Nueva versión de ISO/IEC 27001.2022 ¿Qué beneficios trae a tu empresa?

Montserrat Aguilar

Temario

- Principales cambios de la nueva versión ISO 27001:2022
- ISO 27002 cómo guía en la interpretación de los controles de ISO 27001
- Criterios de transición para empresas certificadas.
- Sistemas de Gestión de Seguridad de la Información en la actualidad.

Principales cambios de la nueva versión ISO/IEC27001:2022

1. ISO/IEC 27001 y 27002 son los estándares "insignia" de la serie 270XX (aplicados por miles de organizaciones en todo el mundo)

2. ISO/IEC 27002:2022 se publicó el 15 de febrero. Esta es la tercera edición, reemplazando la edición de 2013.

   a) El título de la norma se cambia de "Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información" a "Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información", que también indica un enfoque de seguridad "más amplio".

   b) Objetivo de la revisión para 27002:

      1) Modernizar: actualizar el conjunto de controles de seguridad de la información (incluida la orientación) para reflejar los desarrollos y las prácticas actuales de seguridad de la información en varios sectores de empresas y gobiernos. Los desarrollos incluyen cambios en amenazas y vulnerabilidades (escenarios de seguridad) y cambios en Tecnologías (por ejemplo, servicios en la nube, IA y ML)

      2) Simplificación y usabilidad mejorada:

      - Número reducido de controles (21 menos que en la edición de 2013)

      - Estructura de los controles menos compleja

ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información – Requisitos" se publicó el 25 de octubre de 2022.

Principales cambios de la nueva versión ISO/IEC27001:2022

- Como ISO/IEC 27001 (en el Anexo A) hace referencia a los controles en 27002 como Normativos, esta norma refleja el conjunto revisado de controles de 27002.
- Por lo tanto, los cambios en 27001:2022 están relacionados casi exclusivamente con los controles del Anexo A.
  - Para la Cláusula 4-10 en el estándar, solo hay cambios menores y en su mayoría editoriales, que están relacionados principalmente con las alineaciones con los contenidos de la última edición de las Directivas ISO/IEC Parte 1 (Anexo SL, Apéndice 2), que contienen una estructura armonizada y un texto común. para las normas ISO MS. Además, hay enmiendas menores en 6.1.3 c) y d) para alinearse con la nueva terminología para los controles
- Por lo tanto, esta presentación se centra principalmente en los cambios en 27002:2022 para los controles, y solo resume brevemente las modificaciones en la cláusula 4-10 (en la diapositiva 6-10).

Cambios en 27001:2022 - Clausulas 4-10

Principales cambios de la nueva versión ISO/IEC27001:2022

- Las notas en la Cláusula 6.1.3 c) se modifican para reflejar la nueva estructura en el Anexo A, se eliminó la referencia a los "objetivos de control"

27001:2013

NOTA 1 El Anexo A contiene una lista completa de objetivos de control y controles. Usuarios de este estándar internacional se dirigen al Anexo A para garantizar que no se pasen por alto los controles necesarios.
NOTA 2 Los objetivos de control están implícitamente incluidos en los controles elegidos. Los objetivos de control y los controles enumerados en el Anexo A no son exhaustivos y es posible que se necesiten controles y objetivos de control adicionales.

27001:2022

Clause 6.1.3
Notas 1 y 2 reemplazadas con:
NOTA 2 El Anexo A contiene una lista de posibles controles de seguridad de la información. Se dirige a los usuarios de este documento al Anexo A para garantizar que no se pasen por alto los controles necesarios de seguridad de la información.
NOTA 3 Los controles de seguridad de la información enumerados en el Anexo A no son exhaustivos y se pueden incluir controles de seguridad de la información adicionales si es necesario.

- 6.1.3 d) se reorganiza como viñetas (para eliminar posibles ambigüedades)

27001:2013

Clause 6.1.3

d) producir una Declaración de Aplicabilidad que contenga los controles necesarios (ver 6.1.3 b) y c)) y justificación de las inclusiones, ya sea que se implementen o no, y la justificación de las exclusiones de controles del Anexo A;

27001:2022

Clause 6.1.3
d) producir una Declaración de Aplicabilidad que contenga:
— los controles necesarios (ver 6.1.3 b) yc));
— justificación de su inclusión; — si se aplican o no los controles necesarios; y
— la justificación para excluir cualquiera de los controles del Anexo A.

DNV

Principales cambios de la nueva versión ISO/IEC 27001:2022

1. Agregado nuevo c) en 4.2

- 4.2 Comprender las necesidades y expectativas de las partes interesadas
  a) partes interesadas que son relevantes para el sistema de gestión de seguridad de la información;
  b) los requisitos pertinentes de estas partes interesadas;
  c) cuál de estos requisitos se abordará a través de la gestión de seguridad de la información sistema

2. Texto indicado insertado en 4.4

- 4.4 Sistema de gestión de seguridad de la información 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.

Principales cambios de la nueva versión ISO/IEC 27001:2022

3. Nota añadida en 5.

- 5 Liderazgo 5.1 Liderazgo y compromiso…
- **NOTA La referencia a “negocios” en este documento puede interpretarse en sentido amplio para referirse a aquellas actividades que son fundamentales para los propósitos de la existencia de la organización.**.

Principales cambios de la nueva versión ISO/IEC 27001:2022

4. Se agregaron d) y g) en 6.2

6.2 Objetivos de seguridad de la información y planificación para lograrlos

La organización debe establecer objetivos de seguridad de la información en las funciones y niveles pertinentes. Los objetivos de seguridad de la información deberán:

a) ser coherente con la política de seguridad de la información;

b) ser medible (si es factible);

c) tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la evaluación y el tratamiento del riesgo;

d) ser monitoreado;

e) ser comunicado;

f) actualizarse según corresponda;

g) estar disponible como información documentada.

Principales cambios de la nueva versión ISO/IEC 27001:2022

5. Añadido nuevo 6.3 “Planificación de cambios”

6.3 Planificación de cambios

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.

6. 7.4 Comunicación:

Se eliminó “e) los procesos mediante los cuales se efectuará la comunicación” de 2013-ed.

7. 8.1 Planificación y control operativo: Texto modificado como se indica

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información y para implementar las acciones determinadas en 6.1. **La organización también debe implementar planes para lograr los objetivos de seguridad de la información determinados en 6.2.**

— establecer criterios para los procesos;

— implementar el control de los procesos de acuerdo con los criterios.

Principales cambios de la nueva versión ISO/IEC 27001:2022

5. Añadido nuevo 6.3 “Planificación de cambios”

6.3 Planificación de cambios

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.

6. 7.4 Comunicación:

Se eliminó “e) los procesos mediante los cuales se efectuará la comunicación” de 2013-ed.

7. 8.1 Planificación y control operativo: Texto modificado como se indica

…
— establecer criterios para los procesos;
— implementar el control de los procesos de acuerdo con los criterios.
…
La organización debe garantizar que los procesos, productos o servicios proporcionados externamente que sean relevantes para el sistema de gestión de la seguridad de la información estén controlados.

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información y para implementar las acciones determinadas en 6.1. **La organización también debe implementar planes para lograr los objetivos de seguridad de la información determinados en 6.2.**

Principales cambios de la nueva versión ISO/IEC 27001:2022

8. 9.2 Auditoría interna: Texto reorganizado y dividido en nuevos subcapítulos 9.2.1 y 9.2.2

9. Cláusula 9.3 Revisión por la dirección: Se agregó la nueva cláusula 9.3.2 c) + texto reorganizado bajo tres nuevos subcapítulos 9.3.1 – 9.3.3

c) cambios en las necesidades y expectativas de las partes interesadas que sean relevantes para el sistema de gestión de seguridad de la información;

10. Cambio de numeración para 10.1 y 10.2

Cambios clave en 27002:2022 en comparación con la edición de 2013

- Cambios en la estructura y número de controles
- Nuevos términos y definiciones

Principales cambios de la nueva versión ISO/IEC27001:2022

- Título modificado ("Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información" a "Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información",)
- Cláusula 2: “Referencias normativas”: **Sin referencia normativa**. (En 2013-ed.: Referencia a ISO/IEC 27000)
- Cláusula 3: “Términos, definiciones y términos abreviados”: Se eliminó ISO/IEC 27000 como referencia normativa como lo era en 2013-ed. Incluye 38 términos y definiciones relevantes para el estándar
- Tenga en cuenta que 22 de estas definiciones se adoptan de otras fuentes (estándares) como 27000, 29100, 27050, 27035-1

Principales cambios de la nueva versión ISO/IEC27001:2022

- Reestructuración de los controles existentes: los controles se reagrupan en 4 "temas", en lugar de las 14 categorías de la versión de 2013:
- “Organizacional” (37 controles, cap. 5)
- “Gente” (8 controles, cap. 6)
- “Físico” (14 controles, cap. 7)
- “Tecnológico” (34 controles, cap. 8)

Hay 93 controles en la nueva versión mientras que había 114 controles en la versión 2013

Principales cambios de la nueva versión ISO/IEC27001:2022

- Cambios clave en ISO/IEC 27002:2022 en comparación con la edición de 2013 - Cambios en la estructura de cada Control

2nd Ed (2013)

5 Information security policies
5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 Policies for information security

Control

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

Implementation guidance

At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives.

Information security policies should address requirements created by:

... ...

Other information

Some organizations use other terms for these policy documents, such as "Standards", "Directives" or "Rules".

3rd Ed (2022)

5 Organizational controls

5.1 Policies for information security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

Control

Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Purpose

To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business requirements, legal, statutory, regulatory and contractual requirements.

Guidance

At the highest level, organizations should define an "information security policy" which is approved by top management and which sets out the organization's approach to managing its information security.

The information security policy should take into consideration requirements derived from:

... ...

Other information

Topic-specific policies can vary across organizations.

Principales cambios de la nueva versión ISO/IEC27001:2022

- Cambios clave en ISO/IEC 27002:2022 en comparación con la edición de 2013 - Cambios en la estructura de cada Control
- Se agregó "Propósito" para cada control.
- Reemplaza el Objetivo por un grupo de controles en 2013-ed.
- La "tabla de atributos" es nueva con 5 atributos, cada uno con los valores de atributos correspondientes
- Se agregó para crear una vista diferente de la categorización de los controles en comparación con los 4 "temas" para respaldar las diferencias en el contexto empresarial, etc.

Principales cambios de la nueva versión ISO/IEC27001:2022

- Cambios clave en ISO/IEC 27002:2022 en comparación con la edición de 2013 - Cambios en la estructura de cada Control
- Se agregó "Propósito" para cada control.
- Reemplaza el Objetivo por un grupo de controles en 2013-ed.
- La "tabla de atributos" es nueva con 5 atributos, cada uno con los valores de atributos correspondientes
- Se agregó para crear una vista diferente de la categorización de los controles en comparación con los 4 "temas" para respaldar las diferencias en el contexto empresarial, etc.

Principales cambios de la nueva versión ISO/IEC27001:2022

- El número de controles ha disminuido de 114 controles en 14 cláusulas en la edición de 2013 a 93 controles categorizados en 4 "temas" de control que son:
  - "Controles organizacionales",
  - "Controles de personas",
  - "Controles físicos" y
  - "Controles tecnológicos".

- Dentro de los 93 controles (y en comparación con la edición de 2013), 11 controles son nuevos, 24 se fusionan y 58 se actualizan.
- Para todos los controles fusionados y controles actualizados, la intención de los controles sigue siendo la misma. Sin embargo, **todos los controles han sido revisados/actualizados con orientación actualizada** (algunos con cambios sustanciales y otros solo con cambios editoriales/menores)

Principales cambios de la nueva versión ISO/IEC27001:2022

2nd Ed – 114 controls (14 clauses)
5 Information security policies (1/2)
6 Organization of information security (2/7)
7 Human resource security (3/6)
8 Asset management (3/10)
9 Access control (4/14)
10 Cryptography (1/2)
11 Physical and environmental security (2/15)
12 Operations security (7/14)
13 Communications security (2/7)
14 System acquisition, development and maintenance (3/13)
15 Supplier relationships (2/5)
16 Information security incident management (1/7)
17 Information security aspects of business continuity management (2/4)
18 Compliance (2/8)

11 new controls
24 merged controls
58 updated controls

3rd Ed - 93 controls (4 clauses)
5. Organizational controls (37)
6. People controls (8)
7. Physical controls(14)
8. Technological controls (34)

11 New controls included

- Threat intelligence
- Information security for use of cloud services
- ICT readiness for business continuity
- Physical security monitoring
- Configuration management
- Information deletion
- Data masking
- Data leakage prevention
- Monitoring activities
- Web filtering
- Secure coding

Control identifier in 2013-ed.	Control identifier in 2022-ed.	Control name according to 2022-ed
5.1.1, 5.1.2	5.1	Policies for information security
6.1.5, 14.1.1	5.8	Information security in project management
8.1.1, 8.1.2	5.9	Inventory of information and other associated assets
8.1.3, 8.2.3	5.10	Acceptable use of information and other associated assets
13.2.1, 13.2.2, 13.2.3	5.14	Information transfer
9.1.1, 09.1.2	5.15	Access control
9.2.4, 9.3.1, 9.4.3	5.17	Authentication information
9.2.2, 9.2.5, 9.2.6	5.18	Access rights
15.2.1, 15.2.2	5.22	Monitoring, review and change management of supplier services
17.1.1, 17.1.2, 17.1.3	5.29	Information security during disruption
18.1.1, 18.1.5	5.31	Legal, statutory, regulatory and contractual requirements
18.2.2, 18.2.3	5.36	Conformance with policies, rules and standards for information security
16.1.2, 16.1.3	6.8	Information security event reporting
11.1.2, 11.1.6	7.2	Physical entry
8.3.1, 8.3.2, 8.3.3, 11.2.5	7.10	Storage media
6.2.1, 11.2.8	8.1	User endpoint devices
12.6.1, 18.2.3	8.8	Management of technical vulnerabilities
12.4.1, 12.4.2, 12.4.3	8.15	Logging
12.5.1, 12.6.2	8.19	Installation of software on operational systems
10.1.1, 10.1.2	8.24	Use of cryptography
14.1.2, 14.1.3	8.26	Application security requirements
14.2.8, 14.2.9	8.29	Security testing in development and acceptance
12.1.4, 14.2.6	8.31	Separation of development, test and production environments
12.1.2, 14.2.2, 14.2.3, 14.2.4	8.32	Change management

Ejemplo:
un control en la edición de 2013 se ha dividido en dos Controles en la edición de 2022: 18.2.3 "Revisión de cumplimiento técnico" dividido en 5.36 "Cumplimiento de políticas, reglas y estándares para la seguridad de la información" y 8.8 “Gestión de vulnerabilidades técnicas”

Principales cambios de la nueva versión ISO/IEC27001:2022

5.25 Assessment and decision on information security events

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_securi-ty_event_management	#Defence

Control

The organization should assess information security events and decide if they are to be categorized as information security incidents.

Purpose

To ensure effective categorization and prioritization of information security events.

Guidance

A categorization and prioritization scheme of information security incidents should be agreed for the identification of the consequences and priority of an incident. The scheme should include the criteria to categorize events as information security incidents. The point of contact should assess each information security event using the agreed scheme.

Personnel responsible for coordinating and responding to information security incidents should perform the assessment and make a decision on information security events.

Results of the assessment and decision should be recorded in detail for the purpose of future reference and verification.

Other information

The ISO/IEC 27035 series provides further guidance on incident management.

Principales cambios de la nueva versión ISO/IEC27001:2022

Control identifier in 2013-ed.	Control identifier in 2022-ed.	Control name according to 2022-ed
6.1.1	5.2	Information security roles and responsibilities
6.1.2	5.3	Segregation of duties
7.2.1	5.4	Management responsibilities
6.1.3	5.5	Contact with authorities
6.1.4	5.6	Contact with special interest groups
8.1.4	5.11	Return of assets
8.2.1	5.12	Classification of information
8.2.2	5.13	Labelling of information
9.2.1	5.16	Identity management
15.1.1	5.19	Information security in supplier relationships
15.1.2	5.20	Addressing information security within supplier agreements
15.1.3	5.21	Managing information security in the ICT supply chain
16.1.1	5.24	Information security incident management planning and preparation
16.1.4	5.25	Assessment and decision on information security events
16.1.5	5.26	Response to information security incidents
16.1.6	5.27	Learning from information security incidents
16.1.7	5.28	Collection of evidence
18.1.2	5.32	Intellectual property rights
18.1.3	5.33	Protection of records
18.1.4	5.34	Privacy and protection of PII
18.2.1	5.35	Independent review of information security

Control identifier in 2013-ed.	Control identifier in 2022-ed.	Control name according to 2022-ed
12.1.1	5.37	Documented operating procedures
7.1.1	6.1	Screening
7.1.2	6.2	Terms and conditions of employment
7.2.2	6.3	Information security awareness, education and training
7.2.3	6.4	Disciplinary process
7.3.1	6.5	Responsibilities after termination or change of employment
13.2.4	6.6	Confidentiality or non-disclosure agreements
6.2.2	6.7	Remote working
11.1.1	7.1	Physical security perimeters
11.1.3	7.3	Securing offices, rooms and facilities
11.1.4	7.5	Protecting against physical and environmental threats
11.1.5	7.6	Working in secure areas
11.2.9	7.7	Clear desk and clear screen
11.2.1	7.8	Equipment siting and protection
11.2.6	7.9	Security of assets off-premises
11.2.2	7.11	Supporting utilities
11.2.3	7.12	Cabling security
11.2.4	7.13	Equipment maintenance
11.2.7	7.14	Secure disposal or re-use of equipment
9.2.3	8.2	Privileged access rights
9.4.1	8.3	Information access restriction
9.4.5	8.4	Access to source code

Control identifier in 2013-ed.	Control identifier in 2022-ed.	Control name according to 2022-ed
9.4.2	8.5	Secure authentication
12.1.3	8.6	Capacity management
12.2.1	8.7	Protection against malware
12.3.1	8.13	Information backup
17.2.1	8.14	Redundancy of information processing facilities
12.4.4	8.17	Clock synchronization
9.4.4	8.18	Use of privileged utility programs
13.1.1	8.20	Networks security
13.1.2	8.21	Security of network services
13.1.3	8.22	Segregation of networks
14.2.1	8.25	Secure development life cycle
14.2.5	8.27	Secure system architecture and engineering principles
14.2.7	8.30	Outsourced development
14.3.1	8.33	Test information
12.7.1	8.34	Protection of information systems during audit testing

Principales cambios de la nueva versión ISO/IEC27001:2022

Descripción general de los nuevos controles

Título del control	Control	Propósito
Inteligencia de amenazas (5.7)	La información relacionada con las amenazas a la seguridad de la información debe recopilarse y analizarse para generar información sobre amenazas.	Proporcionar conciencia sobre el entorno de amenazas para que se puedan tomar las medidas apropiadas.
Seguridad de la información para uso de servicios en la nube (5.23)	El proceso de adquisición, uso, gestión y salida del servicio en la nube debe establecerse de acuerdo con los requisitos de seguridad de la información de la organización.	Especificar y administrar la seguridad de la información para el uso de servicios en la nube
Preparación de las TIC para la continuidad del negocio (5.30)	La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.	Para garantizar la disponibilidad de la información de la organización y otros activos asociados durante la interrupción
Vigilancia de la seguridad física (7.4)	Las instalaciones deben monitorearse continuamente para detectar accesos físicos no autorizados.	Para detectar y disuadir el acceso físico no autorizado.

Principales cambios de la nueva versión ISO/IEC27001:2022

Descripción general de los nuevos controles

Título del control	Control	Propósito
Gestión de la configuración (8.9)	La configuración, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes debe establecerse, documentarse, implementarse, monitorearse y revisarse.	Para garantizar que el hardware, el software, los servicios y las redes funcionen correctamente con la configuración de seguridad requerida, y que la configuración no se altere por cambios no autorizados o incorrectos.
Eliminación de información (8.10)	La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento debe ser eliminada cuando ya no sea necesaria.	Para evitar la exposición innecesaria de información confidencial y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales para la eliminación de información.
Enmascaramiento de datos (8.11)	El enmascaramiento de datos debe usarse de acuerdo con la política específica del tema de la organización sobre el control de acceso y los requisitos comerciales, teniendo en cuenta los requisitos de la legislación aplicable.	Limitar la exposición de datos confidenciales, incluida la PII, y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales.

Principales cambios de la nueva versión ISO/IEC27001:2022

Descripción general de los nuevos controles

Título del control	Control	Propósito
Prevención de fuga de datos (8.12)	Las medidas de prevención de fuga de datos deben aplicarse a los sistemas, redes y dispositivos finales que procesan, almacenan o transmiten información confidencial.	Para detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.
Actividades de seguimiento (8.16)	Las redes, los sistemas y las aplicaciones deben monitorearse para detectar comportamientos anómalos y deben tomarse las medidas apropiadas para evaluar posibles incidentes de seguridad de la información.	Para detectar comportamientos anómalos y posibles incidentes de seguridad de la información.
Filtrado web (8.23)	El acceso a sitios web externos debe administrarse para reducir la exposición a contenido malicioso	Para proteger los sistemas contra el malware y evitar el acceso a recursos web no autorizados.
Codificación segura (8.28)	Los principios de codificación segura deben aplicarse al desarrollo de software.	Garantizar que el software se escriba de forma segura, reduciendo así la cantidad de posibles vulnerabilidades de seguridad de la información en el software.

Arreglos de transición para ISO/IEC 27001:2022

Principales cambios de la nueva versión ISO/IEC27001:2022

Lo siguiente se basa en el Documento Obligatorio 26:2023 de **IAF** (Número 2) "Requisitos de transición para ISO/IEC 27001:2022"

- 36 meses a partir de la última fecha del mes de publicación de ISO/IEC 27001:2022, todos los certificados existentes se trasladarán al nuevo estándar. Después de esta fecha, los certificados de la edición de 2013 dejan de ser válidos (**la fecha límite es el 31 de octubre de 2025).**

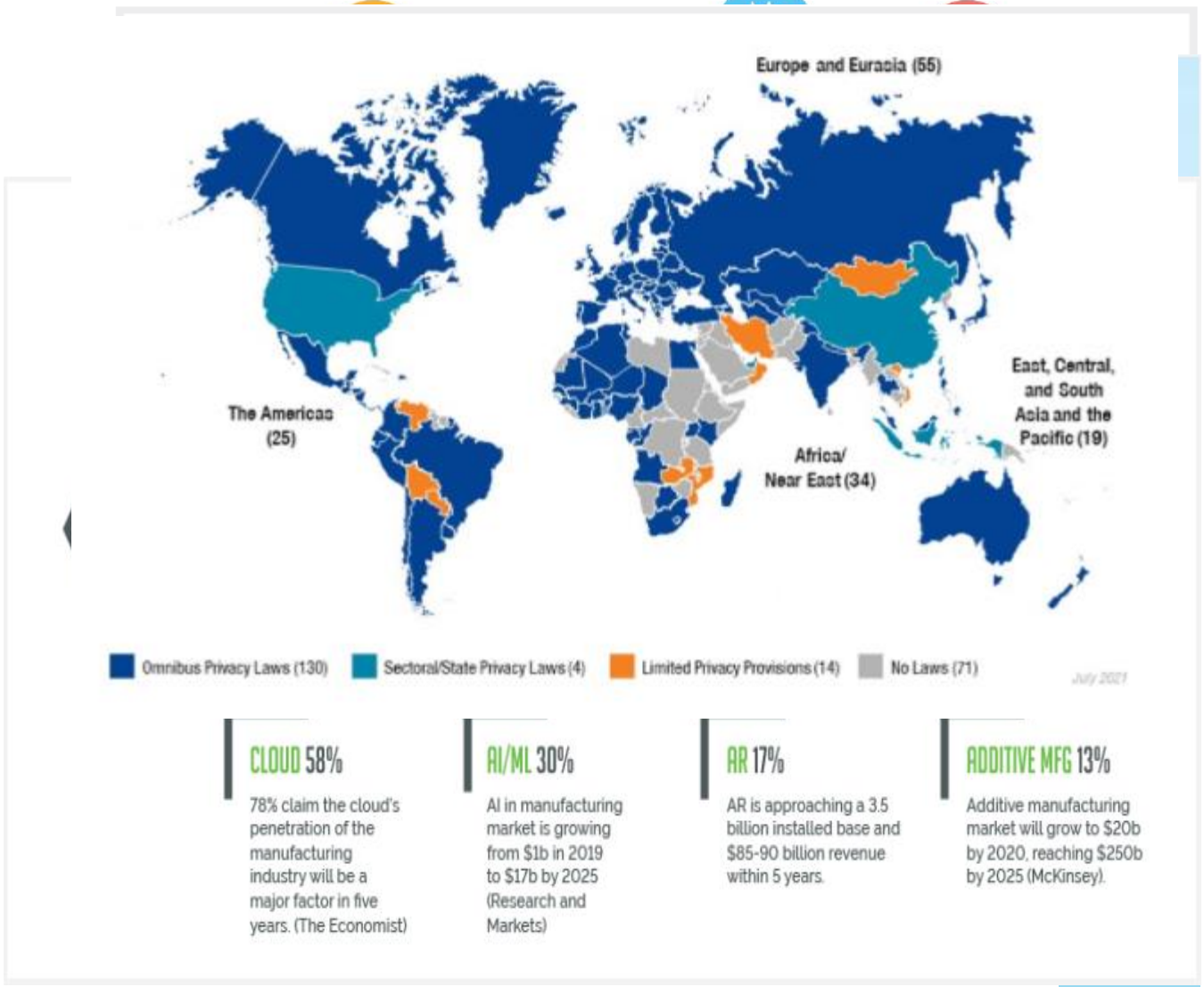
- A partir de los 18 meses posteriores a la última fecha del mes de publicación de ISO/IEC 27001:2022 (**a partir del 31 de octubre de 2023**), DNV realizarán auditorías iniciales y recertificaciones de ISO/IEC 27001:2022 (**lo que significa a partir del 30 de abril de 2024**)

- La auditoría de transición se puede realizar en relación con una auditoría periódica programada o en una auditoría especial en el período de transición. Se requerirá algo de tiempo adicional para la auditoría de transición. Mín. 0,5 días si la transición se realiza junto con una recertificación programada mín. 1 día si la transición se realiza junto con una auditoría periódica programada

Sistemas de Gestión de Seguridad de la Información en la actualidad.

Contexto – Realidades del riesgo

- **Panorama de amenazas en constante evolución**
- **Más trabajo en casa**
- **Mayor uso de servicios en la nube**
- **Tecnologías digitales de rápido crecimiento**
- **Introducción de leyes de privacidad a nivel mundial**



Gracias!

Montserrat Aguilar

www.dnv.com