NUEVA ISO27001

De 2013 a 2022

By: Xavier Vila

¿QUIÉN SOY?

https://www.xaviervila.net

linkedin.com/in/xaviervila

PROYECTO: ArMathor.io

QRZ: EA3ISS

Xavier Vila i Espinosa

Actualmente, Responsable de Seguridad de Validated ID y profesor en temas de Seguridad y Privacidad.
Ex consultor de seguridad. Ex PCI QSA. Ex perito tecnologico (ANTPJI, ACPJT i Aspertic). NIS Expert de ENISA.

Ingeniero Técnico en Telecomunicaciones - Telemática – EUPMT/UPC + Eur ING
Postgrado en auditoria técnica y peritaje forense – UOC
Postgrado en Asia Oriental. Experto en economia de Japón – UOC
Postgrado en Dirección de Seguridad Integral – UVic
Máster en Blockchain y sus aplicaciones empresariales – Threepoints + UPC

CERTIFICACIONES ACTIVAS

CISA, CISM, CRISC & CDPSE de ISACA
ISO27001 & ISO22301 Lead Auditor por BSI
CDPP de ISMS Forum
TIP de Jefe y Director de Seguridad Privada por el Ministeri del Interior de España
BSAFE por UN DSS
TCCC/AC por NAEMT

ORGANIZACIONES

Miembro de la Junta de Aspertic y de ISACA Barcelona.
Asesor de Blockchain Catalunya.
Colaborador de BCNSoluciona.

HISTORIA DEL ESQUEMA

Año 1995: BS 7799-1 – Recomendaciones, no certificable.
Año 1998: BS 7799-2 – Requisitos para certificarse.
Año 2002: BS 7799-1:2002 – Versión oficial para acreditarse.
Año 2005: ISO 27001:2005 – Cambio de nombre y pasa a ser internacional.
Año 2007: ISO 27002:2005 – Buenas prácticas del Anexo A.
Año 2013: ISO 27001:2013 – Revisión esquema para acercarlo al anexo SL.
Año 2022: ISO 27002:2022 (Febrero)– Nuevas buenas prácticas - Anexo A.
Año 2022: ISO 27001:2022 (Octubre) – Revisión y actualización esquema.

CALENDARIO ACTUAL

3 años de transición

Publicación ISO27001 – 31 Octubre 2022
Año 2023
Se siguen emitiendo certificaciones ISO27001:2013
No se pueden hacer primeras auditorías o recertificaciones a partir del 31 de octubre de 2024.

Año 2025
TODOS los certificados de ISO27001:2013 caducan el 31 de octubre de 2025

TRANSICIÓN

Antes del 31 de octubre del 2025

Se puede hacer de varias formas:

- Auditoría de recertificación
- Auditoría de revisión anual
- Auditoría especial

Se debe considerar tiempo extra de auditoría para hacer la transición. El tiempo dependerá, entre otros, del tamaño de la empresa, complejidad del alcance de la auditoría, etc.

CAMBIOS EN EL ESQUEMA (I)

- "International Standard" desaparece y se sustituye por "Este documento" (This document)
- En Inglés, se reestructuran frases para una mejor traducción.
- Modificaciones menores de numeración para armonizarla con el anexo SL
- Se requiere documentar las interacciones con los procesos del SGSI
- Se debe comunicar, de forma explícita, en la empresa, los roles relacionados con la Seguridad de la Información.

CAMBIOS EN EL ESQUEMA (II)

- Ya no existen los objetivos de control en la 27002.
- Se deben monitorizar de forma continuada los objetivos de seguridad.
- Introduce gestión de cambios obligatoria.
- En la cláusula 7.4, comunicación interna, se debe documentar el COMO se comunican (2013 no lo pedía, si en otras normas como la ISO9001:2015)

ARMONIZACIÓN ANEXO SL

Para uniformizar o armonizar, todos los esquemas o normas han de tener el mismo orden.

2013	2022
9 Evaluación del desempeño	9 Performance evaluation
10 Mejora	10 Improvement
10.1 No conformidad y acciones correctivas	10.1 Continual improvement
10.2 Mejora continua	10.2 Nonconformity and corrective action

CLÁUSULA 4.4

“La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de este documento”

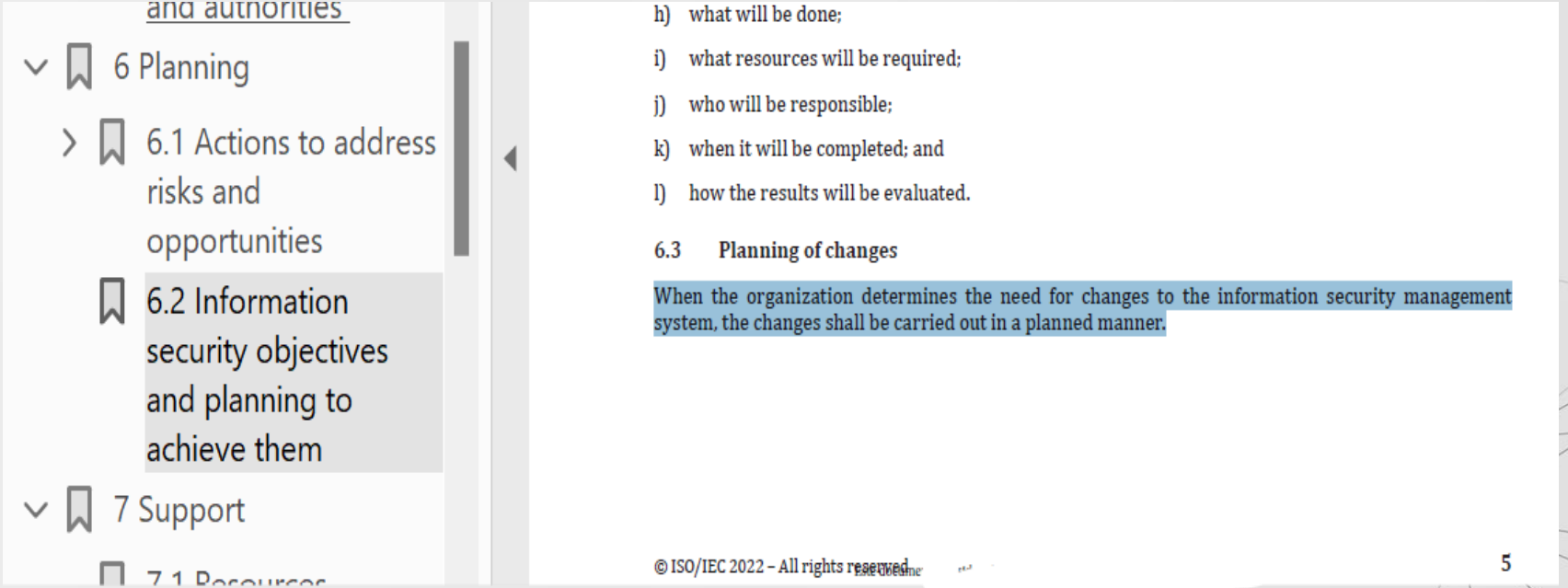
Esto incluye, no solamente los procesos que gestionen la confidencialidad, integridad y disponibilidad de la información, si no TODOS los procesos necesarios para la gestión del SGSI.

Se deberá analizar TODA la interdependencia de procesos internos y externos

- ¿Inventario de procesos?
- ¿Auditoría Interna?
- Gestión por Dirección.

CLÁUSULA 6.3

Primero, ni aparece en el índice



CLÁUSULA 6.3

“Cuando la organización determina la necesidad de cambios en el sistema de gestión de la seguridad de la información, los cambios deben llevarse a cabo de manera planificada.”

- ¿Cómo demostrar esa planificación?

- Recomendación: Usar algo que ya se hace, un ejemplo: ISO9001:2015 – Cláusula 6.3 Planificación de los cambios.

PECULIARIDADES

Cláusula 6.2 Objetivos de seguridad de la información y cómo lograrlos

¿Los objetivos de seguridad deben ser SMART?

SMART de Specific, Measurable, Achievable, Realistic, Time-bound

PECULIARIDADES

Pues no…

6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy;

b) be measurable (if practicable);

¿Y LOS CONTROLES NUEVOS?

APARTADOS ANEXO A

5-ORGANIZATIVO

37 controles

34 preexistentes

3 controles nuevos

6-PERSONAS

8 controles

TODOS preexistentes.

7-FÍSICOS

14 controles

13-preexistentes

1 control nuevo

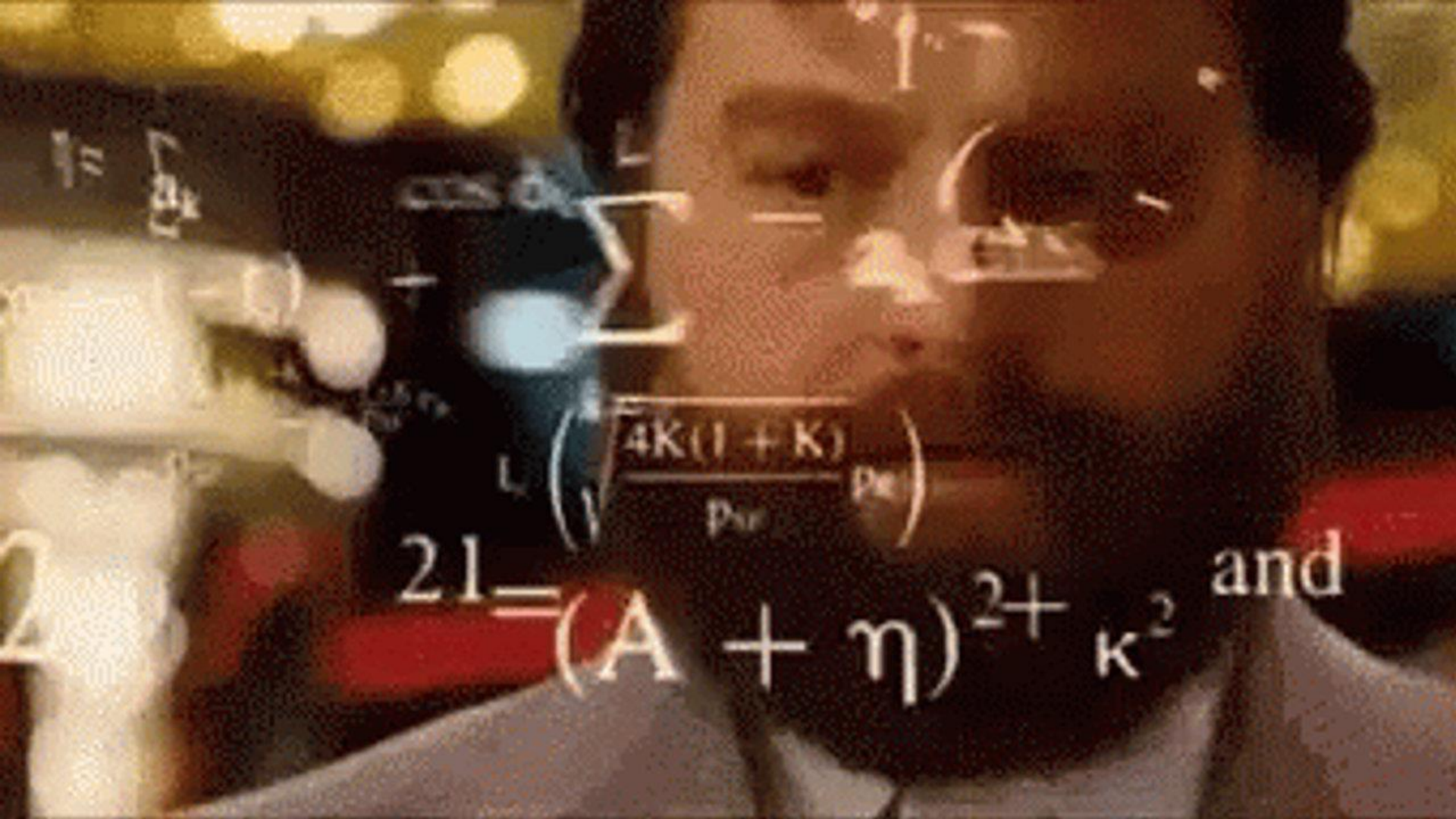
8-TECNOLÓGICOS

34 controles

27 preexistentes

7 controles nuevos

Pasamos de 114 controles (ISO27001:2013) a 93 (ISO27001:2022).
De los 93 actuales, hay 11 controles nuevos y no se elimina ninguno.


$\sum$
$\left(\frac{4K(1+K)}{Pr}\right)$
$21 = (A+\eta)^2 + \kappa^2$ and

CONTROLES ANEXO A

Hay controles actuales que integran varios de la versión anterior.

Se puede ver el mapeo en la ISO 27002:2022

ISO/ IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name
5.1	05.1.1, 05.1.2	Policies for information security
5.2	06.1.1	Information security roles and responsibilities
5.3	06.1.2	Segregation of duties
5.4	07.2.1	Management responsibilities
5.5	06.1.3	Contact with authorities
5.6	06.1.4	Contact with special interest groups
5.7	New	Threat intelligence
5.8	06.1.5, 14.1.1	Information security in project management
5.9	08.1.1, 08.1.2	Inventory of information and other associated assets
5.10	08.1.3, 08.2.3	Acceptable use of information and other associated assets
5.11	08.1.4	Return of assets
5.12	08.2.1	Classification of information
5.13	08.2.2	Labelling of information
5.14	13.2.1, 13.2.2, 13.2.3	Information transfer
5.15	09.1.1, 09.1.2	Access control
5.16	09.2.1	Identity management
5.17	09.2.4, 09.3.1, 09.4.3	Authentication information

CONTROLES ANEXO A

ISO/ IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name
8.8	12.6.1, 18.2.3	Management of technical vulnerabilities
8.9	New	Configuration management
8.10	New	Information deletion
8.11	New	Data masking
8.12	New	Data leakage prevention
8.13	12.3.1	Information backup
8.14	17.2.1	Redundancy of information processing facilities
8.15	12.4.1, 12.4.2, 12.4.3	Logging

Aquí se ven algunos controles nuevos. Hay que tenerlo en cuenta para el SOA.

ATRIBUTOS

Los controles del Anexo A disponen de atributos, voluntarios, para organizarlos.

Atributos de control	Valores del atributo
Control type	#Preventive, #Detective, #Corrective
Information security property	#Confidentiality, #Integrity, #Availability
Cybersecurity concepts	#Identify, #Protect, #Detect, #Respond, #Recover
Operational capabilities	#Governance, #Asset_management, #information_protection, #Human_resources_security, #Physical_security, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Threat_and_vulnerability_management, #Continuity #Supplier_relationship_security, #Legal_and_compliance, #Information_security_event_management, #Information_security_assurance
Security domains	#Governance_and_Ecosystem, #Protection, #Defence, #Resilience

ATRIBUTOS

Como se ven estos atributos.
ISO27002:2022

5.7 Threat intelligence

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_vulner- ability_management	#Defence #Resilience

Control

Information relating to information security threats should be collected and analysed to produce threat intelligence.

NUEVOS CONTROLES

Listado de controles nuevos:

A.5.7 – Threat intelligence
A.5.23 – Information Security for use of cloud services
A.5.30 – Information and Communications Technology readiness for business continuity
A.7.4 – Physical Security monitoring
A.8.9 – Configuration Management
A.8.10 – Information deletion
A.8.11 – Data masking
A.8.12 – Data leakage prevention
A.8.16 – Monitoring activities
A.8.23 – Web filtering
A.8.28 – Secure coding

A.5.7 – Threat Intelligence

Se deben considerar amenazas relevantes, que puedan afectar a la organización.
Tanto internas como externas a la organización.
Se deben considerar a nivel estratégico, táctico y operativo.

Se debe recoger información, analizarla y tomar decisiones (comunicar a las partes implicadas) (Y guardar evidencias)

Se pueden compartir la inteligencia de amenazas entre organizaciones para mejorarla a nivel global

Los controles 5.25, 8.7, 8.16 y 8.23 dependen de la calidad de esta inteligencia.

A.5.23 – IS for use in cloud services

Política clara y aceptada de la responsabilidad compartida del uso de servicios de Cloud.

Razón de la elección de este proveedor y no otro.
Roles y responsabilidades de gestión con el proveedor Cloud.
El uso de la seguridad de la información que ofrece el proveedor.
Gestión de los incidentes de seguridad de la información.
La monitorización de los servicios.
Política de salida y cambio de proveedor.
….

Más de 10 consideraciones en el acuerdo entre la organización y el proveedor Cloud.

A.5.30 – ICT readiness for business continuity

Se debe disponer de un BIA donde estén marcados y definidos el RPO y el RTO y hacer las pruebas adecuadas de los planes definidos e identificados en el análisis de riesgos.

Recomiendo indicar, también, el MTPD.

Se considera nuevo, pero es el A.17.1 de la versión 2013 más alienado con la ISO22301 o con la ISO 27031.

A.7.4 – Physical security monitoring

Monitorización (proporcional y acorde a la legislación vigente) de los accesos a las instalaciones físicas.

CCTV, tornos de acceso, detectores de presión, de apertura de puertas, sensores de rotura de cristales, …

Los sistemas usados se recomiendan sean confidenciales, para no ayudar a buscar puntos ciegos.

Vigilar mucho la proporcionalidad del tratamiento de Datos personales y las notificaciones a los trabajadores.

A.8.9 – Configuration management

Se recomienda el uso de una CMDB.

Identificar como deben estar configurados los equipos de la organización para asegurar un buen funcionamiento.

Definir equipos y como deberían estar configurados (versión SO, parches, segmento de red y máscara, accesos, …)

A.8.10 – Information deletion

Control de la fase final del ciclo de vida de la información y prevención de exposición innecesaria de información interna.

Determinar métodos de borrado

Evidencias del borrado

Considerar el borrado seguro por parte de terceras partes (proveedores, Cloud, …). Asegurar contratos.

A.8.11 – Data masking

Técnicas de enmascaramiento de datos recogidas en la ISO 20889.
(Data scrambling, Data Encryption, Nulling out, Value variance, Data substituion, Data shuffling, Pseudonymisation, Obfuscation, …)

Se deben identificar los datos que deben ser enmascarados (datos personales, datos de prueba, …) y determinar qué procedimiento es el adecuado.

Vigilar con las obligaciones legales o contractuales

A.8.12 – Data leakage prevention

Se deben identificar los datos que deben ser especialmente protegidos (datos personales, datos estratégicos…)

No hace falta aplicarla a toda empresa, “solamente” a los equipos o redes que gestionen, almacenen o transmitan datos sensibles.

Vigilar con las fuentes públicas de información (OSINT)

A.8.16 – Monitoring activities

Monitorizar la red para detectar funcionamientos anómalos y que pueda reaccionar de la forma más automática posible.

Sistema de monitorización que se actualice con las últimas amenazas.

Relacionado con la 5.7 Inteligencia e las amenazas

A.8.23 – Web filtering

Control y protección de la navegación web de los trabajadores.

Tener identificadas las webs a las que pueden navegar (lista blanca), o a las que no (lista negra).

Puede haber diferentes permisos según necesidades de trabajo.

La herramienta debe estar acompañada de una formación adecuada sobre la navegación segura.

A.8.16 – Secure coding

Monitorización y control de librerías de terceras partes.

Establecer y aceptar un nivel mínimo de seguridad en el código desarrollado

Considerar la reutilización de código, así como su aceptación.

Actualizar la formación y las herramientas de análisis a las últimas vulnerabilidades / ataques.

Análisis continuo

GRACIAS

¿Preguntas?

info@xaviervila.net
XavierVila.net
ArMathor.io