ISO 27002:2022 NUEVOS CONTROLES E IMPACTO EN LA ORGANIZACIÓN

TLP:WHITE

seresco

Realizado por el Equipo de Seguridad de la información y cumplimiento normativo de Seresco.

ISO 27002:2022
NUEVOS CONTROLES E IMPACTO EN LA ORGANIZACIÓN

Probablemente, en estas últimas semanas, habréis escuchado que hace un par de meses se publicó la norma ISO 27002:2022, que describe los controles que, a finales de este año si se cumple el calendario, sustituirán al anexo A de la norma UNE-EN ISO/IEC 27001:2017. Esta adaptación no generará un cambio de versión de la norma, si no una corrección de errores que modificará la estructura del anexo A.

A diferencia de una actualización de versión de una norma, una corrección de errores implica un plazo de adecuación menor, probablemente no superior a 12 meses, por lo que es muy recomendable que las organizaciones empiecen a aproximarse a este nuevo marco normativo cuanto antes, ya que, como veremos a continuación, algunos de los nuevos controles pueden requerir un esfuerzo importante, tanto a nivel económico como en su implementación.

PRINCIPALES CAMBIOS EN LA ESTRUCTURA ORGANIZATIVA DE LOS CONTROLES

La norma ISO 27002 ha sufrido una reestructuración importante, si **antes contaba con 14 dominios de seguridad, ahora los controles se distribuyen en 4 grupos: 37 organizativos, 8 de personal, 14 físicos y 34 tecnológicos.**

Otro concepto que desaparece son los "objetivos de control" que se establecían para cada agrupación de controles relacionados, dejando paso a un propósito individualizado para cada control.

ATRIBUTOS: EL NUEVO CRITERIO DE CLASIFICACIÓN

Esta distribución en cuatro grupos pierde relevancia a favor del nuevo criterio de estructuración de los controles mediante **atributos.**

Con esto se consigue una mayor flexibilidad en la norma y ofrece múltiples posibilidades de organización, ya que la propia norma indica que los atributos predefinidos son genéricos, y da libertad a las organizaciones para crear sus propios atributos, ajustando así la visión de controles a los resultados que se quieren obtener.

- El primer atributo se denomina **tipo de control** y puede tener tres valores: **preventivo, detectivo y correctivo.** Este atributo indica cómo actuará el control frente a un incidente de seguridad y no se limita necesariamente a un único valor.

- El segundo atributo son las **propiedades de seguridad de la información**: **confidencialidad, integridad y disponibilidad.** Cada control indica qué propiedad o propiedades ayuda a proteger.

- **Conceptos de ciberseguridad** es un atributo que organiza los controles según la estructura de cinco fases que utilizan los estándares de ciberseguridad, como la norma ISO/IEC TS 27110. Estas fases son: **identificar, proteger, detectar, responder y recuperar.** Este atributo es muy útil, ya que facilita la relación entre marcos normativos de seguridad de la información y ciberseguridad.

- **Capacidades operativas,** permite estructurar los controles desde el punto de vista de un profesional de seguridad de la información. Si nos fijamos en la terminología de este atributo, los valores recuerdan un poco a los dominios de seguridad de la versión anterior de la norma, algunos de ellos son: **gobierno, gestión de activos, protección de la información, seguridad de los recursos humanos, seguridad física, seguridad de sistemas y redes, continuidad, etc.**

- Por último, el atributo **dominios de seguridad** categoriza los controles desde la perspectiva de cuatro dominios de seguridad de la información: **gobierno y ecosistema, protección, defensa y resiliencia;** y nuevamente podemos apreciar la similitud de la terminología entre estos dos últimos atributos.

UNA NORMA ORIENTADA HACIA LA PROTECCIÓN

Si analizamos el reparto de los valores de los atributos a los controles, encontramos que **el 75 % son de tipo preventivo**, lo que evidencia que la norma continúa enfocándose en la prevención de incidentes de seguridad.

¿Y QUÉ IMPLICACIONES TIENE?

Este es un aspecto a tener muy en cuenta porque todas las organizaciones son diferentes y tienen visiones diferentes, y todo depende de cuál sea su enfoque. Por ejemplo, si una organización se enfoca en la detección, puede ser recomendable que complemente la implantación de estos controles con otro marco de referencia que profundice más en la detección.

Respecto a las **propiedades de seguridad de la información,** muy pocos controles protegen únicamente una propiedad, ya que el 85 % tienen asignados las tres dimensiones (confidencialidad, integridad y disponibilidad). Nuevamente, considerar si esto es, o no, adecuado, dependerá de la visión de cada organización. Poniendo de nuevo un ejemplo, en caso de que quiera enfocarse más en la disponibilidad, deberá analizar la necesidad de emplear estándares adicionales que traten esta dimensión en concreto.

Por último, los **atributos recuperación y resiliencia** son los que menos controles tienen asignados, por tanto, si esto es lo que nos interesa, debemos analizar la necesidad de contar con otros estándares que se enfoquen más en la recuperación.

NUEVOS CONTROLES

Se plantean once nuevos controles, algunos de los cuales requerirán un profundo análisis sobre cómo se van a abordar, especialmente los que involucran la contratación de herramientas o servicios.

- **Inteligencia de amenazas** (5.7). Deberemos ser capaces de recoger y analizar información sobre amenazas, bien sea de carácter estratégico, táctico u operacional.

- **Seguridad de la información en el uso de servicios en la nube** (5.23). Requiere que desarrollemos procedimientos específicos para la adquisición, uso, gestión y finalización de servicios en la nube; a diferencia de los controles preexistentes sobre servicios prestados por terceros, este control se centra en distinguir cómo abordar los servicios en la nube.

- **Preparación de las TIC para la continuidad de negocio** (5.30). Debemos establecer una forma específica de planificar, implementar, mantener y probar la continuidad TIC. Este control se enfoca en la continuidad TIC, diferenciándola de la continuidad del negocio.

- **Monitorización de la seguridad física** (7.4). Como su nombre indica, será necesario implementar algún mecanismo de control de acceso que detecte si se producen accesos físicos no autorizados.

- **Gestión de la configuración** (8.9). Es un requisito perteneciente a la ISO 20000 y se incorpora de manera equivalente a la ISO 27002. Busca controlar la configuración de los activos para asegurar que funcionan correctamente y que no se producen cambios no autorizados o erróneos en su configuración.
- **Borrado de información** (8.10) y **enmascaramiento de datos** (8.11). Son dos controles muy ligados a la

protección de datos personales, aunque su aplicación es extensible a cualquier tipo de información. El primero alude al cumplimiento del principio de limitación del plazo de conservación de la información (5.1.e RGPD), mientras que el segundo busca utilizar mecanismos que protejan la información y eviten su exposición pública en caso de incidente.

- **Prevención de fuga de datos** (8.12) y **monitorización de actividades** (8.16). Será necesario implementar herramientas que detecten las fugas de información (DLP) y que detecten comportamientos anómalos y potenciales incidentes de seguridad, es decir, sistemas SIEM.

- **Filtrado web** (8.23). Se busca restringir la navegación de los usuarios para reducir el riesgo de acceso a contenidos maliciosos y, por tanto, la exposición a incidentes de seguridad.

- **Control de codificación segura** (8.28). Va un paso más allá del control "política de desarrollo seguro" de la versión anterior de la norma, requiriendo además de una política, que se implementen metodologías de desarrollo seguro.

www.seresco.es