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

Año VII, vol. 2, 2026 | Envío: 23 de octubre de 2026 | Aceptación: 28 de octubre de 2026 | Publicación: 2 de noviembre de 2026

Operaciones en la nube y DevOps con un enfoque centrado en la gobernanza para instituciones con una misión clara: un modelo práctico para la confianza, la auditabilidad y la inclusión digital.
Operaciones en la nube y DevOps con enfoque en la gobernanza para instituciones con una misión social: un modelo práctico para la confiabilidad, la auditabilidad y la inclusión digital.
Operaciones en la nube y DevOps con prioridad en la gobernanza para instituciones orientadas a la misión: un modelo práctico para la fiabilidad, la auditabilidad y la inclusión digital.

Obed Bessa Rocha da Silva
Arquitecto independiente de soluciones en la nube e investigador de DevOps.

RESUMEN
Las instituciones con una misión social dependen cada vez más de la computación en la nube y las prácticas DevOps; sin embargo, muchas operan con equipos reducidos, procesos heredados y altas expectativas en cuanto a continuidad, rendición de cuentas y confianza pública. Este artículo propone un modelo operativo con prioridad en la gobernanza para entornos institucionales de nube y DevOps. El modelo organiza las prácticas en torno a cinco capacidades que se refuerzan mutuamente: base arquitectónica, estandarización operativa, seguridad y auditabilidad, observabilidad y respuesta a incidentes, y capacitación del personal. En lugar de tratar la gobernanza como una capa de documentación posterior a la implementación, el artículo la plantea como un control de ingeniería que puede incorporarse a arquitecturas de referencia, manuales de procedimientos, guías de procedimientos, rutinas de acceso y ciclos de mejora continua. Este artículo está dirigido a líderes y profesionales de TI de organizaciones del sector público, educativo, sin fines de lucro y comunitarias que necesitan modernizar su infraestructura digital sin perder la trazabilidad ni la disciplina operativa. El texto sintetiza patrones de práctica profesional en arquitectura de la nube, DevOps, seguridad e ingeniería de confiabilidad en un modelo aplicable y adaptable a instituciones con diferentes niveles de madurez.

Palabras clave: gobernanza en la nube; DevOps; infraestructura digital; tecnología institucional; ingeniería de confiabilidad; auditabilidad; respuesta a incidentes; inclusión digital.

1. INTRODUCCIÓN

La computación en la nube y DevOps han transformado los costes y la velocidad de la infraestructura digital.

En las organizaciones tecnológicas comerciales, el discurso predominante suele hacer hincapié en la velocidad:

Ciclos de lanzamiento más cortos, plataformas elásticas, automatización y entrega continua. Instituciones

Las organizaciones orientadas a la misión se enfrentan a las mismas presiones técnicas, pero su contexto operativo es

diferente. Organismos públicos, organizaciones educativas, instituciones sociales, iglesias, programas sin

Las iniciativas con fines de lucro y comunitarias a menudo requieren infraestructura moderna y

Al mismo tiempo, deben preservar la continuidad, la rendición de cuentas y unos controles comprensibles.

Incluso sin grandes equipos especializados en plataformas, sus sistemas admiten servicios de

de lo que la gente depende.

En estos entornos, la cuestión central no es simplemente cómo migrar cargas de trabajo a

Plataformas en la nube o automatización de despliegues. La pregunta más difícil es cómo hacerlas gobernables.

Prácticas de Cloud y DevOps: cómo garantizar que las configuraciones sean reproducibles,

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: 23 de octubre de 2026 | Aceptación: 28 de octubre de 2026 | Publicación: 2 de noviembre de 2026

Los incidentes pueden diagnosticarse, las decisiones de acceso pueden ser auditables y el conocimiento
La gobernanza operativa no debe limitarse a la memoria de un único líder técnico. En este sentido, la gobernanza no es
burocracia. Es el conjunto de prácticas de ingeniería y gestión que permiten a la institución generar confianza.
en su infraestructura digital.
Este artículo presenta un modelo que prioriza la gobernanza para las operaciones institucionales en la nube.
y DevOps. El modelo fue diseñado para organizaciones que necesitan un puente práctico entre
No pretende sustituir los requisitos de gobernanza de alto nivel ni el trabajo de ingeniería diario.
Estándares consolidados y arquitecturas de proveedores. En cambio, traduce estos puntos de referencia en
Un modelo operativo centrado en la fiabilidad, la seguridad, la auditabilidad y la inclusión digital.

2. Por qué la gobernanza debería integrar la práctica de la ingeniería.

La gobernanza de TI tradicional a menudo se manifiesta en documentos de política, puntos
Procesos de aprobación formales y revisiones periódicas. Estos instrumentos siguen siendo útiles, pero...
insuficiente en entornos de nube y DevOps, donde la infraestructura puede modificarse.
El acceso se puede delegar rápidamente entre servicios y pueden producirse desviaciones de configuración sin...
visibilidad. Un sistema de gobernanza restringido a documentos tiende a quedar obsoleto en comparación con un sistema que...
debería controlar.
Un modelo operativo que prioriza la gobernanza incorpora la gobernanza en el flujo de trabajo.
Ingeniería. Requiere que los equipos definan arquitecturas de referencia antes de las implementaciones.
hoc, codificar patrones de configuración reproducibles, documentar rutinas de incidentes antes de la
gestionar emergencias e integrar registros, permisos, rutinas de copia de seguridad e historiales de cambios en la superficie.
Práctica de diseño habitual. Esta directriz se enmarca dentro de la tendencia general hacia la seguridad.
Desde la concepción hasta la ingeniería de confiabilidad y el cumplimiento continuo.
Esta necesidad es especialmente evidente en las instituciones con misiones sociales o públicas.
Una organización pequeña puede no describir su trabajo como ingeniería de plataformas, pero
Todavía necesita una gestión de identidades fiable, una disciplina de copias de seguridad, una revisión de accesos y un inventario.
de activos, continuidad de los servicios y capacitación técnica. Cuando estas prácticas están ausentes,
La modernización puede aumentar el riesgo: la institución adquiere nuevas herramientas, pero pierde claridad.
operacional.

3. El modelo de gobernanza priorizada

El modelo propuesto reúne cinco capacidades. Cada una de ellas puede implementarse de forma incremental.

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: 23 de octubre de 2026 | Aceptación: 28 de octubre de 2026 | Publicación: 2 de noviembre de 2026

Pero los resultados más sólidos surgen cuando se refuerzan mutuamente. La línea de base de
La arquitectura define el modelo operativo deseado. La estandarización operativa lo transforma.
Un modelo basado en rutinas reproducibles. La seguridad y la auditabilidad hacen que las decisiones sean rastreables.
La observabilidad y la respuesta ante incidentes garantizan que los fallos puedan detectarse y gestionarse.
La capacitación de la fuerza laboral hace que el modelo sea sostenible al convertir el conocimiento técnico en
capacidad institucional compartida.

Tabla 1 – Capacidades del modelo de gobernanza priorizada para las operaciones institucionales
nube y DevOps

Capacidad	Controles prácticos	Resultado institucional
Línea base arquitectónica	Arquitecturas de referencia, clasificación del entorno, objetivos de copia de seguridad y recuperación, modelo de identidad y responsabilidad del servicio.	Un mapa compartido de la infraestructura digital y la postura de riesgo de la institución.
Estandarización operativa	Directrices operativas, planes de respuesta, estándares de configuración, rutinas de gestión de cambios, inventario de activos y gestión de proveedores y acuerdos de nivel de servicio (SLA).	Menor variabilidad, integración más rápida y menor dependencia del conocimiento no documentado.
Seguridad y auditabilidad	Acceso con privilegios mínimos, revisión periódica del acceso, requisitos de registro, retención de pruebas y correspondencia entre políticas y controles.	Decisiones rastreables y mayor preparación para revisiones internas o externo.
Observabilidad y respuesta ante incidentes	Supervisión, envío de alertas, revisión de registros, niveles de gravedad de los incidentes, revisión posterior al incidente e indicadores de integridad del servicio.	Diagnóstico más rápido, recuperación más disciplinada y aprendizaje a partir de los errores.
Formación de la fuerza laboral	Formación aplicada, hábitos de documentación, iniciativas de inclusión digital y orientación técnica basada en roles.	Operaciones sostenibles y una mayor participación en la transformación digital.

3.1 Línea base de la arquitectura

Una base arquitectónica constituye la representación mínima factible y fiable del entorno.
La infraestructura tecnológica de la institución. Identifica servicios críticos, responsabilidades, dependencias, entornos,
Modelos de acceso, expectativas de recuperación y riesgos conocidos. En entornos de nube, la línea
El marco básico también debe abarcar la estructura de la cuenta o del proyecto, la segmentación de la red y los límites.
identidad, configuración de registro predeterminada, responsabilidades de respaldo y condiciones en

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: 23 de octubre de 2026 | Aceptación: 28 de octubre de 2026 | Publicación: 2 de noviembre de 2026

Los servicios gestionados son preferibles a los componentes gestionados por la propia institución.
La línea base debe ser lo suficientemente simple como para poder mantenerse. Un error común es producir una
El documento arquitectónico es demasiado extenso para actualizarlo. Para instituciones más pequeñas, un
Una arquitectura de referencia compacta, un catálogo de servicios y un registro de decisiones pueden ofrecer
Ofrece un valor práctico mayor que un repositorio de arquitectura completo pero obsoleto.

3.2 Estandarización operativa

La estandarización operativa traduce la arquitectura en prácticas reproducibles. Directrices operativas.
Los manuales de procedimientos y los libros de jugadas son artefactos centrales. Una guía operativa describe
cómo realizar una tarea conocida, cómo integrar un usuario, restaurar una copia de seguridad, renovar una
para acreditar o validar una implementación. Un plan de respuesta describe cómo reaccionar ante una clase de
eventos, como la indisponibilidad del servicio, sospecha de compromiso de la cuenta o problemas con
integridad de los datos.
La estandarización no elimina el juicio profesional. Reduce el número de situaciones en las que...
Es necesario tomar decisiones bajo presión y con información incompleta. Esto también crea una base.
Capacitación para miembros del equipo con menos experiencia, promoviendo la inclusión digital dentro del equipo.
de la propia institución.

3.3 Seguridad y auditabilidad

La seguridad y la auditabilidad deben tratarse como requisitos de ingeniería. Controles de acceso,
Es necesario definir de antemano el registro de eventos, la retención de pruebas y la revisión de la configuración.
que un sistema se vuelve crítico. El Marco de Ciberseguridad 2.0 del NIST destaca la gobernanza como
Una función central que determina cómo se entiende y se gestiona el riesgo de ciberseguridad.
En entornos institucionales, esto significa que los equipos técnicos deben poder explicar que no.
No se trata solo de si existe un control determinado, sino de por qué existe, quién es responsable de él y cómo funciona.
Se conservan pruebas de su funcionamiento.
Los principios de confianza cero son útiles porque promueven la verificación explícita y el principio del mínimo privilegio.
y evaluación continua de las relaciones de confianza. Para las organizaciones más pequeñas, el punto de partida práctico
Puede ser algo sencillo: centralizar la identidad, eliminar las cuentas compartidas y el acceso a los documentos.
Permisos privilegiados y revisarlos periódicamente.

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
PROMAD - Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 23 de octubre de 2026 | Aceptación: 28 de octubre de 2026 | Publicación: 2 de noviembre de 2026

3.4 Observabilidad y respuesta ante incidentes

La observabilidad proporciona las señales necesarias para gestionar la fiabilidad. Monitorización y
El registro de eventos debe estar alineado con la criticidad del servicio. No todos los sistemas lo requieren.
mismo nivel de instrumentación, pero cada servicio crítico debe tener una persona responsable, una definición de
Integridad, expectativas de alerta y un flujo de trabajo de manejo de incidentes. Ingeniería de
La fiabilidad de los sitios web ha popularizado los objetivos de nivel de servicio y los presupuestos de errores como...
formas de conectar el trabajo de ingeniería con la fiabilidad percibida por el usuario. Incluso cuando
Aunque una institución no adopte formalmente la SRE (Evaluación Sistemática de la Fiabilidad), el principio sigue siendo válido: la fiabilidad debe ser...
descrito en términos relevantes para las personas que dependen del servicio.
La revisión posterior al incidente es igualmente importante. Una revisión que priorice la gobernanza no es...
Se limita a la causa técnica. Evalúa si la organización tenía procedimientos de detección adecuados,
documentación, acceso, copia de seguridad, escalabilidad y comunicación. El resultado debería ser un conjunto
Mejoras reducidas cuyo progreso puede ser monitoreado hasta su finalización.

3.5 Formación de la fuerza laboral e inclusión digital

La inclusión digital se suele definir como el acceso a la tecnología por parte de comunidades externas.
Las instituciones también necesitan inclusión digital interna: los empleados y voluntarios deberían
comprender los sistemas que utilizan, los riesgos que gestionan y las rutinas que mantienen los servicios.
Confiable. Por lo tanto, la formación debe estar vinculada a las herramientas operativas. Una guía
El control operacional no es solo una herramienta; también es una herramienta de aprendizaje. Un plan de respuesta.
No es solo una herramienta para gestionar incidentes; también es una forma de distribuir la capacidad.
juicio de toda la organización.
Esta perspectiva es particularmente importante en las organizaciones impulsadas por la misión, en las que la
El trabajo tecnológico a menudo trasciende los límites formales de los títulos de los puestos de trabajo. El objetivo no es...
Transformar a cada parte interesada en un ingeniero. El objetivo es crear un entendimiento común.
suficiente para que las decisiones tecnológicas sean más transparentes, resilientes y estén alineadas con
propósito institucional.

4. PLAN DE IMPLEMENTACIÓN

Las organizaciones pueden adoptar el modelo a través de una hoja de ruta paso a paso. La hoja de ruta es...
intencionalmente ligero, ya que muchas instituciones no pueden interrumpir sus operaciones para realizar

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: 23 de octubre de 2026 | Aceptación: 28 de octubre de 2026 | Publicación: 2 de noviembre de 2026

un amplio programa de transformación.

• Paso 1: Establecer la línea de base. Identificar los servicios críticos, las partes responsables, las dependencias y las cuentas.
recursos privilegiados, rutinas de respaldo y riesgos no resueltos.

• Paso 2: Estandarizar las tareas más frecuentes. Crear guías operativas concisas para la integración de
Usuarios, cambios de acceso, copias de seguridad, comprobaciones de recuperación y mantenimiento rutinario.

• Paso 3: Definir clases de incidentes. Acordar niveles de gravedad, flujos de escalamiento,
Comunicación, recopilación de pruebas y expectativas para las revisiones posteriores a los incidentes.

• Paso 4: Incorporar seguridad y auditabilidad. Asignar políticas a controles, programar revisiones de
Acceder a los registros críticos del sistema, preservarlos y documentar las excepciones.

• Paso 5: Enseñe el modelo operativo. Utilice guías operativas, planes de respuesta y lecciones aprendidas.
Los incidentes sirven como material de capacitación para las partes interesadas, tanto técnicas como no técnicas.

La hoja de ruta debe evaluarse en función de su madurez operativa, no del volumen de documentación.
Entre los indicadores útiles se incluye la capacidad del equipo para identificar a los responsables de los servicios,
restaurar una copia de seguridad crítica, explicar el acceso privilegiado, reproducir una configuración, reenviar
un incidente y empoderar a un nuevo participante sin depender completamente de la memoria informal.

5 RIESGOS Y BENEFICIOS

El modelo que prioriza la gobernanza implica concesiones. Una estandarización excesiva puede...
Retrasar la experimentación. Una estandarización insuficiente puede hacer que los sistemas sean frágiles. Equilibrio
La idoneidad depende del riesgo institucional, la criticidad de los servicios y la madurez del equipo.
Una regla útil es estandarizar los puntos donde una falla causaría daño institucional y preservar el
Flexibilidad donde el aprendizaje es el objetivo principal.
Otro riesgo es la gobernanza puramente performativa: producir documentos que cumplan con una lista de verificación.
Verificación de auditoría, pero no influye en las operaciones. Este riesgo puede reducirse.
vincular cada artefacto de gobernanza a una rutina operativa. Una política debe corresponder a
un control; un control debe corresponder a la evidencia; y la evidencia debe poder ser verificada.
recuperado por las personas responsables del servicio.

6. CONCLUSIÓN

Las prácticas de Cloud y DevOps pueden ayudar a las organizaciones orientadas a la misión a modernizar sus
Infraestructura, pero la modernización sin gobernanza puede aumentar la fragilidad. Un modelo
Gobernanza operativa, con énfasis en la confiabilidad, la seguridad, la auditabilidad 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: 23 de octubre de 2026 | Aceptación: 28 de octubre de 2026 | Publicación: 2 de noviembre de 2026

Transferencia de conocimiento como responsabilidad de ingeniería. Al incorporar la gobernanza en arquitecturas de referencia, guías operativas, planes de respuesta, rutinas de acceso, observabilidad

Con capacitación y desarrollo de capacidades, las instituciones pueden crear una infraestructura digital que no solo sea moderna, sino también

Comprensible y fiable.

El modelo presentado es intencionalmente práctico. Su valor no reside en añadir otra [característica/función].

no solo una capa de terminología, sino que ayuda a las instituciones a desarrollar hábitos reproducibles que

Proteger la continuidad y ampliar la participación en la transformación digital.

EXPRESIONES DE GRATITUD

El autor utilizó OpenAI ChatGPT como apoyo en la redacción, el refinamiento estructural y...

Organización editorial. El autor ha revisado y corregido el manuscrito y asume la responsabilidad de su

Contenido final. El artículo no incluye figuras, imágenes ni datos experimentales generados por inteligencia artificial.

artificial.

REFERENCIAS

[1] IEEE Computer Society, “Información del autor: Profesional de TI”. [En línea]. Disponible en: https://www.computer.org/csdl/magazine/it/write-for-us

[2] Instituto Nacional de Estándares y Tecnología, “El Marco de Ciberseguridad (CSF) del NIST” 2.0”, NIST, febrero de 2024. [En línea]. Disponible en: https://www.nist.gov/cyberframework

[3] S. Rose, O. Borchert, S. Mitchell y S. Connelly, «Zero Trust Architecture», Publicación especial 800-207 del NIST, agosto de 2020. [En línea]. Disponible en: https://doi.org/10.6028/NIST.SP.800-207

[4] B. Beyer, C. Jones, J. Petoff y NR Murphy, Ingeniería de confiabilidad de sitios: Cómo Google gestiona los sistemas de producción. Sebastopol, CA, EE. UU.: O'Reilly Media, 2016. [En línea]. Disponible en: https://sre.google/sre-book/table-of-contents/

[5] AWS, “Marco de arquitectura bien diseñada de AWS”. [En línea]. https:// Disponible en: docs.aws.amazon.com/wellarchitected/latest/framework/welcome.html

[6] Google Cloud, “DORA: Investigación y evaluación de DevOps”. [En línea]. Disponible en: https://dora.dev/

[7] Cloud Security Alliance, “Matriz de controles en la nube”. [En línea]. Disponible en: https://cloudsecurityalliance.org/research/cloud-controls-matrix

[8] IEEE, “Políticas de envío y revisión por pares de IEEE”. [En línea]. Disponible en: https://journals.ieeeauthorcenter.ieee.org/submit-your-article-for-peer-review/ieee-submission-and-peer-review-policies/

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.