Machine Translated by Google
ROMUS - Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 15/01/2026 | Aceptación: 20/01/2026 | Publicación: 25/01/2026

Gobernanza basada en evidencia y cambios en la gobernanza en infraestructuras nativas de la nube.
Gobernanza basada en la evidencia y cambios en la gobernanza en infraestructuras nativas de la nube.
Gobernanza basada en evidencia y desviación de la gobernanza en infraestructuras nativas de la nube.

Obed Bessa Rocha da Silva
Especialista independiente en arquitectura de soluciones en la nube, DevOps y gobernanza de infraestructura digital.

RESUMEN

Este artículo propone un modelo conceptual de gobernanza basada en evidencia para analizar la divergencia entre la intención institucional aprobada y el estado operativo en infraestructuras nativas de la nube. Se realizó una revisión narrativa estructurada y no exhaustiva de normas, especificaciones, investigaciones revisadas por pares e informes técnicos, organizada en cinco categorías: representación de la intención, automatización del cambio, identidad y procedencia, observación del estado y gestión de desviaciones. La síntesis delimita la deriva de la gobernanza en relación con las desviaciones de configuración y las violaciones aisladas de políticas, describe un ciclo de seis pasos que vincula la intención, el estado declarado, la entrega, el estado observado, la clasificación de la materialidad y la respuesta, y presenta una taxonomía de desviaciones y un modelo de...
Madurez en cinco niveles. Se argumenta que la gobernanza persistente depende de evidencia verificable, identidades estables, comparación semántica y respuestas proporcionales al riesgo. El trabajo es conceptual: no valida escalas, umbrales universales ni eficacia organizacional. Su contribución radica en explicitar las relaciones y los criterios necesarios para la futura operacionalización y evaluación empírica de la deriva de la gobernanza.

Palabras clave: gobernanza digital; desviación de la gobernanza; nativo de la nube; DevSecOps; procedencia; gestión de la configuración.

ABSTRACTO

Este artículo propone un modelo de gobernanza basado en la evidencia para analizar la divergencia entre la intención institucional aprobada y el estado operativo en infraestructuras nativas de la nube. Se realizó una revisión narrativa estructurada, aunque no exhaustiva, de estándares, especificaciones, investigaciones revisadas por pares e informes técnicos, organizada en cinco categorías: representación de la intención, automatización del cambio, identidad y procedencia, observación del estado y tratamiento de la desviación. La síntesis distingue la deriva de la gobernanza de la deriva de la configuración y las violaciones aisladas de políticas, describe un ciclo de seis etapas que vincula la intención, el estado declarado, la entrega, el estado observado, la clasificación de la materialidad y la respuesta, y presenta una taxonomía de la desviación y un modelo de madurez de cinco niveles. Se argumenta que la gobernanza persistente depende de la evidencia consultable, las identidades estables, la comparación semántica y las respuestas proporcionales al riesgo. El trabajo es conceptual: no valida una escala, umbrales universales ni la eficacia organizacional. Su contribución radica en explicitar las relaciones y los criterios necesarios para la futura operacionalización y evaluación empírica de la deriva de la gobernanza.
Palabras clave: gobernanza digital; deriva de la gobernanza; nativo de la nube; DevSecOps; procedencia; gestión de la configuración.

1. INTRODUCCIÓN

Las arquitecturas nativas de la nube reemplazan conjuntos de servidores relativamente estables con

ecosistemas compuestos por microservicios, contenedores, controladores, canalizaciones de integración y

Entrega continua e interfaces declarativas. Este cambio aumenta la velocidad y la elasticidad, pero...

También profundiza en los puntos en los que una decisión autorizada puede no corresponderse con el Estado.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 15/01/2026 | Aceptación: 20/01/2026 | Publicación: 25/01/2026

Implementado eficazmente. El desafío de la gobernanza ya no se trata solo de aprobar un cambio, sino de llevarlo a cabo.
reconstruir quién lo autorizó, qué artefactos se produjeron, cómo llegaron a producirse, qué
El resultado se determinó en función de si la divergencia se mantenía dentro del riesgo aceptado.
La gestión de configuración tradicional proporciona principios básicos, control de cambios y...
La monitorización, junto con la infraestructura como código y GitOps, forman parte de la intención de control de versiones.
y conciliables (NIST, 2019; RAHMAN; MAHDAVI-HEZAVEH; WILLIAMS, 2019; BEETZ;
(HARRER, 2022). Sin embargo, estas capacidades no garantizan que la configuración declarada tenga
autoridad institucional, que la cadena de suministro permanezca intacta o que el estado observado
Mantener un vínculo verificable con las aprobaciones y excepciones. La documentación sobre procedencia y seguridad.
La cadena de suministro de software cubre parcialmente esta brecha, pero no reemplaza la decisión de gobernanza con respecto a...
materialidad, legitimidad y respuesta (W3C, 2013; TORRES-ARIAS et al., 2019; SLSA)
COMUNIDAD, 2025).

En este artículo, la desviación de la gobernanza se refiere a la divergencia material entre la intención institucional autorizada.
y la realidad operativa observable. La intención puede expresarse en políticas y decisiones.
Aspectos arquitectónicos, configuraciones declaradas, requisitos reglamentarios y excepciones aprobadas. La realidad.
El término "operacional" incluye los recursos en funcionamiento, las identidades, las relaciones, los permisos y las pruebas producidas.
durante la entrega y la operación. La divergencia solo adquiere importancia para la gobernanza cuando se interpreta
con respecto a autoridad, riesgo, alcance, duración y responsabilidad; diferencia técnica aislada no
Ya es suficiente.

El estudio responde a tres preguntas: RQ1 — ¿Cómo distinguir la desviación de la gobernanza de las desviaciones técnicas?
¿Adyacentes? RQ2 — ¿Qué evidencia vincula la intención aprobada, la entrega y el estado observado? RQ3 —
¿Cómo clasificar y gestionar las discrepancias sin confundir la automatización con el control absoluto?
Las contribuciones son: una construcción bien definida; un ciclo analítico de seis pasos; y una taxonomía de...
desviaciones y respuestas; modelo de madurez impulsado por capacidades verificables; y agenda de
validación empírica.

La relevancia práctica proviene de la escala alcanzada por el sustrato nativo de la nube. En la encuesta anual de
En la encuesta de la CNCF de 2023, el 66% de los consumidores potenciales o actuales que respondieron afirmaron utilizar Kubernetes.
en producción y el 18% dijo que lo estaba evaluando (CNCF, 2024). Estos porcentajes no demuestran
La madurez de la gobernanza no representa universalmente a todas las organizaciones, pero sí indica que
Las decisiones automatizadas y los estados efímeros se han convertido en una parte habitual de la infraestructura digital.

2. METODOLOGÍA

Se realizó una revisión narrativa estructurada y no exhaustiva, adecuada para el propósito de integrar conceptos.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 15/01/2026 | Aceptación: 20/01/2026 | Publicación: 25/01/2026

derivados de la ingeniería de software, la seguridad, la gobernanza y las operaciones, sin estimar los efectos.
agregados. La calidad de la revisión se guió por los seis dominios de SANRA: relevancia, objetividad,
Descripción de la búsqueda, las referencias, el razonamiento científico y la presentación de los datos relevantes.
(BAETHGE; GOLDBECK-WOOD; MERTENS, 2019). SANRA fue contratada como
Instrumento crítico, no como protocolo de revisión sistemática.

La búsqueda dirigida se completó el 25 de agosto de 2026 en IEEE Xplore, la biblioteca digital de la ACM.
ScienceDirect y USENIX, además de los repositorios oficiales de NIST, ISO, W3C, CNCF, DORA y SLSA.
Los términos "deriva de la gobernanza", "deriva de la configuración" y "política" se combinaron en portugués e inglés.
código, infraestructura como código, GitOps, gobernanza nativa de la nube, monitoreo continuo, software
procedencia, SLSA, DevSecOps y cadena de suministro de software. La búsqueda abarcó publicaciones hasta la fecha de
recortado, sin un límite inferior rígido, debido a las normas fundamentales de procedencia y seguimiento.
Siguen siendo técnicamente válidos.

Se incluyeron documentos con autoría y origen rastreables que contribuyeron directamente al proyecto.
al menos una de las cinco categorías analíticas: representación de la intención; automatización del cambio;
Identidad y procedencia; observación del estado; y manejo de desviaciones. Se priorizaron las normas y los estándares.
Especificaciones primarias, investigaciones revisadas por pares e informes con metodología descrita. Fueron
Excluyendo materiales promocionales, duplicados, textos sin autoría identificable y fuentes que solo
Mencionaron herramientas sin discutir mecanismos, evidencia o riesgos. El corpus final compilado 21
documentos.

La síntesis se llevó a cabo mediante comparación conceptual. Para cada fuente, se registraron objetos de control.
autoridad presunta, artefacto observado, garantía ofrecida, riesgo residual y respuesta anticipada. En
A continuación, los mecanismos se organizaron en el ciclo propuesto y se sometieron a tres pruebas de consistencia:
distinción entre disponibilidad de evidencia y corrección semántica; separación entre autorización y
configuración; y preservación de la responsabilidad humana. No se realizó ninguna evaluación de la organización.
experimento, entrevista o medición de incidentes.

Como limitaciones metodológicas, la búsqueda no pretende una cobertura bibliométrica exhaustiva, ni tampoco realizó...
La doble evaluación independiente combina la literatura científica con estándares y evidencia técnica.
institucional. En consecuencia, la síntesis respalda la plausibilidad conceptual y la trazabilidad de
proposiciones, pero no prevalencia, causalidad, umbrales universales o efectividad del modelo en
producción.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 15/01/2026 | Aceptación: 20/01/2026 | Publicación: 25/01/2026

3. FUNDAMENTOS CONCEPTUALES Y DELIMITACIÓN

3.1 La gobernanza como capacidad sociotécnica

La gobernanza digital define los derechos de toma de decisiones, los límites de la autonomía, los criterios de aceptación de riesgos y...
formas de rendición de cuentas. En entornos nativos de la nube, estos elementos se entrecruzan.
Repositorios, catálogos de servicios, canalizaciones, registros, clústeres y plataformas de observabilidad.
Las normas NIST SP 800-53 Rev. 5 e ISO/IEC 27001:2022 ubican los controles dentro de los procesos.
Estrategias de gestión de riesgos organizacionales, evitando reducirlas a una lista de verificación aplicada después de su implementación.
(NIST, 2020; ISO, 2022a).
Su naturaleza sociotécnica se deriva de la interdependencia entre código, infraestructura y coordinación.
humano. Una política técnicamente correcta puede fallar sin un propietario, una ruta de remediación o
Excepción documentada: un proceso bien diseñado puede verse comprometido por un exceso de credenciales.
Cambios manuales y fuentes de información contradictorias. Los estudios de DevOps vinculan el rendimiento.
sostenible a través de la combinación de capacidades técnicas, culturales y de aprendizaje, y la investigación de
La infraestructura como código demuestra que su adopción no elimina los desafíos de las pruebas, el mantenimiento y el soporte.
(FORSGREN; HUMBLE; KIM, 2018; GUERRIERO et al., 2019).
Los controladores declarativos especifican explícitamente el estado deseado y ejecutan bucles de reconciliación.
Sin embargo, los sistemas distribuidos permiten divergencias transitorias, fallos parciales e intervenciones.
emergencias. La experiencia adquirida en Borg, Omega y Kubernetes demuestra la centralidad de
mecanismos de control y convergencia continuos, sin implicar que cada diferencia de estado sea una
Violación de la gobernanza (BURNS et al., 2016). El análisis requiere autoridad, contexto y materialidad.

3.2 Desviación de la gobernanza y conceptos relacionados

La Tabla 1 describe el concepto propuesto. La deriva de configuración describe la diferencia entre la línea base o
Configuración deseada y configuración observada. Se produce una violación de la política como código cuando una regla
No se cumple el requisito ejecutable. Aparece una brecha de procedencia cuando no es posible demostrarlo.
Origen, proceso o identidad. La deriva de la gobernanza puede incluir cualquiera de estas condiciones, pero
Esto requiere un elemento adicional: una divergencia significativa entre la realidad operativa y la intención.
institución autorizada.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
ROMUS - Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 15/01/2026 | Aceptación: 20/01/2026 | Publicación: 25/01/2026

Tabla 1 – Delimitación entre la deriva de la gobernanza y conceptos adyacentes.

Concepto	Objeto comparado	cuestión central	Respuesta típica
desviación de la configuración	Configuración de referencia/ deseada × configuración observada	¿Hubo alguna divergencia en la situación técnica?	Conciliar o actualizar la línea base.
Violación de la política	Estado o artefacto × regla aplicable	¿Se infringió alguna condición codificada?	Bloquear, alertar o crear una excepción.
Brecha de procedencia	Artefacto/estado × origen, proceso e identidad	¿Se puede verificar la cadena?	Preservar, correlacionar o reconstruir la evidencia.
Desviación de la gobernanza	Intención autorizada frente a realidad operativa	¿Afecta esta divergencia al riesgo, la legitimidad o la rendición de cuentas?	Clasificar, contener, reconciliar, aceptar o investigar.

Fuente: compilado por el autor con base en NIST (2019, 2022a, 2024), W3C (2013), Rahman, Mahdavi-Hezaveh y Williams (2019), Beetz y Harrer (2022) y SLSA Community (2025).

La distinción evita dos errores. El primero es clasificar cualquier cambio de emergencia como un fallo, incluso cuando está autorizado, registrado y es temporal. El segundo es presumir la conformidad porque un La configuración coincide con el repositorio, aunque el repositorio no representa la decisión actual o la La cadena de entrega no se puede verificar. Por lo tanto, la deriva de la gobernanza es una relación entre estados y autoridad, no un atributo aislado de un archivo.

4. Modelo de gobernanza basado en la evidencia

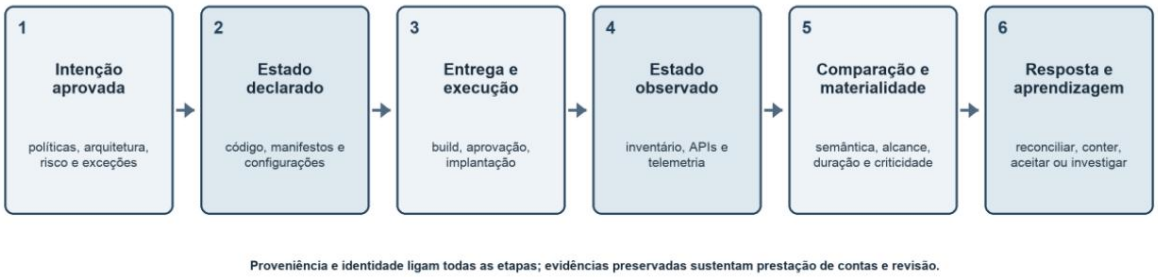
El modelo organiza la gobernanza persistente en seis pasos interconectados. Cada paso produce o consume. evidencia, pero ninguna fuente por sí sola prueba la exactitud general. La verificabilidad depende de identidad estable, semántica temporal y la capacidad de relacionar decisiones, artefactos, actividades y estados.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 15/01/2026 | Aceptación: 20/01/2026 | Publicación: 25/01/2026

Figura 1 – Ciclo de gobernanza basado en la evidencia



Fuente: elaborado por el autor.

4.1 Intención aprobada y estado declarado

La intención aprobada abarca políticas, decisiones arquitectónicas, criterios de riesgo y requisitos.
Procedimientos reglamentarios y de excepción. El primer requisito es declarar qué artefacto tiene autoridad para cada uno.
La decisión y por cuánto tiempo. La norma ISO/IEC 27001:2022 exige que el sistema de gestión de seguridad sea
apropiado al contexto y los riesgos de la organización, mientras que el NIST SSDF recomienda integrar
Prácticas de desarrollo seguras a lo largo de todo el ciclo de vida (ISO, 2022a; NIST, 2022b).
El estado declarado traduce parte de esta intención en código de infraestructura, manifiestos, catálogos y
Reglas ejecutables. La infraestructura como código mejora el versionado y la repetibilidad, pero los estudios
Señalan limitaciones en las pruebas, el mantenimiento y el soporte de herramientas (RAHMAN; MAHDAVI-HEZAVEH;
WILLIAMS, 2019; GUERRIERO et al., 2019). GitOps agrega reconciliación basada en
repositorios, sin resolver unilateralmente la autoridad, los conflictos entre fuentes o la legitimidad de las excepciones.
(BEETZ; HARRER, 2022).

4.2 Entrega, ejecución y estado observado

Entre la declaración y la ejecución hay construcciones, verificaciones, firmas, aprobaciones, mutaciones de
Acciones de admisión y control. Fallo parcial, dependencia no disponible o intervención manual.
Esto puede producir un resultado diferente al previsto. Por lo tanto, no se recomienda comparar únicamente el repositorio y la configuración.
Los datos generados son insuficientes: el estado observado debe incluir inventario, API del plano de control,
Telemetría, identidades y relaciones en tiempo de ejecución.
La política como código permite anticipar los controles, pero las reglas codificadas siguen siendo software: pueden
Contienen errores, se vuelven obsoletos y producen efectos sistémicos. La norma NIST SP 800-204C describe la política.
La observabilidad como código y la observabilidad como código como componentes de DevSecOps nativo de la nube y NIST SP 800-
204D integra controles de cadena de software en pipelines (NIST, 2022a, 2024). La gobernanza debería

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 15/01/2026 | Aceptación: 20/01/2026 | Publicación: 25/01/2026

Pruebe las reglas, cree versiones de las mismas, supervise su impacto y conserve los procedimientos de excepción.

4.3 La procedencia como vínculo verificable

La procedencia describe las entidades, actividades y agentes involucrados en la producción de un artefacto o...
estado. El modelo PROV del W3C proporciona un vocabulario interoperable para representar estas relaciones.
(W3C, 2013). En la cadena de software, in-toto, SLSA y Sigstore demuestran mecanismos
Medidas complementarias para la declaración, la certificación, la firma vinculada a la identidad y la transparencia.
(TORRES-ARIAS et al., 2019; NEWMAN; MEYERS; TORRES-ARIAS, 2022; SLSA
COMUNIDAD, 2025).
Los metadatos, por sí solos, no garantizan la fiabilidad. Si el mismo actor puede alterar tanto el artefacto como el registro...
Sin detección, la evidencia tendrá una independencia limitada. Los controles más estrictos utilizan la separación de
funciones, identidades efímeras, constructores controlados, firmas verificables y almacenamiento
con la retención adecuada. La cadena también debe ser buscable: identificadores inmutables, como
Los resúmenes reducen las correlaciones manuales y permiten la localización de artefactos afectados por vulnerabilidad o
incidente.
La recopilación de datos debe centrarse en la minimización y la finalidad. Las pruebas no deben revelar secretos ni información confidencial.
Personal innecesario. La gobernanza basada en la evidencia no es lo mismo que la vigilancia total;
Busca los elementos necesarios para respaldar la toma de decisiones, la rendición de cuentas y la reconstrucción, con acceso y
retención proporcional al riesgo.

5. DETECCIÓN, CLASIFICACIÓN Y RESPUESTA

La detección de la deriva requiere una función de comparación y un modelo de materialidad. Las diferencias sintácticas pueden ser...
irrelevante, como un cambio semántico menor, por ejemplo, ampliar una política de red o
Cambiar la identidad de ejecución puede alterar sustancialmente el riesgo. Los comparadores deberían
normalizar las representaciones, conocer los valores estándar, considerar las relaciones entre los recursos y registrar las
el momento de validez de cada observación.
El monitoreo continuo de NIST SP 800-137 proporciona principios aplicables: visibilidad en
activos, amenazas, vulnerabilidades y eficacia de los controles (NIST, 2011). En entornos efímeros,
La frecuencia de la recopilación de datos debe ir al ritmo del cambio. Controlar eventos, instantáneas
Los documentos firmados y las consultas periódicas proporcionan pruebas complementarias; las revisiones periódicas son lentas.
Es posible que no capturen recursos que existieron durante minutos.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
ROMUS - Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 15/01/2026 | Aceptación: 20/01/2026 | Publicación: 25/01/2026

Tabla 2 – Taxonomía operativa de las divergencias

Clase	Condición	Tratamiento estándar	Evidencia mínima
Autorizado y temporal	Cambio aprobado, con fecha límite y responsable.	Realizar el seguimiento y la conciliación al vencimiento.	Aprobación, alcance, validez y estado
Operacional benigno	Variación prevista sin cambios sustanciales en el riesgo.	Registrar o normalizar la comparación	Regla de tolerancia y observación
deriva de control	Control ausente, obsoleto o eludido.	Control correcto y evaluación de la cobertura.	Versión de la política, resultado y excepción.
desviación de seguridad	Divulgación de información sobre confidencialidad, integridad o disponibilidad del material.	Contener, preservar las pruebas e investigar.	Cronología, identidad, alcance y artefactos
Indeterminado	Pruebas insuficientes o contradictorias	Absténgase de realizar correcciones destructivas y recoja contexto	Brechas y nivel de confianza declarado

Fuente: elaborado por el autor.

La clase indeterminada es necesaria para evitar la certeza artificial. Corrección automática basada en
Las pruebas incompletas pueden ocultar señales útiles, interrumpir los servicios o ampliar la interpretación.
equivocado. Para riesgos bajos y reglas bien probadas, la conciliación automática es plausible; para
Altos riesgos o baja confianza, preservación del contexto, contención y revisión humana deberían
para prevenir cambios irreversibles.

Los indicadores útiles incluyen el tiempo entre la desviación y la detección, el tiempo hasta la conciliación y la proporción de cambios fuera del flujo de trabajo aprobado, cobertura de recursos por política, tasa de excepciones vencidas y integridad de los vínculos de procedencia. Estos indicadores deberían apoyar el aprendizaje, no el aprendizaje. Clasificación de individuos. Los objetivos aislados fomentan la optimización local; una lectura precisa tiene esto en cuenta. Incidentes, carga de trabajo, experiencia del desarrollador y resultados de confiabilidad.

6 controles incorporados al ciclo DevSecOps

La integración de la gobernanza en los procesos permite anticipar problemas y reducir el costo de la remediación. Los controles pueden... Verifique las dependencias, los secretos, el código de infraestructura, las imágenes, las firmas y las políticas antes de... Promoción, mantenimiento de resultados y aprobaciones. La entrega continua ya gestiona la compilación, las pruebas y el despliegue. como un flujo automatizado; la característica distintiva de la gobernanza basada en evidencia es preservar la conexión.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
IRCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 15/01/2026 | Aceptación: 20/01/2026 | Publicación: 25/01/2026

entre cada resultado, la decisión que lo autorizó y el estado que realmente surgió (HUMBLE;
FARLEY, 2010).

El enfoque "shift left" no transfiere toda la responsabilidad a los desarrolladores. Equipos de seguridad y plataforma.
Deben proporcionar reglas comprensibles, herramientas confiables y rutas de manejo de excepciones. Controles con
Los mensajes poco claros y las altas tasas de falsos positivos fomentan la elusión de las medidas de seguridad. El informe DORA de 2024 relaciona esto con...
Las plataformas internas generan ganancias en productividad y rendimiento organizacional, pero también registran
reducciones de rendimiento y estabilidad en ciertos contextos; experiencia del usuario, independencia y
La adopción como producto son condiciones de diseño, no detalles cosméticos (GOOGLE CLOUD;
DORA, 2024).

Es necesario combinar los controles preventivos con mecanismos de detección y respuesta.
Las vulnerabilidades surgen después del despliegue, las dependencias cambian y las identidades pueden verse comprometidas...
Comprometido. Las políticas de tiempo de ejecución, observabilidad y respuesta cubren los riesgos residuales. A
La separación de funciones debe ser proporcional: los servicios críticos pueden requerir una revisión independiente.
mientras que los cambios de bajo riesgo pueden ir precedidos de la automatización con límites claros.
El principio fundamental no es multiplicar las aprobaciones, sino evitar que una sola identidad las altere.
Intención, artefacto, evidencia y producción sin posibilidad de detección. Firmas y registros de
La transparencia reduce este riesgo, pero garantizarla depende de un modelo de amenazas, verificación y...
protección de identidades (NEWMAN; MEYERS; TORRES-ARIAS, 2022).

7. Modelo de madurez basado en la evidencia

La madurez se considera una capacidad demostrable, no una cantidad de herramientas. El marco
3 presenta cinco niveles acumulativos. La progresión debe evaluarse según los servicios y los riesgos materiales;
Una organización puede encontrarse en diferentes niveles dependiendo del ámbito que se esté analizando.

Tabla 3 – Niveles de madurez y criterios verificables

Nivel	Capacidad dominante	Evidencia esperada	Criterios de progresión
1 — Fragmentado	Inventario incompleto y responsabilidades	Registros dispersos y cambios manuales	Identificar los activos críticos, las partes responsables y las fuentes de información fidedigna.
2 — Declarado	Revisión de la intención y los cambios según la versión	Repositorios, líneas base y aprobaciones	Observa el estado actual y relaciónalo con la versión declarada.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 15/01/2026 | Aceptación: 20/01/2026 | Publicación: 25/01/2026

Nivel	Capacidad dominante	Evidencia esperada	Criterios de progresión
3 — Rastreable	Procedencia en todas las etapas: revisión, compilación, artefacto y despliegue.	Certificaciones, firmas, identidades y resúmenes	Consultar la cadena de suministro dentro del plazo establecido y detectar deficiencias.
4 — Sensible	La deriva se clasifica y se trata como un riesgo.	Alertas priorizadas, excepciones con periodos de validez y conciliaciones.	Demostrar puntualidad, cobertura, fiabilidad y resultados.
5 — Adaptado	Los controles aprenden de los incidentes y las métricas.	Revisiones de eficacia, ensayos controlados y cambios transparentes.	Reducir la reincidencia sin aumentar la fricción ni el riesgo residual.

Fuente: elaborado por el autor.

La progresión no presupone una automatización completa. Entornos sencillos, con responsabilidades claras y
Las pruebas fiables pueden ser más fáciles de gestionar que los conjuntos de datos extensos y desconectados.
Las evaluaciones deben probar si la organización puede reconstruirse después del cambio, identificar la exposición,
restablecer el estatus y explicar las decisiones a una parte independiente.
En el nivel adaptativo, las políticas se versionan y se prueban, las excepciones caducan y se realizan cambios en los controles.
Siguen un proceso transparente. La plataforma ofrece rutas aprobadas, pero permite...
Desafío y evolución. La automatización recopila, compara y ejecuta respuestas predecibles; las personas definen.
Valoran las cosas, aceptan riesgos y consideran las consecuencias.

8. DISCUSIÓN

8.1 Implicaciones teóricas y prácticas

La principal implicación teórica es separar la gobernanza de la conformidad momentánea. Una instantánea.
ya que puede que no explique cómo se produjo el estado; una desviación puede ser legítima cuando
Autorizado y temporal. El modelo cambia la unidad de análisis del archivo aislado a la cadena.
entre decisión, artefacto, actividad y observación. Esto acerca la gobernanza, la procedencia y la operación.
sin afirmar que uno de ellos reemplaza a los demás.
En la práctica, la organización puede comenzar con preguntas verificables: ¿qué artefacto tiene autoridad?
¿Quién aprobó la versión actual? ¿El despliegue se basa en la compilación prevista? ¿Cuál es el estado observado?
¿Está dentro de los límites aceptables? ¿Se puede recuperar la evidencia en el plazo requerido? Cuando la respuesta
Dado que la información es desconocida, la laguna debe registrarse como incertidumbre, no como una suposición que la rellene.
El modelo también reduce el falso dilema entre velocidad y control. Rutas y políticas aprobadas

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
ROMUS - Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 15/01/2026 | Aceptación: 20/01/2026 | Publicación: 25/01/2026

Las pruebas y la evidencia producidas durante el flujo de trabajo impiden la reconstrucción manual posterior. Sin embargo,
Los controles mal diseñados aumentan la carga cognitiva y fomentan rutas paralelas. Se necesitan medidas de gobernanza.
Debe ser consumible, observable y ajustable, además de técnicamente riguroso.

8.2 Limitaciones y agenda de investigación

Este trabajo no valida la construcción, no define ponderaciones ni establece umbrales de materialidad.
Las categorías pueden superponerse y los distintos revisores pueden discrepar al respecto.
Legitimidad, alcance y respuesta. La bibliografía seleccionada se centra en la seguridad, la ingeniería y...
El software y las normas internacionales, así como los aspectos legales, sectoriales y culturales, requieren estudios separados.
La agenda de investigación incluye: operacionalizar las dimensiones sin ocultar sus componentes; medir
Acuerdo entre evaluadores; prueba de si la exhaustividad de la procedencia y el tiempo de evidencia son predictivos.
Calidad de la reconstrucción; comparación de la detección sintáctica y semántica; análisis de costes y efectos adversos.
de conciliación automática; y realizar estudios multiorganizacionales que separen la correlación de
causalidad.

También son necesarios los protocolos de refutación. El modelo pierde su utilidad si la clasificación no es...
Mejorar la priorización de alertas técnicas simples si la procedencia no reduce el tiempo o
Incertidumbre de la investigación, si los controles incorporados simplemente cambian el trabajo o si los niveles de
Los niveles de madurez no pueden evaluarse con un acuerdo aceptable. Estos resultados deberían ser
tratado como evidencia en contra del modelo, no como un fracaso de su adopción.

9. CONCLUSIÓN

Las infraestructuras nativas de la nube hacen que la gobernanza basada únicamente en evaluaciones resulte insuficiente.
publicaciones periódicas. La divergencia relevante no es ninguna diferencia textual, sino la separación material entre
intención autorizada y realidad operativa, interpretadas según riesgo, legitimidad, duración y
Responsabilidad. La deriva de la gobernanza ofrece una categoría analítica para examinar esta deriva.
sin presuponer que todo desacuerdo constituye un defecto.
La síntesis mostró que la intención versionada, el estado observado, la procedencia buscable, la comparación
La semántica y la respuesta proporcional conforman capacidades complementarias. Política como código y flujos de trabajo.
DevSecOps mejora la prevención, pero no elimina los riesgos residuales ni sustituye el criterio profesional.
La madurez deseada es la capacidad de explicar, verificar y corregir los cambios con pruebas.
incertidumbre suficiente y explícita.
El modelo propuesto sigue siendo conceptual. Su contribución consiste en proporcionar límites, etapas, clases y...

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 15/01/2026 | Aceptación: 20/01/2026 | Publicación: 25/01/2026

criterios que pueden ser cuestionados empíricamente. El siguiente paso científico es comprobar si estos
Las capacidades mejoran la reconstrucción, la priorización y la recuperación en diferentes organizaciones, sin
Confundir un mayor volumen de registros con una mejor gobernanza.

DECLARACIONES

Financiación: Este estudio no recibió financiación externa.

Conflictos de interés: el autor declara no tener conflictos de interés.

Disponibilidad de datos: el estudio no produjo un conjunto de datos; las fuentes analizadas son:
identificado en las referencias.

Uso de inteligencia artificial generativa: la herramienta de IA generativa de OpenAI se utilizó como
Apoyo editorial, lingüístico y estructural. El autor revisó el contenido, verificó las referencias y asume la responsabilidad.
Responsabilidad total por la versión enviada.

REFERENCIAS

BAETHGE, Christopher; GOLDBECK-WOOD, Sandra; MERTENS, Stephan. SANRA: una escala para la evaluación de la calidad de los artículos de revisión narrativa. Research Integrity and Peer Review, vol. 4, art. 5, 2019. DOI: 10.1186/s41073-019-0064-8.

BEETZ, Florian; HARRER, Simon. GitOps: ¿La evolución de DevOps? IEEESoftware, vol. 39, n.º 4, págs. 70–75, 2022. DOI: 10.1109/MS.2021.3119106.

BURNS, Brendan; GRANT, Brian; OPPENHEIMER, David; BREWER, Eric; WILKES, John. Borg, Omega y Kubernetes. Communications of the ACM, vol. 59, n.º 5, págs. 50-57, 2016. DOI: 10.1145/2890784.

CNCF — Fundación para la Computación Nativa en la Nube. Encuesta Anual de la CNCF 2023. San Francisco: CNCF, 2024. Disponible en: https://www.cncf.io/reports/cncf-annual-survey-2023/.
Consultado el 25 de agosto de 2026.

FORSGREN, Nicole; HUMBLE, Jez; Kim, Gene. Accelerate: The Science of Lean Software and DevOps. Portland: IT Revolution, 2018.

GOOGLE CLOUD; DORA. Acelerar el estado de DevOps 2024. Mountain View: Google Cloud, 2024. Disponible en: https://dora.dev/research/2024/dora-report/. Consultado el 25 de agosto de 2026.

GUERRERO, Michele; GARRIGA, Martín; TAMBURRI, Damián A.; PALOMBA, Fabio.
Adopción, soporte y desafíos de la infraestructura como código: perspectivas de la industria. En: IEEE INTERNATIONAL CONFERENCE ON SOFTWARE MAINTENANCE AND EVOLUTION, 2019. Actas [...]. IEEE, 2019. págs. 580–589. DOI: 10.1109/ICSME.2019.00092.

HUMBLE, Jez; FARLEY, David. Entrega continua: lanzamientos de software confiables a través de Build,

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 15/01/2026 | Aceptación: 20/01/2026 | Publicación: 25/01/2026

Automatización de pruebas e implementación. Boston: Addison-Wesley, 2010.

ISO — ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO/IEC 27001:2022: Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos. Ginebra: ISO, 2022a.

ISO — ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO/IEC 27002:2022: Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información. Ginebra: ISO, 2022b.

NEWMAN, Zachary; MEYERS, John Speed; TORRES-ARIAS, Santiago. Sigstore: Software de firma para todos. En: ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 2022. Actas [...]. Nueva York: ACM, 2022. págs. 2353–2367.
DOI: 10.1145/3548606.3560596.

NIST — INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA. SP 800-137: Monitoreo continuo de la seguridad de la información (ISCM) para sistemas y organizaciones de información federales. Gaithersburg: NIST, 2011. DOI: 10.6028/NIST.SP.800-137.

NIST — INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA. SP 800-128: Guía para la gestión de la configuración de sistemas de información centrada en la seguridad. Actualización 1.
Gaithersburg: NIST, 2019. DOI: 10.6028/NIST.SP.800-128.

NIST — INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA. SP 800-53 Rev. 5: Controles de seguridad y privacidad para sistemas y organizaciones de información. Gaithersburg: NIST, 2020.
DOI: 10.6028/NIST.SP.800-53r5.

NIST — INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA. SP 800-204C: Implementación de DevSecOps para una aplicación basada en microservicios con malla de servicios.
Gaithersburg: NIST, 2022a. DOI: 10.6028/NIST.SP.800-204C.

NIST — INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA. SP 800-218: Marco de desarrollo de software seguro (SSDF), versión 1.1. Gaithersburg: NIST, 2022b. DOI: 10.6028/NIST.SP.800-218.

NIST — INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA. SP 800-204D: Estrategias para la integración de la seguridad de la cadena de suministro de software en las canalizaciones de CI/CD de DevSecOps.
Gaithersburg: NIST, 2024. DOI: 10.6028/NIST.SP.800-204D.

RAHMAN, Akond; MAHDAVI-HEZAVEH, Rezvan; WILLIAMS, Laurie. Un estudio de mapeo sistemático de la investigación sobre infraestructura como código. Information and Software Technology, vol. 108, págs. 65–77, 2019. DOI: 10.1016/j.infsof.2018.12.004.

COMUNIDAD SLSA. Niveles de la cadena de suministro para artefactos de software: Especificación, versión 1.2. 2025. Disponible en: https://slsa.dev/spec/v1.2/. Consultado el: 25 de agosto de 2026.

TORRES-ARIAS, Santiago; AFZALI, Hammad; KUPPUSAMY, Trishank Karthik; CURTMOLA, Reza; CAPPOS, Justin. in-toto: Proporcionando garantías de granja a mesa para bits y bytes. En: USENIX SECURITY SYMPOSIUM, 28., 2019. Actas [...]. Berkeley: USENIX Association, 2019. págs. 1393–1410.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 15/01/2026 | Aceptación: 20/01/2026 | Publicación: 25/01/2026

W3C — CONSORCIO DE LA WORLD WIDE WEB. PROV-O: La ontología PROV. Recomendación del W3C, 30 de abril de 2013. Disponible en: https://www.w3.org/TR/prov-o/. Consultado el 25 de agosto de 2026.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.