BOLETÍN INFORMATIVO N° 01

Nuevos Cambios en el ISO 27002:2021

EFICIENCIA GERENCIAL
Y PRODUCTIVIDAD S.A.C.

Índice

1. Introducción

El 26 de noviembre del 2020 fue publicado el Draft International Standard (DIS) de la norma ISO 27002, definida como ISO/IEC DIS 27002, la cual viene a actualizar el estándar ISO 27002:2013.

Con este borrador comienzan las etapas de revisión final establecidas en el ciclo de revisión de los estándares ISO, lo cual permite estimar que la publicación final del estándar será realizada en el tercer trimestre del 2021.

En la etapa actual del estándar, etapa de consulta (etapa 40), considera la duración de 12 semanas, cuyo comienzo está establecido del 28 de enero del 2021, finalizando el 22 de abril del 2021.

Si el borrador es aprobado, se transforma en borrador final (FDIS) debiendo este borrador final pasar a una etapa de consulta (etapa 50), la cual tiene una duración de 8 semanas, en caso de aprobarse pasaría a la etapa de revisión (etapa 60), que dura 20 semanas, transformándose de esta forma en el estándar final.

Considerando los tiempos, es muy probable que entre Noviembre y Diciembre del 2021 ya esté publicada la nueva ISO/IEC 27002:2021.

2. Situación Actual de la Norma

El borrador de la norma se encuentra disponible en "iso.org". El proceso de oficialización de una nueva norma pasa por un ciclo que se denomina "Ciclo de Vida de un Estándar". En la Figura N° 1 se presentan las etapas del ciclo.

Figura N° 1

3. Principales Cambios

La nueva versión trae consigo importantes cambios, siendo los más significativos:

- El cambio de nombre.
- Incorporación de nuevos términos y definiciones.
- La nueva estructura de temas de seguridad de la información.
- La nueva estructura de atributos de los controles.
- Cambios en controles desde la versión ISO 27002:2013.

4. El Cambio de Nombre

El nombre de la norma cambia, de llamarse “Código de Práctica para Controles de Seguridad de la Información”, simplemente se denominará “Controles de Seguridad de la Información”. En la figura N° 2 se presenta el detalle del cambio.

Figura N° 2

Nombre 2013	Tecnología de Información – Técnicas de Seguridad – Código de Práctica para Controles en Seguridad de Información.
Nombre 2021	Seguridad de Información, Ciberseguridad y Protección Privada – Controles para Seguridad de Información.

5. Nuevos Términos y Definiciones

Al igual que otras normas ISO, en la sección 3 “Términos y Definiciones”, establecen los términos y definiciones.

En total define 37 términos, entre los cuales se incluyen algunos generales y ya definidos en ISO 27000 “Glosario de Términos”, tales como: control de acceso, ataque, autenticación, autenticidad, entidad, instalación de procesamiento de información, evento de seguridad de la información, incidente de seguridad de la información, gestión de incidentes de seguridad de la información, sistema de información, parte interesada, no repudio, política, procedimiento, proceso, registro, fiabilidad, amenaza y vulnerabilidad.

Los nuevos términos son:

Cadena de custodia, Información confidencial, disrupción, endpoint, brecha de seguridad de la información, personal, información de identificación personal, valuación del impacto de la privacidad, punto objetivo de recuperación (RPO) tiempo objetivo de recuperación (RTO) regla, información sensitiva, política específica y usuario.

En total incorpora 16 nuevos términos, buscando establecer un alcance más amplio en elementos propios de la ciberseguridad, la gestión de evidencia electrónica, la gestión de PII y privacidad, la gestión de incidentes y la gestión de la continuidad del negocio.

6. Nueva Estructura de Temas y Controles

Un cambio radical con respecto a la versión anterior es la restructuración de los 14 dominios de controles definidos en ISO 27002:2013 en torno a 4 grandes temas:

- Controles Organizacionales (37 controles).
- Controles de Personas (8 controles).
- Controles Físicos (14 controles).
- Controles Tecnológicos (34 controles).

Esta clasificación de funciones es mucho más simple que la provista por la versión 2013 de la norma, la cual se encuentra mucho más orientada al contexto de aplicación del control (organizacional, personas, físicos y tecnológicos).

En la versión 2013, en cada dominio se establecía una serie de objetivos de control (34) y luego los controles de seguridad de la información (114).

En esta nueva versión, no existe la definición de objetivos de control (se elimina), definiendo en total la nueva norma 93 controles.

Sin embargo, la norma incluye un atributo que permite la clasificación específica del control, en la cual cada control es clasificado en uno o más de las 15 categorías establecidas.

El cambio es acertado, el establecimiento de controles de acuerdo con su contexto de aplicación deja mucho más en evidencia las responsabilidades del personal de la empresa, para la gestión de la seguridad de la información, ciberseguridad y protección de la privacidad, las cuales se establecen en torno a los 37 controles organizacionales.

La eliminación de los objetivos de control es un aspecto positivo, dado que estos se encuentran intrínsecamente definidos en el control mismo, siendo escasamente utilizados en la versión 2013, aportando en la práctica muy poco valor.

7. La Nueva Estructura de Atributos de los Controles

Uno de los aspectos relevantes que proporciona la norma para cada control son cinco atributos, los cuales establecen subclasificaciones del atributo que permiten caracterizar al control, a modo de ejemplo se presentan los primeros tres controles del tema de controles organizacionales definidos en la nueva versión de la norma. En la Figura N 3 se tiene una ilustración.

Figura N° 3: Subclasificaciones de los Controles

ISO/IEC 27002 Identificador de Control	Nombre Control	Tipo de Control	Propiedades Seguridad de Información	Conceptos Ciberseguridad	Capacidad Operacionales	Dominios de Seguridad
5.1	Políticas de Seguridad de Información	Preventivo	Confidencialidad Integridad Disponibilidad	Identificación	Gobernanza	Gobernanza Ecosistema Resiliencia
5.2	Roles y Responsabilidad en Seguridad de Información	Preventivo	Confidencialidad Integridad Disponibilidad	Identificación	Gobernanza	Gobernanza Ecosistema Protección Resiliencia
5.3	Segregación de Tareas	Preventivo	Confidencialidad Integridad Disponibilidad	Protección	Gobernanza	Gobernanza Ecosistema

8. Definición de los Controles

- **Tipo de Control. -**

  Este atributo posibilita identificar cuando o como el control impacta en la gestión de riesgos con respecto a la ocurrencia de un incidente de seguridad de la información. Los posibles valores son:

  - ✓ Preventivo (el control actúa antes de que la amenaza actué),
  - ✓ Detección (el control actúa cuando la amenaza ocurre) y
  - ✓ Correctivo (el control actúa después de que la amenaza ocurre).

- **Propiedades de Seguridad de la Información.-**

  Este atributo proporciona información sobre como el control contribuye en la preservación de los resultados esperados de la seguridad de la información. Los posibles valores son: Confidencialidad, Integridad y Disponibilidad.

- **Conceptos de Ciberseguridad.-**

  Este atributo puede ser empleado cuando la organización busca la implementación de un Sistema de Gestión de Seguridad de la Información o un Marco de Referencia de Ciberseguridad como el del NIST, el cual se alinea con los cinco grandes dominios de ciberseguridad establecidos en el ISO 27101. Los posibles valores que toma el atributo son: Identificar, Proteger, Detectar, Responder y Recuperar.

- **Capacidades Operacionales.-**

  Este atributo puede ser usado cuando la organización requiere una clasificación de controles desde una perspectiva práctica, cuando la organización quiere asignar responsabilidades o establecer lineamientos de implementación. Los posibles valores que puede tomar este atributo son: Gobernanza, Gestión de Activos, Protección de la Información, Seguridad en los Recursos Humanos, Seguridad Física, Seguridad en Sistemas y Redes, Seguridad en Aplicaciones, Seguridad en la Configuración, Gestión de Accesos e Identidades, Gestión de Amenazas y Vulnerabilidades, Continuidad, Seguridad en Relaciones con Proveedores, Legal y Cumplimiento, Gestión de Eventos de Seguridad de la Información, y Aseguramiento de la Seguridad.

- **Dominio de Seguridad.-**

  Este atributo puede ser usado en el caso que la organización quiera clasificar sus controles desde una perspectiva del campo de aplicación de la seguridad de la información y ciberseguridad, su competencia, servicios y productos relacionados. Los posibles valores que toma el atributo son: Gobernanza y ecosistema, Protección, Defensa y Resiliencia.

- **Tipo de Control.-**

  Este atributo aportará mucho a fortalecer el control interno organizacional, para permitir, identificar controles de diversa naturaleza para la gestión de riesgos de alta criticidad incorporando controles preventivos, detección y correctivos).

  La definición de los atributos es un importante aporte en la definición de la nueva norma, el contexto de uso es muy amplio de cada uno de ellos, posibilitando el desarrollo de diversos mecanismos de gestión de los controles que fortalecerán el control interno, el plan de tratamiento de riesgos, la evaluación de controles, la asignación de responsabilidades, y la auditoría.

  A nivel de definición de los controles específicamente, estos no sufren mayores cambios con respecto a la versión 2013, estando definidos de la siguiente forma: Control, Propósito, Directrices y Otra Información (Sólo en caso de ser necesaria).

9. Cambios en Controles en la Versión 2021

Al margen de los cambios de dominio o temas y la definición de los atributos para cada control, el desarrollo de la nueva norma contempla la reducción de controles pasando de los 114 existentes en la versión 2013 a 93 controles en la nueva versión.

10. Nuevos Controles

En total se definen 11 nuevos controles, los cuales corresponden a:

- 5.7 Inteligencia de Amenazas
- 5.23 Seguridad de la información para el uso de servicios en la nube
- 5.30 Preparación de las TIC para la continuidad del negocio
- 7.4 Monitoreo de la seguridad física
- 8.9 Gestión de la configuración
- 8.10 Eliminación de la información
- 8.11 Enmascaramiento de datos
- 8.12 Prevención de la fuga de datos
- 8.16 Monitoreo de actividades
- 8.22 Filtrado Web
- 8.28 Codificación Segura

Controles que se fusionan con otros controles desde la perspectiva del ISO 27002.2013

Diversos controles fueron reordenados y reorganizados en otros controles, generando nuevos controles, provenientes desde el ISO 27002:2013:

- 5.1.1(Políticas para la seguridad de la información) y 5.1.2 (Revisión de las políticas para la seguridad de la información) se fusionan en el control 5.1 de políticas de seguridad de la información
- 6.2.1(Política de dispositivos móviles) y 11.2.8 (Equipo de usuario desatendido) se funcionan en el control 8.1 Dispositivos de punto final del usuario.
- 8.1.1 (Inventario de activos) y 8.1.2 (Propiedad de los activos) se fusionan en el control 5.9 de Inventario de información y otros activos asociados.
- 8.1.3 (Uso aceptable de los activos) y 8.2.3 (Manipulado de la información) se fusionan en el control 5.10 Uso aceptable de la información y activos asociados.
- 8.3.1(Gestión de soportes extraíbles), 8.3.2 (Eliminación de soportes) y 8.3.3 (Soportes físicos en tránsito) se fusionan en el control 7.10 Medios de Almacenamiento.
- 9.1.1(Política de control de acceso) y 9.1.2(Acceso a las redes y a los servicios de red) se fusionan en el control 5.15 Control de Accesos.
- 9.2.4 (Gestión de la información secreta de autenticación de los usuarios), 9.3.1 (Uso de la información secreta de autenticación) y 9.4.3 (Restricción del acceso a la información) se fusionan en el control 5.17 de Autenticación de información.
- 9.2.2 (Provisión de acceso de usuario) y 9.2.5 (Revisión de los derechos de acceso de usuario), 9.2.6(Retirada o reasignación de los derechos de acceso) se fusionan en el control 5.18 de Derechos de Acceso
- 10.1.1(Política de uso de los controles criptográficos) y 10.1.2 (Gestión de claves) se fusionan en el control 8.24 Uso de Criptografía.
- 11.1.2 (Controles físicos de entrada) y 11.1.6 (Áreas de carga y descarga) se fusionan en el control 7.2 Controles de entrada física.

- 12.1.4(Separación de los recursos de desarrollo, prueba y operación) y 14.2.6 (Entorno de desarrollo seguro) se fusionan en el control 8.31 Separación de ambientes de desarrollo, prueba y producción.
- 12.4.1(Registro de eventos), 12.4.2(Protección de la información del registro) y 12.4.3 (Registros de administración y operación) se fusionan en el control 8.15 Inicio de Sesión
- 12.5.1(Instalación del software en explotación) y 12.6.2 (Restricción en la instalación de software) se fusionan en el control 8.19 Instalación de software en sistemas operativos
- 12.6.1(Gestión de las vulnerabilidades técnicas) y 18.2.3 (Comprobación del cumplimiento técnico) se fusionan en el control 8.8 Gestión de vulnerabilidades técnicas.
- 12.1.2 (Gestión de cambios), 14.2.2 (Procedimiento de control de cambios en sistemas), 14.2.3 (Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo) y 14.2.4 (Restricciones a los cambios en los paquetes de software)se fusionan en el control 8.32 Gestión del Cambio
- 13.2.1 (Políticas y procedimientos de intercambio de información), 13.2.2 (Acuerdos de intercambio de información), 13.2.3 (Mensajería electrónica) se fusionan en el control 5.14 Transferencia de información
- 14.1.2 (Asegurar los servicios de aplicaciones en redes públicas) y 14.1.3(Protección de las transacciones de servicios de aplicaciones) se fusionan en el control 8.26 Requerimientos de seguridad en aplicaciones
- 14.2.8 (Pruebas funcionales de seguridad de sistemas) y 14.2.9 (Pruebas de aceptación de sistemas) se fusionan en el control 8.29 de Pruebas de seguridad en el desarrollo y aceptación.
- 15.2.1(Control y revisión de la provisión de servicios del proveedor) y 15.2.2 (Gestión de cambios en la provisión del servicio del proveedor) se fusionan en el control 5.22 Monitoreo, revisión y gestión del cambio con proveedores de servicios.
- 16.1.2 (Notificación de los eventos de seguridad de la información) y 16.1.3(Notificación de puntos débiles de la seguridad) se fusionan en el control 6.8 Reporte de eventos de seguridad de la información.
- 17.1.1 (Planificación de la continuidad de la seguridad de la información), 17.1.2 (Implementar la continuidad de la seguridad de la información) y 17.1.3 (Verificación, revisión y evaluación de la continuidad de la seguridad de la información) se fusionan en el control 5.29 Disrupción durante la seguridad de la información.
- 18.1.1 (Identificación de la legislación aplicable y de los requisitos contractuales) y 18.1.5 (Regulación de los controles criptográficos) se fusionan en el control 5.31 Identificación de requerimientos legales, estatutarios, regulatorios y contractuales.
- 18.2.2 (Cumplimiento de las políticas y normas de seguridad) y 18.2.3 (Comprobación del cumplimiento técnico) se fusionan en el control 5.36 Cumplimiento con políticas y estándares para la seguridad de la información

11. Controles que se Eliminan del ISO 27002.2013

Solo un control fue eliminado desde la versión 2013, el cual corresponde al 11.2.5 Retirada de materiales propiedad de la empresa.

12. Conclusiones

La nuevas estructura de la norma es un importante paso para la simplificación y facilidad de uso de esta, teniendo importantes cambios, no solo en lo estructural, sino que incluso a nivel de lenguaje acercándose a temas más cercanos a la ciberseguridad actual.

La fusión y definición de controles es uno de los aspectos más relevantes, la incorporación de 11 nuevos controles y el reordenamiento de más de 54 controles para definir 23 controles nuevos nos permite contar con una norma con definiciones mucho más actualizadas, más alineada al contexto de ciberseguridad, protección de la privacidad y gestión de incidencias, y con una mayor simplicidad en controles de gestión de activos, control de acceso e identidades, seguridad física, seguridad en las operaciones y seguridad en el software, lo cual hace a la norma mucho más comprensible y aplicable.

Este un breve resumen de los cambios que provee la norma, según la versión DIS.

Cuando aparezca la versión FDIS, será tema central de nuestro próximo Boletín. Muchos de los aspectos presentados en la versión DIS, pudiesen cambiar. De todas maneras, la versión DIS, nos da una clara idea de los cambios en la norma ISO 27002:2021. Las modificaciones son de cierta profundidad.

13. Enlaces de Referencia:

Etapas y recursos para el desarrollo de estándares ISO.

https://www.iso.org/stages-and-resources-for-standards-development.html

ISO/DIS 27002:2021

27.002. https://www.iso.org/standard/75652.html