Anexo del monográfico 4

Correspondencia funcional de Kumoss con ISO IEC 42001

Relacionar capacidades observadas del producto con preguntas, requisitos y áreas de control que el SGIA debe valorar según su alcance y tratamiento de riesgos.

Cómo leer la matriz

La matriz es una correspondencia funcional del curso. No demuestra conformidad de Kumoss ni de una implantación de Inditex.

Se citan áreas del Anexo A, no subcontroles cuyo texto no se haya contrastado. Su selección y aplicabilidad se justifican en el SGIA.

La cláusula 6.3 se refiere a planificar cambios del SGIA. Para una operación de infraestructura se examina principalmente el control operacional de 8.1; se añade 6.3 cuando cambie el propio sistema de gestión.

A.8 trata la información a las partes interesadas. A.10 trata relaciones con terceros y clientes. No se usan como etiquetas generales de auditoría de cumplimiento o de control de accesos.

Hash, firma, formato y método de autorización se determinan en el procedimiento aplicable. La matriz no los presenta como funciones nativas acreditadas ni como requisitos universales.

Correcciones que debes retener

Referencia	Lectura que utiliza el curso
6.3	Planificación de cambios del SGIA; no se asigna automáticamente a cada modificación de infraestructura.
A.8	Información a partes interesadas; no es un rótulo general para el auditor de cumplimiento.
A.10	Relaciones con terceros y clientes; el control interno de roles se estudia desde organización y uso.

La columna de evidencia describe qué buscar según el criterio aplicable. No afirma que esas evidencias existan en una instalación concreta.

Matriz integrada mecanismos y evidencias

Revisión del código 21eb7866ac995f6d6f3159f2ea342e472893638c | Áreas del Anexo A sujetas a aplicabilidad.

Mecanismo	Capacidad observada	Cláusulas	Área del Anexo A	Evidencia a solicitar
Plan fijado y aplicación	Generar conserva el plan y la raíz de trabajo; apply exige ese artefacto, lo ejecuta sin replanificar y lo descarta al terminar el intento.	8.1 Operación; 7.5 Información documentada. 6.3 solo si cambia el SGIA.	A.6 Ciclo de vida; A.9 Uso de sistemas de IA, según aplicabilidad.	Relación entre petición, commit, plan identificado, decisión válida, ejecución y estado posterior. Hash o firma cuando el procedimiento los exija. Comprobar cómo se protege la identidad del artefacto.
Revisión de cumplimiento	Un modelo evalúa petición y plan bajo reglas configuradas; el programa deriva el veredicto de sus hallazgos. La revisión es opcional y corresponde al modo Generar.	8.1 Operación; 9.1 Seguimiento y evaluación; 7.5 Información documentada.	A.6 Ciclo de vida; A.9 Uso. A.8 si hay requisitos específicos de información a interesados.	Configuración efectiva, reglas y versiones de prompts activas en Phoenix, entrada evaluada, hallazgos y resultado. Pruebas de eficacia y decisión sobre sus límites. El YAML por sí solo no acredita todas las reglas efectivas.
Identidad y roles OIDC	OIDC valida identidad cuando se habilita. Roles y propiedad de sesiones limitan acciones. El emisor vacío distribuido utiliza una identidad local elevada.	5.3 Responsabilidades y autoridad; 8.1 Operación; 7.5 Información documentada.	A.3 Organización interna; A.9 Uso. A.10 para responsabilidades de un proveedor de identidad externo, si procede.	Configuración efectiva saneada del emisor y cliente, validación de tokens, asignación y revisión de roles, propiedad y pruebas de permisos. Relación entre permisos técnicos y atribuciones de la organización; nunca adjuntar secretos.
Reconciliación de drift	El recorrido dedicado ajusta código hacia lo observado, utiliza selección y excepciones y termina sin fijar un plan para apply.	8.1 Operación; 8.2 y 8.3 Evaluación y tratamiento del riesgo.	A.6 Ciclo de vida; A.9 Uso de sistemas de IA.	Ámbito, código de referencia, diferencias observadas, targets, excepciones y propuesta de diff. Criterio y decisión de aceptar, excluir o corregir. La remediación cloud se evalúa por un procedimiento distinto del modo Drift.

Matriz integrada continuación

Revisión del código 21eb7866ac995f6d6f3159f2ea342e472893638c | Áreas del Anexo A sujetas a aplicabilidad.

Mecanismo	Capacidad observada	Cláusulas	Área del Anexo A	Evidencia a solicitar
Importación y estado	La importación relaciona inventario y recursos gestionados y escribe el estado durante la ronda. La revisión posterior de una PR no precede a todas esas escrituras.	8.1 Operación; 7.5 Información documentada; 8.2 Evaluación del riesgo.	A.6 Ciclo de vida; A.9 Uso de sistemas de IA.	Alcance autorizado, inventario y exclusiones, correspondencia de recursos e identificadores, cambios de estado y resultados parciales. Protección y recuperación del backend; evidencias del momento en que se autoriza cada efecto.
Trazas y datos del proceso	Las trazas y las llamadas al modelo pueden contener peticiones, mensajes, herramientas, resultados y metadatos. El registro facilita investigar, pero su mera presencia no prueba minimización.	7.5 Información documentada; 9.1 Seguimiento; 8.2 y 8.3 Riesgo.	A.6 Ciclo de vida; A.9 Uso. A.7 cuando se evalúan datos utilizados por el sistema de IA.	Mapa de datos y destinos, acceso y retención, muestra autorizada y saneada cuando exista, reglas de filtrado y pruebas de minimización. Identificar exactamente qué dato se observó; ausencia de muestra no equivale a fuga demostrada.
Modelos y servicios externos	La solución combina modelos, motor IaC, proveedor Git, bibliotecas y servicios. Las reglas efectivas pueden depender del registro de prompts en Phoenix.	8.1 Operación; 6.1.2 y 6.1.3 Evaluación y tratamiento del riesgo.	A.10 Relaciones con terceros y clientes.	Versiones y procedencia, dependencias, licencias, condiciones del proveedor, flujos de datos, responsabilidades de actualización y aceptación de riesgos. No atribuir al proyecto la seguridad de toda su cadena sin contraste.
Cambios de políticas y responsabilidades del SGIA	Kumoss permite configurar reglas y roles. La aprobación y modificación de políticas, autoridades o criterios del SGIA pertenece al proceso de gestión de la organización.	6.3 Planificación de cambios del SGIA; 5.3 Autoridad; 7.5 Información documentada.	A.2 Políticas de IA; A.3 Organización interna, según aplicabilidad.	Cambio del procedimiento o política, motivo, consecuencias, responsables, revisión, versión y comunicación. Si se propone automerge, política previa y comprobación por cambio mediante controles externos; no capacidad nativa acreditada.

Fuentes de nomenclatura

IEC Vista previa e índice oficial de ISO IEC 42001 2023

BSI AI Controls Implementation Agenda

Las rutas del código y el detalle de esta correspondencia se conservan en la guía HTML y en el registro de fuentes del paquete.