
3	Términos y definiciones				
4	Contexto de la organización				
5	Liderazgo				
6	Planificación				
7	Soporte				
8	Operación				
9	Evaluación del desempeño				
10	Mejoras				
Anexo A	Marco de referencia para la política				

MARCO DE REFERENCIA PARA LA POLÍTICA

5

NTP-ISO/IEC 27004:2018
SGSI. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

INSTITUTO NACIONAL DE CALIDAD

ESTRUCTURA NTP-ISO/IEC 27004:2018

1	Alcance
2	Referencias normativas
3	Términos y definiciones
4	Estructura y visión general
5	Justificación
6	Características
7	Tipos de mediciones
8	Procesos
Anexo A	Un modelo de medición de la seguridad de la información
Anexo B	Ejemplo de construcciones de medición
Anexo C	Un ejemplo de constructor de medición basado en formato de texto simple

DEFINICIÓN

NTP-ISO/IEC 27001:2014, 9.1

- a) qué necesita ser monitoreado y medido, incluyendo procesos y controles de seguridad de la información
- c) cuándo el monitoreo y medición debe ser realizado
- e) cuándo los resultados del monitoreo y medición deben ser analizados y evaluados
- d) quién debe monitorear y medir
- f) quién debe analizar y evaluar estos resultados
- b) los métodos para monitoreo, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válido

NTP-ISO/IEC 27004:2018

- 6.2 Seguimiento
  6.3 Qué Medir
- 6.4 Cuándo realizar el seguimiento, medición, análisis y evaluación
- 6.5 Quién va a hacer el seguimiento, medición, análisis y evaluación
- 7 Tipos de mediciones
  8 Procesos
- Anexo A Un modelo de medición de la seguridad de la información

- Anexo B Ejemplo de construcciones de medición
- Anexo C Un ejemplo de constructor de medición basado en formato de texto simple

6

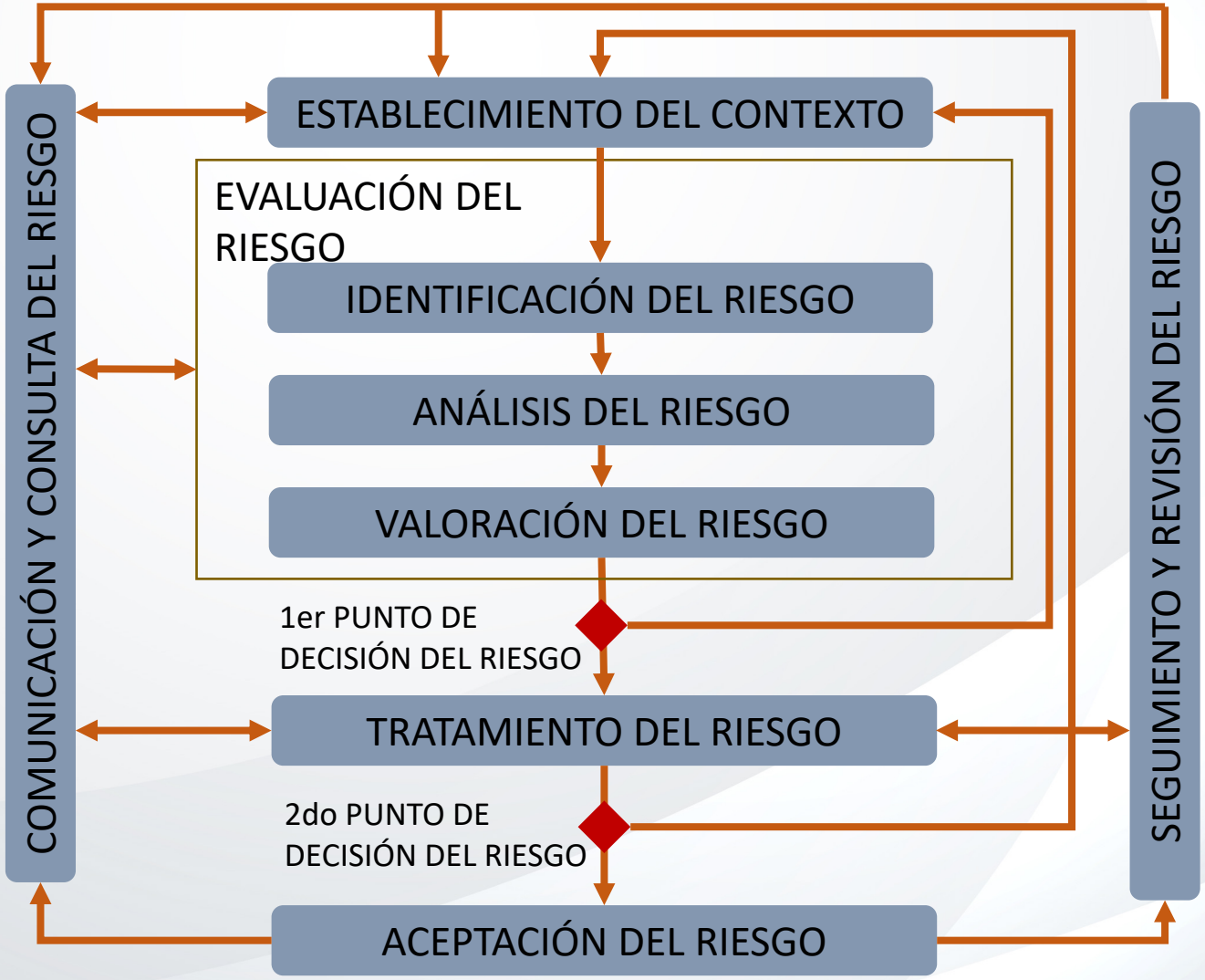
NTP-ISO/IEC 27005:2018
GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

INSTITUTO NACIONAL DE CALIDAD

ESTRUCTURA NTP-ISO/IEC 27005:2018

1	Alcance
2	Referencias normativas
3	Términos y definiciones
4	Estructura de este documento
5	Antecedentes (Background)
6	Descripción del proceso de gestión de riesgos de seguridad de la información
7	Establecimiento el contexto
8	Evaluación de riesgos de seguridad de la información
9	Tratamiento del riesgo de seguridad de la información
10	Aceptación del Riesgo de seguridad de la información
11	Comunicación y consulta del riesgo de seguridad de la información
12	Seguimiento y revisión del riesgo de seguridad de la información
Anexo A	Definición del alcance y límites del proceso de gestión de riesgos de seguridad de la información
Anexo B	Identificación y evaluación de activos y evaluación de impacto
Anexo C	Ejemplos de amenazas típicas
Anexo D	Vulnerabilidades y métodos para evaluación de vulnerabilidades
Anexo E	Enfoques a la evaluación de riesgos de seguridad de la información
Anexo F	Restricciones para la modificación del riesgo

ESTRUCTURA NTP-ISO/IEC 27005:2018



ESTRUCTURA NTP-ISO/IEC 27005:2018

		Entrada	Acción	Guía de implementación	Salida
7	Establecimiento el contexto				
8	Evaluación de riesgos de seguridad de la información				
9	Tratamiento del riesgo de seguridad de la información				
10	Aceptación del Riesgo de seguridad de la información				
11	Comunicación y consulta del riesgo de seguridad de la información				
12	Seguimiento y revisión del riesgo de seguridad de la información				

PERÚ Ministerio de la Producción

INACAL
Instituto Nacional de Calidad

INSTITUTO NACIONAL **DE CALIDAD**

GRACIAS

GUSTAVO VALLEJO LA TORRE

Miembro del CTN Codificación e Intercambio Electrónico de Datos

BICENTENARIO PERÚ 2021

PERÚ Ministerio de la Producción

INACAL
Instituto Nacional de Calidad

Cambios en la nueva edicion de ISO/IEC 27002:2022

Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de la seguridad de la información

Carlos A. Horna Vallejos
Miembro del CTN-EDI
Miembro del ISO/IEC JTC1 SC27/W1

BICENTENARIO PERÚ 2021

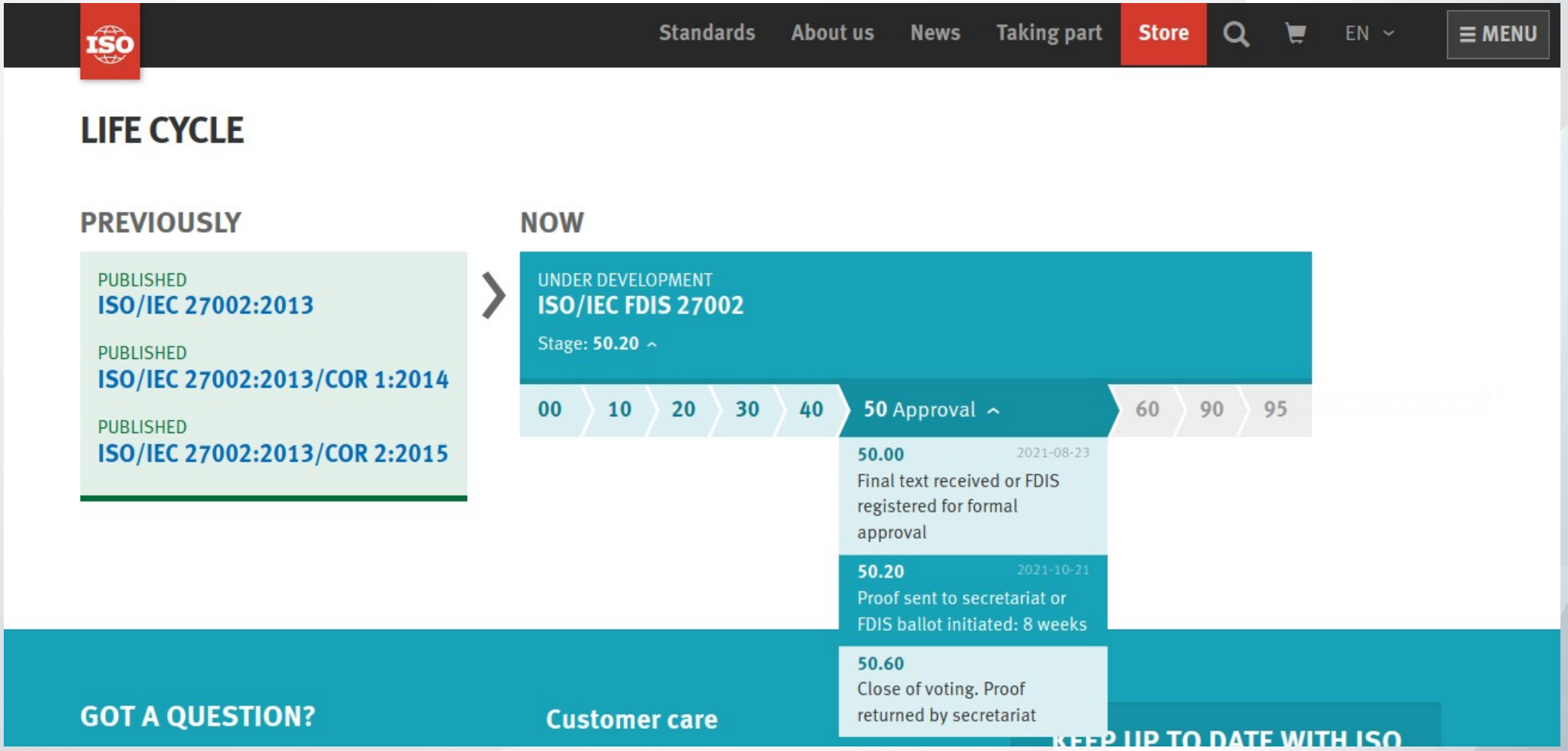
ÍNDICE / CONTENIDO

1

Alcances generales

INSTITUTO NACIONAL DE CALIDAD

Última etapa del proceso de desarrollo

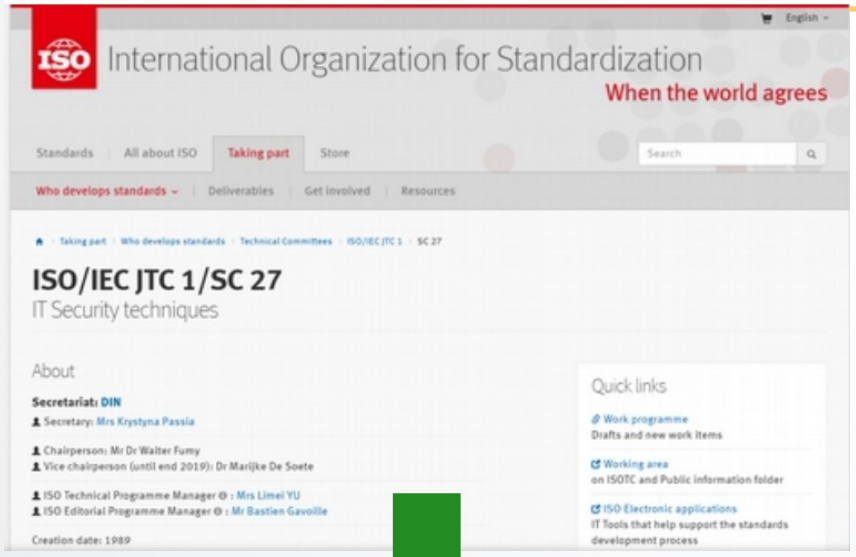


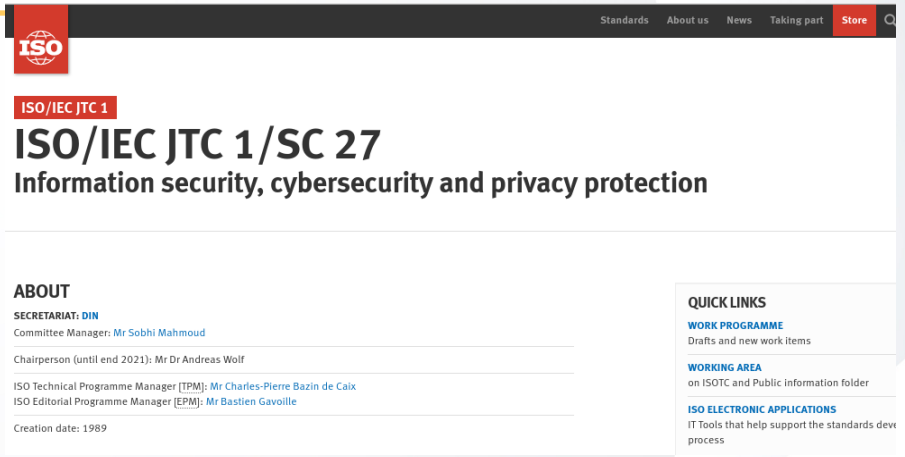
2

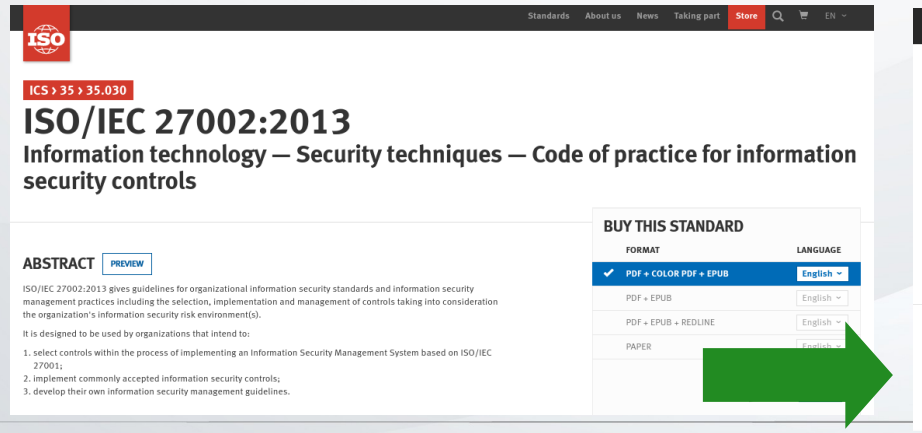
Cambio en el título

INSTITUTO NACIONAL DE CALIDAD

Cambio en el título







3

Estructura de la norma

INSTITUTO NACIONAL DE CALIDAD

Temas

Controles agrupados por temas

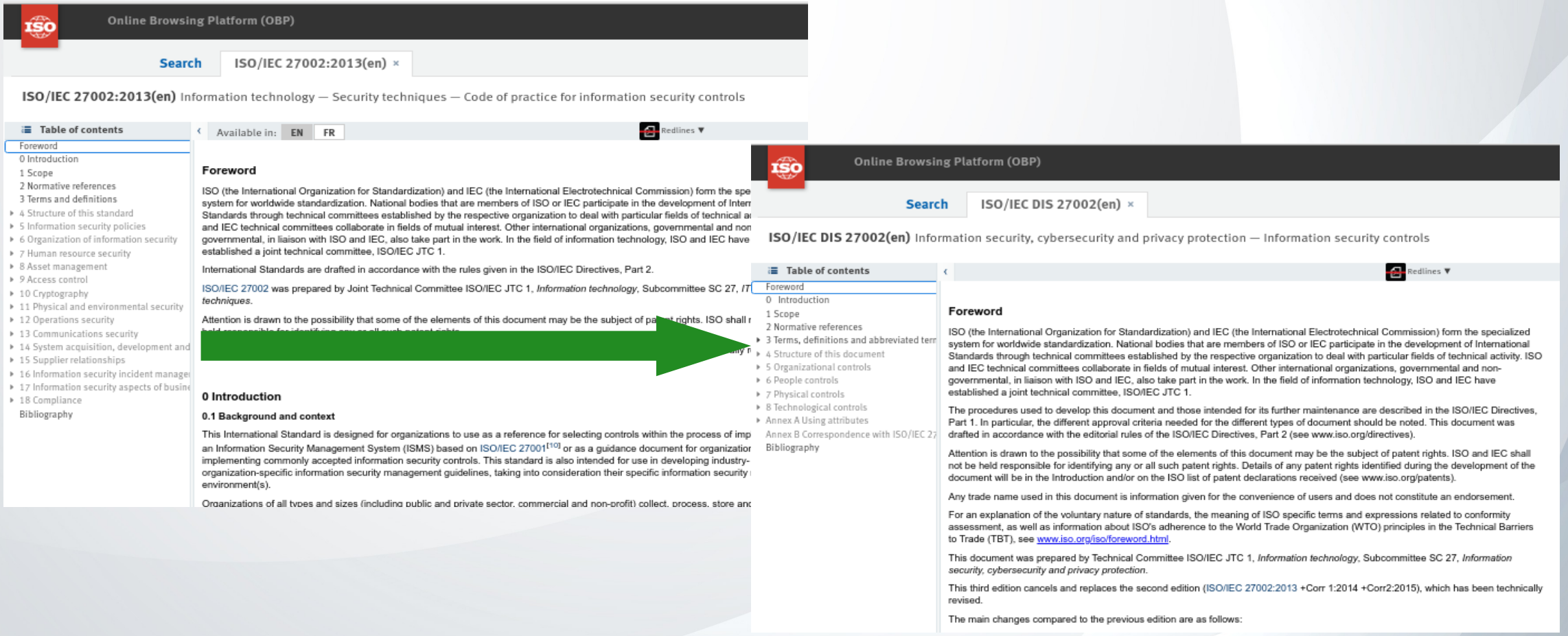
Personas (8)
se refieren a personas individuales

Físicos (14)
se refieren a objetos físicos

Tecnológicos (34)
se refieren a tecnología

Otros (37)
se clasifican como organizacionales

Estructura


Online Browsing Platform (OBP)
Search
ISO/IEC 27002:2013(en)
ISO/IEC 27002:2013(en) Information technology — Security techniques — Code of practice for information security controls
Table of contents
Foreword
0 Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Structure of this standard
5 Information security policies
6 Organization of information security
7 Human resource security
8 Asset management
9 Access control
10 Cryptography
11 Physical and environmental security
12 Operations security
13 Communications security
14 System acquisition, development and
15 Supplier relationships
16 Information security incident manage
17 Information security aspects of busine
18 Compliance
Bibliography
Available in: EN FR
Redlines
Foreword
ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the spe
system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of Intern
Standards through technical committees established by the respective organization to deal with particular fields of technical a
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.
ISO/IEC 27002 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT
techniques.
Attention is drawn to the possibility that some of the elements of this document may be the subject of pa rights. ISO shall
0 Introduction
0.1 Background and context
This International Standard is designed for organizations to use as a reference for selecting controls within the process of imp
an Information Security Management System (ISMS) based on ISO/IEC 27001[10] or as a guidance document for organizatio
implementing commonly accepted information security controls. This standard is also intended for use in developing industry-
organization-specific information security management guidelines, taking into consideration their specific information security
environment(s).
Organizations of all types and sizes (including public and private sector, commercial and non-profit) collect, process, store and
Online Browsing Platform (OBP)
Search
ISO/IEC DIS 27002(en)
ISO/IEC DIS 27002(en) Information security, cybersecurity and privacy protection — Information security controls
Table of contents
Foreword
0 Introduction
1 Scope
2 Normative references
3 Terms, definitions and abbreviated ter
4 Structure of this document
5 Organizational controls
6 People controls
7 Physical controls
8 Technological controls
Annex A Using attributes
Annex B Correspondence with ISO/IEC 27
Bibliography
Redlines
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.
The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).
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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).
Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.
For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.
This document was prepared by Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, Information security, cybersecurity and privacy protection.
This third edition cancels and replaces the second edition (ISO/IEC 27002:2013 +Corr 1:2014 +Corr2:2015), which has been technically revised.
The main changes compared to the previous edition are as follows:

Estructura de los controles (93)

Título del control: Nombre corto del control

Tabla de atributos: Tabla que muestra los valores de cada atributo para el control dado

Control: Descripción del control

Propósito: Texto que explica el propósito del control

Orientación: Guía de implementación para el control

Otra información: Texto explicativo o referencias a otros documentos relacionados.

Atributos

#Preventivo #Detectivo #Correctivo

#Confidencialidad #Integridad #Disponibilidad

#Identificar #Proteger #Detectar #Responder #Recuperar

#Gobernanza #Gestión de activos #Protección_de_información ...

#Gobernanza_y_Ecosistema #Protección #Defensa #Recuperación

Ejemplo

5.6 Contact with special interest groups

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence

Control

The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.

Purpose

To ensure appropriate flow of information takes place with respect to information security.

4

Controles nuevos y el Anexo B

INSTITUTO NACIONAL DE CALIDAD

Controles nuevos

Nuevos

5.7 Inteligencia de amenazas
5.23 Seguridad de la información para uso de servicios cloud
5.30 Preparación TIC para continuidad del negocio
7.4 Monitoreo de seguridad física
8.9 Gestión de la configuración
8.10 Borrado de la información
8.11 Enmascaramiento de datos
8.12 Prevención de fuga de datos
8.16 Monitoreo de actividades
8.22 Filtrado web
8.28 Codificación segura

Reemplazado

11.2.5 Retiro de activos

Anexo B

Correspondencia con ISO/IEC 27002:2013

Table B.1
Correspondencia entre controles de este documento y los controles de ISO/IEC 27002:2013

Table B.2
Correspondencia entre controles de ISO/IEC 27002:2013 y los controles de este documento

PERÚ Ministerio de la Producción

INACAL
Instituto Nacional de Calidad

INSTITUTO NACIONAL **DE CALIDAD**

GRACIAS

Carlos A. Horna Vallejos

Miembro del CTN-EDI
Miembro del ISO/IEC JTC1 SC27/WG1

BICENTENARIO PERÚ 2021