RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

El framework Agility de transformación tecnológica regulada: una metodología basada en riesgos para la gobernanza tecnológica, la modernización de sistemas, la seguridad de los datos y la resiliencia operativa en instituciones financieras reguladas

O framework Agility de transformação tecnológica regulada: uma metodologia baseada em risco para governança de tecnologia, modernização de sistemas, segurança de dados e resiliência operacional em instituições financeiras reguladas

The Agility Regulated Technology Transformation Framework: a risk-based methodology for technology governance, systems modernization, data security, and operational resilience in regulated financial institutions

Antonio Garcia Junior
Agility Digital Technologies, LLC., Florida, Estados Unidos
Autor de correspondencia: tony@agilitydigital.net
Breve biografía: fundador y propietario de Agility Digital Technologies, LLC., con experiencia profesional en liderazgo de tecnología financiera, modernización, gobernanza, arquitectura, datos, riesgo y resiliencia operativa en entornos bancarios regulados.

Resumen:
Las instituciones financieras afrontan cada vez más el desafío de modernizar entornos tecnológicos heredados mientras mantienen una gobernanza eficaz, ciberseguridad, protección de datos, preparación regulatoria y resiliencia operativa. Los bancos pequeños y medianos, cooperativas de crédito, empresas fintech, organizaciones de pagos y otras entidades financieras reguladas pueden enfrentar restricciones particulares porque deben responder a expectativas tecnológicas y de supervisión complejas con recursos internos comparativamente limitados. Este artículo propone el Agility Regulated Technology Transformation Framework (ARTTF), una metodología estructurada, repetible, basada en riesgos y desarrollada internamente para ayudar a las organizaciones financieras reguladas a evaluar la madurez tecnológica, identificar riesgos materiales, priorizar la remediación y desarrollar hojas de ruta prácticas de modernización. El framework integra seis dominios de evaluación: gobernanza tecnológica y responsabilidad ejecutiva; sistemas heredados y arquitectura tecnológica; gobernanza de datos, identidad y gestión de accesos; riesgo de nube, proveedores y terceros; ciberseguridad, continuidad del negocio y recuperación; y auditabilidad, preparación regulatoria y gobernanza de la remediación. La metodología combina un modelo de madurez de cinco niveles, un instrumento diagnóstico de 30 preguntas, priorización cualitativa de riesgos, medidas para un panel ejecutivo y planificación de remediación por fases. Su diseño se basa en la ciencia del diseño de sistemas de información, la literatura de transformación digital y orientaciones reconocidas del sector financiero y la ciberseguridad de Estados Unidos. Un escenario ilustrativo de banco comunitario demuestra cómo el framework puede convertir inquietudes tecnológicas fragmentadas en un programa priorizado de gobernanza y modernización, sin sustituir requisitos jurídicos, regulatorios, de auditoría o supervisión específicos de cada institución.

Palabras clave:
Gobernanza de TI. Modernización de sistemas. Seguridad de datos. Resiliencia operativa. Instituciones financieras.

Resumo:
Instituições financeiras enfrentam, de forma crescente, o desafio de modernizar ambientes tecnológicos legados ao mesmo tempo em que preservam governança efetiva, cibersegurança, proteção de dados, preparação regulatória e resiliência operacional. Bancos de pequeno e

médio porte, cooperativas de crédito, fintechs, empresas de pagamentos e outras organizações financeiras reguladas podem enfrentar restrições específicas, pois precisam responder a expectativas tecnológicas e de supervisão complexas com recursos internos comparativamente limitados. Este artigo propõe o Agility Regulated Technology Transformation Framework (ARTTF), uma metodologia baseada em risco, estruturada, repetível e desenvolvida internamente para apoiar organizações financeiras reguladas na avaliação da maturidade tecnológica, identificação de riscos materiais, priorização de remediações e desenvolvimento de roteiros práticos de modernização. O framework integra seis domínios: governança de tecnologia e responsabilidade executiva; sistemas legados e arquitetura tecnológica; governança de dados, identidade e controle de acesso; riscos de nuvem, fornecedores e terceiros; cibersegurança, continuidade de negócios e recuperação; e auditabilidade, preparação regulatória e governança de remediações. A metodologia combina modelo de maturidade de cinco níveis, instrumento diagnóstico com 30 perguntas, priorização qualitativa de riscos, indicadores para dashboard executivo e planejamento de remediação por fases. Seu desenho se baseia em design science de sistemas de informação, literatura de transformação digital e orientações reconhecidas do setor financeiro e de cibersegurança dos Estados Unidos. Um cenário ilustrativo de banco comunitário demonstra como o framework pode converter preocupações tecnológicas fragmentadas em um programa priorizado de governança e modernização, sem substituir requisitos legais, regulatórios, de auditoria ou de supervisão específicos de cada instituição.

Palavras-chave:
Governança de TI. Modernização de sistemas. Segurança de dados. Resiliência operacional. Instituições financeiras.

Abstract:
Financial institutions increasingly face the challenge of modernizing legacy technology environments while maintaining effective governance, cybersecurity, data protection, regulatory readiness, and operational resilience. Smaller and mid-sized banks, credit unions, fintech companies, payment organizations, and other regulated financial entities may face particular constraints because they must address complex technology and supervisory expectations with comparatively limited internal resources. This paper proposes the Agility Regulated Technology Transformation Framework (ARTTF), an internally developed, structured, and repeatable risk-based methodology designed to help regulated financial organizations assess technology maturity, identify material risks, prioritize remediation, and develop practical modernization roadmaps. The framework integrates six assessment domains: technology governance and executive accountability; legacy systems and technology architecture; data governance, identity, and access management; cloud, vendor, and third-party risk; cybersecurity, business continuity, and recovery; and auditability, regulatory readiness, and remediation governance. The methodology combines a five-level maturity model, a 30-question diagnostic instrument, qualitative risk prioritization, executive dashboard measures, and phased remediation planning. Its design draws on information-systems design science, digital-transformation literature, and recognized U.S. financial-sector and cybersecurity guidance, including NIST CSF 2.0 and FFIEC guidance. An illustrative community-bank scenario demonstrates how the framework can convert fragmented technology concerns into a prioritized governance and modernization program. The framework is intended as a practical management methodology and does not replace institution-specific legal, regulatory, audit, or supervisory requirements.

Keywords:

IT governance. Systems modernization. Data security. Operational resilience. Financial institutions.

1. Introducción

La modernización tecnológica en los servicios financieros no es un ejercicio puramente técnico. Cambia la forma en que las instituciones ofrecen productos, gestionan riesgos, protegen datos, interactúan con clientes, dependen de terceros y demuestran la eficacia de los controles ante consejos, auditores y supervisores. La investigación sobre transformación digital también destaca que una transformación significativa exige cambios en las estructuras, procesos, capacidades y gobernanza de la organización, además de la adopción de nuevas tecnologías (Vial, 2019). En entornos financieros regulados, este desafío más amplio se intensifica por los requisitos de seguridad y solidez, seguridad de la información, resiliencia, protección de datos, supervisión de terceros y responsabilidad de gestión auditable.

El desafío es especialmente visible en las instituciones financieras pequeñas y medianas. Los bancos comunitarios y las cooperativas de crédito pueden operar servicios críticos de pagos, préstamos, depósitos e información de clientes con equipos de tecnología y riesgo comparativamente pequeños. Las fintech y las empresas de pagos pueden crecer rápidamente mientras se vuelven más dependientes de proveedores de nube, socios bancarios, API, plataformas de datos y servicios tecnológicos externalizados. En ambos casos, las iniciativas de modernización solo pueden crear valor cuando la institución logra identificar qué riesgos son materiales, establecer responsabilidades claras, secuenciar la remediación y preservar la continuidad durante el cambio.

Las orientaciones del sector financiero de Estados Unidos tratan cada vez más la gobernanza tecnológica, la arquitectura, la ciberseguridad, la resiliencia operativa, la autenticación y la gestión de terceros como responsabilidades de gestión interconectadas. El manual Architecture, Infrastructure, and Operations del FFIEC destaca la planificación de arquitectura e infraestructura, la gobernanza y gestión de riesgos y el control operativo de activos, procesos y terceros interconectados (Federal Financial Institutions Examination Council [FFIEC], 2021a). El manual Business Continuity Management del FFIEC encuadra la continuidad como una disciplina de gestión de riesgos en toda la empresa que abarca tecnología, operaciones, pruebas, comunicación y resiliencia de los servicios críticos (FFIEC, 2019). Las orientaciones interinstitucionales sobre terceros señalan además que el uso de terceros no elimina la responsabilidad de una organización bancaria de operar de forma

segura, sólida y conforme con los requisitos aplicables (Federal Deposit Insurance Corporation [FDIC] et al., 2023).

Por lo tanto, es significativa la necesidad de un mecanismo práctico de integración. Las instituciones suelen mantener inventarios separados de hallazgos de auditoría, riesgos de ciberseguridad, deuda arquitectónica, problemas de calidad de datos, inquietudes sobre proveedores, brechas de recuperación ante desastres y medidas regulatorias. Cuando estos artefactos se gestionan de forma aislada, los líderes pueden carecer de una visión consolidada de cómo interactúan las debilidades tecnológicas o de qué acciones deben priorizarse. Un programa retrasado de gobernanza de identidades, por ejemplo, puede afectar simultáneamente la ciberseguridad, la preparación para auditorías, el acceso de terceros, la protección de datos y la contención de incidentes. Una plataforma de middleware sin soporte puede crear al mismo tiempo riesgos operativos, de seguridad, de integración y de continuidad.

Este artículo presenta el Agility Regulated Technology Transformation Framework (ARTTF) como método práctico para convertir estas inquietudes fragmentadas en un programa estructurado de transformación. El framework está dirigido a bancos comunitarios, bancos pequeños y medianos, cooperativas de crédito, empresas fintech, organizaciones de pagos, proveedores de Banking-as-a-Service y otras organizaciones financieras reguladas o intensivas en datos. Está diseñado para apoyar a patrocinadores ejecutivos, líderes tecnológicos, profesionales de riesgo y cumplimiento, partes interesadas de auditoría interna, gerentes de programas y equipos de arquitectura en el establecimiento de una base factual común, la evaluación de la madurez, la priorización de riesgos y la construcción de una hoja de ruta viable.

El artículo ofrece cuatro contribuciones prácticas. En primer lugar, define seis dominios integrados de evaluación que conectan gobernanza, arquitectura, datos, riesgo de terceros, ciberseguridad, resiliencia y preparación regulatoria. En segundo lugar, presenta un modelo de madurez de cinco niveles y un instrumento diagnóstico de 30 preguntas que pueden utilizarse para una evaluación inicial y el debate ejecutivo. En tercer lugar, define un enfoque de mapa de calor de riesgos con reglas explícitas de escalamiento cualitativo para que una puntuación simple no sustituya el juicio profesional. En cuarto lugar, ofrece un modelo de panel ejecutivo y una estructura de hoja de ruta por fases de 0-90 días, 3-12 meses y 12-24 meses para convertir los hallazgos de la evaluación en una ejecución gobernada. Un caso ilustrativo demuestra la mecánica del enfoque sin utilizar datos confidenciales de clientes.

2. Fundamentos teóricos y regulatorios

2.1 Transformación digital como proceso organizacional y de gestión de riesgos

La transformación digital suele describirse como cambio organizacional posibilitado por combinaciones de tecnologías de información, computación, comunicación y conectividad. Vial (2019) muestra que la transformación digital afecta la creación de valor y exige que las organizaciones aborden cambios estructurales y barreras para la ejecución. En una institución financiera, estas barreras aparecen con frecuencia como aplicaciones heredadas, integración fragmentada, derechos de decisión poco claros, propiedad de datos inconsistente, dependencias de proveedores, controles manuales, observabilidad insuficiente o prioridades empresariales y regulatorias contrapuestas.

Esta perspectiva es importante porque una hoja de ruta de modernización enfocada únicamente en sustituir tecnología puede no abordar el modelo operativo que creó el riesgo. La migración de un sistema central puede dejar sin resolver la propiedad de datos, debilidades de acceso privilegiado, concentración de proveedores o una gobernanza de cambios ineficaz. A la inversa, una iniciativa de gobernanza que no aborde sistemas obsoletos y restricciones arquitectónicas puede producir documentación más sólida sin reducir la fragilidad operativa. Por eso, el ARTTF trata la transformación tecnológica como un problema combinado de gobernanza, arquitectura, datos, seguridad, resiliencia y ejecución.

2.2 Integración de gobernanza, ciberseguridad y riesgo empresarial

El NIST Cybersecurity Framework (CSF) 2.0 ofrece una taxonomía de alto nivel que organizaciones de diferentes tamaños y niveles de madurez pueden utilizar para comprender, evaluar, priorizar y comunicar resultados de ciberseguridad (Pascoe et al., 2024). La versión 2.0 añadió la función Govern y aumentó el énfasis en la gobernanza y el riesgo de la cadena de suministro, reforzando la necesidad de conectar la ciberseguridad con la toma de decisiones empresariales, en vez de tratarla como un programa técnico aislado. El NIST también destaca que el CSF describe resultados y no prescribe un único método de implementación, lo que permite a las organizaciones adaptar su aplicación a su perfil de riesgo.

Las orientaciones del NIST sobre los Tiers del CSF pueden utilizarse para caracterizar el rigor de los procesos de gobernanza y gestión del riesgo de ciberseguridad y proporcionar contexto para la mejora (Quinn et al., 2024). El modelo de madurez de cinco niveles del ARTTF no es una reformulación de los cuatro Tiers del NIST CSF. Es una escala diagnóstica

desarrollada internamente para respaldar una evaluación más amplia de la transformación tecnológica en seis dominios. Los resultados y Tiers del NIST CSF pueden utilizarse como referencias informativas en las partes de la evaluación relacionadas con la ciberseguridad, mientras que la puntuación de madurez del ARTTF ofrece una visión de gestión entre dominios.

2.3 Arquitectura, tecnología heredada y dependencia operativa

Las orientaciones Architecture, Infrastructure, and Operations del FFIEC reconocen que la arquitectura tecnológica, la infraestructura y las operaciones están interconectadas con activos, procesos y proveedores externos de servicios (FFIEC, 2021a). Para las instituciones reguladas, las decisiones de arquitectura influyen en la disponibilidad, seguridad, escalabilidad, dependencia de proveedores, movimiento de datos, complejidad del cambio y prestación de productos y servicios financieros críticos. Esto convierte la revisión de arquitectura en una actividad de gestión de riesgos además de una actividad de diseño.

Por lo tanto, la tecnología heredada no debe evaluarse simplemente por su antigüedad, sino también por la criticidad para el negocio, capacidad de soporte, exposición de seguridad, complejidad de integración, recuperabilidad, concentración de conocimiento, riesgo de falla en cambios y dependencia de componentes obsoletos. El framework utiliza estos factores para identificar prioridades de modernización y distinguir entre tecnología que puede estabilizarse, tecnología que debe desacoplarse progresivamente y tecnología que requiere sustitución planificada.

2.4 Gobernanza de datos, identidad y gestión de accesos

La gobernanza de datos determina qué decisiones deben tomarse sobre los datos y quién responde por ellas. Khatri y Brown (2010) distinguen la gobernanza de la gestión cotidiana y destacan los derechos de decisión y la responsabilidad en los distintos dominios de datos. En los servicios financieros, estas cuestiones están directamente relacionadas con la confiabilidad de los informes, la protección de datos de clientes, los controles de fraude, el riesgo de modelos, la analítica, la preparación para la IA y la evidencia regulatoria.

La gestión de identidades y accesos es igualmente transversal. Las orientaciones de autenticación de 2021 del FFIEC destacan la evaluación de riesgos, la seguridad en capas y prácticas de autenticación más sólidas para clientes, empleados y terceros que acceden a sistemas y servicios (FFIEC, 2021b). Por esta razón, el framework evalúa la gobernanza de accesos junto con la clasificación de datos, el acceso privilegiado, la segregación de

funciones, los procesos de incorporación-movilidad-salida y la revisión periódica de derechos, en lugar de tratar la autenticación como un control aislado.

2.5 Nube, proveedores y riesgo de terceros

La modernización depende cada vez más de proveedores externos de tecnología, plataformas de nube, productos de software como servicio, socios fintech y proveedores especializados. Las orientaciones interinstitucionales de 2023 sobre terceros establecen un enfoque de ciclo de vida basado en riesgos que abarca planificación, debida diligencia y selección, negociación contractual, seguimiento continuo y terminación (FDIC et al., 2023). Las orientaciones también dejan claro que la organización bancaria conserva la responsabilidad de operar de manera segura y sólida cuando utiliza terceros.

La adopción de la nube plantea consideraciones adicionales sobre responsabilidad compartida, concentración, transparencia arquitectónica, planificación de salida, ubicación de datos, identidad, seguimiento, resiliencia y acceso contractual a pruebas. El Tesoro de Estados Unidos y el Financial Services Sector Coordinating Council publicaron recursos destinados a respaldar la adopción segura de la nube y abordar inquietudes sobre terceros, externalización, resiliencia y transparencia para instituciones financieras de diferentes tamaños (U.S. Department of the Treasury, 2024b). Por eso, el ARTTF incorpora la gobernanza de la nube y de terceros a la misma evaluación utilizada para arquitectura y resiliencia operativa.

2.6 Ciberseguridad, continuidad del negocio y resiliencia operativa

El concepto de resiliencia va más allá de la recuperación ante desastres. Las orientaciones del FFIEC destacan prácticas de continuidad en toda la empresa que abarcan tecnología, operaciones, pruebas y comunicaciones, así como el mantenimiento continuo de los sistemas y controles necesarios para sostener servicios críticos (FFIEC, 2019). El informe Cybersecurity and Financial System Resilience de 2026 del OCC describe la ciberseguridad, la resiliencia operativa y el riesgo de terceros como prioridades permanentes de supervisión en el sistema bancario federal (Office of the Comptroller of the Currency [OCC], 2026). La NCUA destaca de forma similar exámenes dirigidos, evaluaciones de riesgos, preparación y resiliencia del sistema en el sector de cooperativas de crédito (National Credit Union Administration [NCUA], 2026).

En el ARTTF, la resiliencia se evalúa mediante la criticidad de los servicios, objetivos de recuperación, mapeo de dependencias, pruebas de copia de seguridad y restauración, preparación para incidentes, gobernanza de crisis, seguimiento, redundancia arquitectónica,

dependencias de recuperación de proveedores y capacidad de la organización para mantener o restaurar servicios financieros críticos. Esta visión más amplia reduce el riesgo de confundir un programa de copias de seguridad técnicamente exitoso con la resiliencia operativa.

2.7 Tecnología emergente y preparación para la IA

La analítica avanzada y la inteligencia artificial pueden aumentar la eficiencia y el apoyo a las decisiones, pero también amplifican la importancia de la calidad de los datos, la explicabilidad, la seguridad, la gobernanza de terceros y la responsabilidad de la gestión. El AI Risk Management Framework del NIST ofrece una estructura voluntaria para gestionar los riesgos que los sistemas de IA generan para las organizaciones y la sociedad (Tabassi, 2023). El trabajo del Tesoro para el sector financiero identifica privacidad de datos, dependencias de terceros, ciberseguridad, sesgos, gobernanza y cumplimiento como consideraciones relevantes en la adopción de IA en servicios financieros (U.S. Department of the Treasury, 2024a). El Financial Stability Board también identifica dependencias de terceros, riesgo cibernético, riesgo de modelos, calidad de datos y gobernanza entre las vulnerabilidades importantes relacionadas con la IA en las finanzas (Financial Stability Board [FSB], 2024).

El ARTTF no es un framework de gobernanza de IA. En cambio, trata la preparación para la IA como resultado de capacidades fundamentales más sólidas: gobernanza responsable, datos confiables, acceso controlado, arquitectura segura, supervisión eficaz de terceros, cambios auditables y operaciones resilientes. Las instituciones pueden ampliar el instrumento diagnóstico con preguntas específicas sobre IA cuando los casos de uso de analítica avanzada o IA sean materiales para el alcance.

3. Metodología

3.1 Orientación aplicada de ciencia del diseño

El framework se desarrolló como un artefacto metodológico orientado a la práctica. La ciencia del diseño en sistemas de información se centra en la creación y aplicación de artefactos destinados a mejorar las capacidades humanas y organizacionales en un dominio de problema definido (Hevner et al., 2004). Peffers et al. (2007) describen un proceso de investigación en ciencia del diseño que incluye identificación del problema, definición de objetivos, diseño y desarrollo, demostración, evaluación y comunicación. El desarrollo del ARTTF sigue esta lógica en un nivel aplicado: identifica un problema de gestión recurrente en la transformación tecnológica regulada, especifica las capacidades necesarias para abordarlo,

diseña un artefacto repetible de evaluación y priorización, demuestra su uso mediante un caso ilustrativo y comunica limitaciones y oportunidades para una futura evaluación empírica.

La metodología combina tres fuentes de conocimiento. La primera son orientaciones públicas reconocidas de reguladores financieros y organismos de normalización de Estados Unidos, utilizadas para identificar temas recurrentes de gobernanza, arquitectura, ciberseguridad, resiliencia, datos, acceso y terceros. La segunda es la literatura de sistemas de información sobre transformación digital, gobernanza de datos y ciencia del diseño. La tercera es la experiencia profesional del autor en liderazgo de tecnología financiera, modernización, gobernanza, arquitectura, datos, riesgo e iniciativas de resiliencia operativa en entornos bancarios regulados. El framework no reproduce un programa de examen, una tarjeta de puntuación ni un catálogo propietario de controles de un regulador. Traduce principios recurrentes en una secuencia orientada a la gestión para la evaluación y planificación de la transformación.

Este artículo no afirma una validación empírica en una muestra estadísticamente representativa de instituciones. El caso ilustrativo de la Sección 9 es hipotético y se utiliza únicamente para demostrar la mecánica de puntuación, priorización, informes ejecutivos y desarrollo de la hoja de ruta. Las investigaciones futuras deben evaluar la consistencia entre evaluadores, la validez predictiva y los resultados prácticos en instituciones de diferentes tipos y tamaños.

3.2 Principios de diseño

Tabla 1. Principios de diseño del Agility Regulated Technology Transformation Framework

Principio de diseño	Significado operativo
Basado en riesgos, no orientado por listas de comprobación	La profundidad de la evaluación y la prioridad de remediación deben reflejar la criticidad empresarial, relevancia regulatoria, impacto sobre clientes y datos, exposición y dependencia operativa.
Responsabilidad ejecutiva	Todo hallazgo material debe tener un responsable, una vía de decisión, una fecha objetivo y un mecanismo de escalamiento.
Orientación por pruebas	Las conclusiones deben poder rastrearse hasta documentos, entrevistas, inventarios, configuraciones, métricas, pruebas de ensayos u otros artefactos de revisión.
Integración entre dominios	Un hallazgo puede afectar varios dominios; la metodología debe evitar puntuaciones aisladas que oculten riesgos interconectados.
Proporcionalidad	La profundidad de la evaluación debe reflejar el tamaño, complejidad, productos, modelo tecnológico, dependencia de terceros y perfil de riesgo de la institución.
Modernización con resiliencia	Los cambios en el estado objetivo deben mejorar la escalabilidad y eficiencia sin debilitar seguridad, continuidad, auditabilidad o control.

Principio de diseño	Significado operativo
Capacidad de acción	La evaluación debe concluir con acciones priorizadas, secuenciación, dependencias, responsables y decisiones ejecutivas, no con una lista estática de observaciones.
Repetibilidad	Los dominios principales, preguntas, definiciones de puntuación y estructuras de reporte deben ser suficientemente consistentes para respaldar la reevaluación y el análisis de tendencias.

Nota. Los principios pretenden orientar el juicio profesional; no sustituyen los requisitos legales o de supervisión específicos de cada institución.

3.3 Alcance y uso previsto

El framework está diseñado para diagnósticos iniciales, revisiones de preparación regulatoria, evaluaciones de modernización, programas de mejora de la gobernanza, debida diligencia, planificación de remediación y gobernanza de la transformación. Puede utilizarse como una evaluación empresarial completa o limitarse a un subconjunto de dominios, unidades de negocio, plataformas o servicios críticos. Una evaluación completa debe establecer los límites del alcance, sistemas y servicios materiales, terceros clave, datos críticos, contexto regulatorio y principales iniciativas de transformación antes de comenzar la puntuación.

Los usuarios previstos incluyen CIO, CTO, CISO, CRO, líderes de riesgo tecnológico, responsables de cumplimiento, líderes de datos, arquitectos empresariales, líderes de programas, partes interesadas de auditoría interna y asesores externos. El framework no pretende crear una certificación, calificación regulatoria o conclusión jurídica. Una puntuación de madurez de 4 o 5 no establece el cumplimiento, y una puntuación más baja no establece por sí sola una infracción regulatoria. La puntuación es una herramienta de gestión para priorización y diálogo.

4. El Agility Regulated Technology Transformation Framework

4.1 Ciclo de ejecución en seis fases

Tabla 2. Ciclo de seis fases del ARTTF

Fase	Objetivo principal	Resultados representativos
Fase 1 - Alineación ejecutiva y confirmación del alcance	Definir contexto empresarial, impulsores regulatorios, alcance, servicios críticos, partes interesadas, criterios de éxito, cronograma y gobernanza.	Acta del trabajo; declaración de alcance; mapa de partes interesadas; lista de documentos solicitados; hipótesis iniciales de riesgo.
Fase 2 - Descubrimiento del estado actual y recopilación de pruebas	Revisar gobernanza, arquitectura, aplicaciones, infraestructura, nube, proveedores, datos, controles, continuidad, hallazgos de auditoría, prácticas de cambio e informes.	Evaluación del estado actual; inventario; registro de pruebas; mapa de dependencias; registro preliminar de riesgos.

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

Fase	Objetivo principal	Resultados representativos
Fase 3 - Evaluación de brechas basada en riesgos y evaluación de madurez	Evaluar prácticas actuales frente a las orientaciones seleccionadas, requisitos empresariales, apetito de riesgo y resultados objetivo; identificar causas raíz y brechas interconectadas.	Puntuaciones de madurez; matriz de brechas; mapa de calor de riesgos; registro de problemas; observaciones ejecutivas.
Fase 4 - Diseño del estado objetivo y hoja de ruta de modernización	Traducir los hallazgos en modelos operativos objetivo, gobernanza, arquitectura, mejoras de controles, secuenciación y prioridades de inversión.	Modelo de estado objetivo; plano de arquitectura; RACI; plan de controles; hoja de ruta de modernización; resumen del impacto empresarial.
Fase 5 - Apoyo dirigido a la implementación	Proporcionar apoyo de gobernanza e implementación sin operar como empresa de dotación de personal, MSP, proveedor de pruebas de penetración o proveedor continuo de operaciones de seguridad.	Plan de implementación; panel de gobernanza; rastreador de proveedores; registro de problemas/riesgos; pruebas de controles; procedimientos actualizados.
Fase 6 - Informes ejecutivos, pruebas de auditoría y mejora continua	Establecer informes sostenibles, métricas, rutinas de gobernanza, pruebas, reevaluación y lecciones aprendidas.	Informe ejecutivo; paquete para el consejo; pruebas de auditoría; panel de remediación; cartera de mejoras; línea de base de reevaluación.

4.2 Seis dominios integrados de evaluación

Tabla 3. Dominios integrados de evaluación

ID	Dominio	Alcance	Principales familias de referencia
D1	Gobernanza tecnológica y responsabilidad ejecutiva	Derechos de decisión, responsabilidad, propiedad de riesgos, políticas, foros de gobernanza, alineación estratégica, informes ejecutivos y al consejo, apetito de riesgo y supervisión de la gestión.	Función Govern del NIST CSF 2.0; conceptos de gestión/AIO del FFIEC; gobernanza de riesgos empresariales.
D2	Sistemas heredados y arquitectura tecnológica	Ciclo de vida de aplicaciones e infraestructura, arquitectura objetivo, deuda técnica, integraciones, API, dependencias en nube y locales, escalabilidad, observabilidad, complejidad de cambios y secuenciación de la modernización.	FFIEC Architecture, Infrastructure, and Operations; literatura de transformación digital.
D3	Gobernanza de datos, identidad y gestión de accesos	Propiedad, clasificación, calidad y linaje de datos, gobernanza de accesos, acceso privilegiado, procesos de incorporación-movilidad-salida, segregación de funciones y confiabilidad de informes.	Literatura de gobernanza de datos; orientaciones del FFIEC sobre autenticación y acceso; resultados del NIST.
D4	Nube, proveedores y riesgo de terceros	Inventario y clasificación por riesgo de terceros, debida diligencia, contratación, SLA, seguimiento continuo, concentración, responsabilidad compartida en la nube, cuartas partes, resiliencia y planificación de salida.	Orientaciones interinstitucionales de 2023 sobre terceros; recursos del Tesoro sobre la nube; gobernanza de la cadena de suministro del NIST.
D5	Ciberseguridad, continuidad del negocio y recuperación	Gobernanza de seguridad, gestión de vulnerabilidades, seguimiento, respuesta a incidentes, copias de seguridad, pruebas de recuperación, RTO/RPO, gestión de crisis, continuidad de servicios críticos y dependencias de resiliencia.	NIST CSF 2.0; FFIEC Business Continuity Management; prioridades de resiliencia del OCC y la NCUA.
D6	Auditabilidad, preparación regulatoria y gobernanza de la remediación	Mapeo de controles, pruebas, hallazgos de auditoría y exámenes, seguimiento de cambios regulatorios, adhesión a políticas, propiedad de problemas, validación de remediación, informes y gobernanza del cierre.	Temas de supervisión del FFIEC/OCC; gobernanza del NIST; prácticas de control interno y pruebas.

4.3 Modelo de madurez de cinco niveles

El modelo de madurez proporciona un lenguaje común para describir la institucionalización de las prácticas. Evalúa si las responsabilidades y controles son informales o repetibles, si están documentados y se ejecutan de forma consistente, si la gestión mide desempeño y riesgo y si la organización estableció mejora continua y resiliencia. La escala es intencionalmente lo bastante amplia para aplicarse a los seis dominios, al tiempo que permite que las pruebas específicas de cada dominio determinen la puntuación.

Una puntuación de madurez solo debe asignarse después de revisar pruebas adecuadas al alcance. Las respuestas de entrevistas por sí solas no deben respaldar una puntuación alta cuando la documentación, las pruebas operativas, los ensayos, las métricas o el historial de problemas contradigan la práctica declarada. Asimismo, la ausencia de un documento formal no debe imponer automáticamente una puntuación baja si la organización puede demostrar un mecanismo equivalente, controlado y repetible.

Tabla 4. Escala de madurez del ARTTF

Nivel	Clasificación	Definición	Características típicas
1	Reactivo	Las prácticas son informales, fragmentadas, dependientes de personas o principalmente impulsadas por eventos. La responsabilidad y las pruebas son limitadas.	Alta variabilidad; pueden desconocerse brechas materiales; la remediación es principalmente reactiva.
2	En desarrollo	Existen controles y responsabilidades básicos, pero la ejecución es inconsistente entre equipos, sistemas o períodos.	Visibilidad parcial; excepciones recurrentes; métricas limitadas; pruebas inconsistentes.
3	Definido	Las prácticas están documentadas, asignadas, estandarizadas y son generalmente repetibles dentro del alcance definido.	Las funciones y procesos son claros; hay pruebas disponibles; las excepciones se gestionan.
4	Gestionado	Las prácticas se miden, se basan en riesgos, se supervisan y se integran en la gobernanza y los informes de gestión.	Se establecen métricas, umbrales, pruebas, análisis de tendencias y remediación responsable.
5	Optimizado / Resiliente	Las prácticas están integradas, son adaptables, mejoran continuamente y demuestran resiliencia bajo condiciones cambiantes.	Aprendizaje continuo; automatización cuando corresponde; pruebas de escenarios; respuesta rápida; optimización estratégica.

Nota. Este modelo de madurez de cinco niveles es una escala diagnóstica del ARTTF y no debe presentarse como equivalente al modelo de cuatro Tiers del NIST CSF.

4.4 Lógica de puntuación de la madurez

Cada pregunta diagnóstica se puntúa de 1 a 5 según las definiciones de la Tabla 4. La puntuación de un dominio es la media aritmética de las cinco preguntas asignadas a ese dominio. La puntuación general predeterminada de madurez es la media de las puntuaciones de los seis dominios. La ponderación igual es adecuada para un diagnóstico empresarial inicial porque evita crear una apariencia de precisión antes de que la institución establezca su

perfil de riesgo. Las organizaciones pueden adoptar ponderaciones basadas en riesgos cuando exista una justificación documentada; por ejemplo, una organización de pagos puede ponderar más la resiliencia cibernética y la dependencia de terceros, mientras que una institución inmersa en un gran programa de modernización del sistema central puede dar mayor énfasis a arquitectura y datos.

La puntuación debe ir acompañada de un indicador de confianza de las pruebas, como Alta, Media o Baja. Una puntuación basada en políticas, pruebas del sistema, métricas, resultados de pruebas e historial de problemas debe tener mayor confianza que una basada principalmente en entrevistas. Cuando las pruebas sean contradictorias, el evaluador debe registrar la contradicción y utilizar la puntuación inferior respaldada hasta que se resuelva la discrepancia.

5. Instrumento diagnóstico de 30 preguntas

5.1 Cuestionario principal

El diagnóstico principal contiene cinco preguntas para cada uno de los seis dominios. El instrumento está destinado a entrevistas estructuradas y revisión de pruebas, no a una lista de autocertificación. Cada pregunta debe estar respaldada por una breve nota de evidencia, una puntuación de madurez de 1 a 5 y cualquier observación de riesgo resultante. Las preguntas pueden complementarse según los productos institucionales, el perímetro regulatorio, los servicios críticos, los proveedores materiales y los programas activos de transformación.

Tabla 5. Diagnóstico principal de 30 preguntas del ARTTF

N.º	Dominio	Pregunta diagnóstica	Puntuación (1-5)
1	D1	¿La estrategia tecnológica, las prioridades de riesgo y las principales decisiones de modernización se gobiernan mediante foros ejecutivos claramente definidos con derechos de decisión documentados?	
2	D1	¿Se asignan formalmente responsables para riesgos tecnológicos materiales, controles, servicios críticos y acciones de remediación?	
3	D1	¿Las políticas y normas tecnológicas están sujetas a procesos definidos de aprobación, excepción, revisión y retiro?	
4	D1	¿Los riesgos tecnológicos y de ciberseguridad se integran en la gestión de riesgos empresariales, el apetito de riesgo y los informes ejecutivos y al consejo?	
5	D1	¿Los informes de gestión utilizan KPI/KRI relevantes para decisiones, umbrales, tendencias y criterios de escalamiento, en lugar de solamente métricas de actividad?	
6	D2	¿La institución mantiene un inventario confiable de aplicaciones, infraestructura, integraciones, dependencias críticas, estado del ciclo de vida y propiedad empresarial?	
7	D2	¿Las tecnologías al final de su vida útil, sin soporte, de alta complejidad o alta dependencia se identifican y gobiernan mediante planes documentados de ciclo de vida y remediación?	

N.º	Dominio	Pregunta diagnóstica	Puntuación (1-5)
8	D2	¿Existe una arquitectura objetivo y una hoja de ruta de modernización documentadas y alineadas con la estrategia empresarial, las prioridades de riesgo y la resiliencia de los servicios críticos?	
9	D2	¿Las integraciones y API se gobiernan mediante prácticas definidas de arquitectura, seguridad, datos, versiones, propiedad y seguimiento?	
10	D2	¿La deuda técnica, complejidad de cambios, excepciones de arquitectura y dependencias de modernización se miden e incorporan a las decisiones de inversión?	
11	D3	¿Los propietarios de datos, custodios, elementos de datos críticos, requisitos de clasificación y responsabilidad por la calidad de los datos están claramente definidos?	
12	D3	¿Los problemas de calidad, linaje, conciliación e informes de datos se miden, investigan y remedian según el impacto empresarial y regulatorio?	
13	D3	¿Los procesos de incorporación-movilidad-salida están integrados con la gobernanza de identidades para que el acceso sea oportuno, rastreable y eliminado cuando deje de estar justificado?	
14	D3	¿Los derechos de acceso privilegiado y de alto riesgo están sujetos a autenticación sólida, aprobación, registro, seguimiento y recertificación periódica?	
15	D3	¿Los conflictos de segregación de funciones y las excepciones de acceso se identifican, evalúan por riesgo, limitan en el tiempo y revisan por una gestión responsable?	
16	D4	¿La institución mantiene un inventario completo y clasificado por riesgo de terceros, servicios de nube, subcontratistas materiales y dependencias tecnológicas?	
17	D4	¿La debida diligencia evalúa seguridad, resiliencia, condición financiera, tratamiento de datos, apoyo regulatorio, concentración y capacidades operativas de forma proporcional al riesgo?	
18	D4	¿Los contratos y SLA abordan seguridad, derechos sobre datos, notificación de incidentes, derechos de auditoría/acceso, resiliencia, subcontratación, desempeño, terminación y necesidades de salida?	
19	D4	¿Los terceros materiales están sujetos a seguimiento continuo de desempeño, riesgo, controles, incidentes y condición financiera con umbrales definidos de escalamiento?	
20	D4	¿Se evalúan el riesgo de concentración, brechas de responsabilidad compartida en la nube, sustituibilidad, portabilidad de datos y planes de salida/transición para proveedores críticos?	
21	D5	¿Las prácticas de seguimiento, registro, alertas, gestión de vulnerabilidades y escalamiento de incidentes de ciberseguridad se basan en riesgos y son eficaces para sistemas y servicios críticos?	
22	D5	¿El programa de respuesta a incidentes se prueba mediante ejercicios que incluyen toma de decisiones ejecutivas, comunicaciones, proveedores, jurídico/cumplimiento y coordinación de recuperación?	
23	D5	¿Los análisis de impacto empresarial, RTO, RPO, dependencias de recuperación y planes de continuidad están actualizados para productos y servicios financieros críticos?	
24	D5	¿Las capacidades de copia de seguridad, restauración, conmutación por error y recuperación ante desastres se prueban con una frecuencia y alcance acordes con la criticidad del servicio y los escenarios de amenaza?	
25	D5	¿Las debilidades significativas de resiliencia, puntos únicos de falla, exposición a ransomware y restricciones de recuperación se rastrean mediante una remediación con responsables?	
26	D6	¿Los controles tecnológicos materiales pueden mapearse a pruebas documentadas que demuestren diseño, responsabilidad, operación, ensayos y tratamiento de excepciones?	
27	D6	¿Los hallazgos de auditoría, examen, cumplimiento y riesgo se gobiernan mediante un proceso común de gestión de problemas con responsables, fechas límite, pruebas y validación?	
28	D6	¿La institución mantiene un proceso estructurado para identificar cambios regulatorios o de supervisión aplicables a la tecnología y traducirlos en acciones?	
29	D6	¿Las políticas, procedimientos, normas, pruebas de sistemas, resultados de ensayos y aprobaciones de gestión están organizados para producirse eficientemente en auditorías o exámenes?	
30	D6	¿Los elementos de remediación vencidos, recurrentes o de alta gravedad se escalan a la dirección ejecutiva y al consejo o comité correspondiente con decisiones claras y aceptación del riesgo?	

5.2 Expectativas de evidencia y disciplina de puntuación

Una respuesta diagnóstica debe documentarse en cuatro campos: puntuación, pruebas revisadas, observación y referencia de acción o riesgo. Las pruebas típicas incluyen estatutos de gobernanza, materiales del consejo o comités, políticas y normas, inventarios de activos y aplicaciones, diagramas de arquitectura, registros de proveedores, contratos, informes de revisión de accesos, métricas de vulnerabilidad, registros de incidentes, resultados de pruebas de copia de seguridad y recuperación, hallazgos de auditoría, rastreadores de problemas, paneles y registros de cambios. El objetivo no es maximizar el volumen de documentación, sino establecer trazabilidad entre la puntuación y la práctica institucional observable.

Las puntuaciones deben describir institucionalización, no aspiración. Una política recién aprobada sin pruebas operativas generalmente respalda una puntuación En desarrollo o Definida, según el alcance de implementación; no debe respaldar automáticamente una madurez Gestionada. A la inversa, un proceso maduro puede estar respaldado por pruebas automatizadas y un historial operativo consistente, aunque la organización utilice una terminología diferente a la del framework. Los evaluadores deben documentar las prácticas compensatorias en lugar de forzar una conformidad artificial.

El cuestionario es deliberadamente conciso. Una evaluación completa debe ampliar cada pregunta en subpruebas basadas en el alcance y la materialidad. Por ejemplo, la Pregunta 24 puede exigir una revisión separada del diseño de copias de seguridad inmutables, pruebas de restauración, aislamiento para recuperación cibernética, conmutación por error de servicios críticos, dependencias de recuperación y evidencias de recuperación de proveedores. Por lo tanto, el instrumento de 30 preguntas debe entenderse principalmente como un diagnóstico ejecutivo y organizador del programa de trabajo.

6. Modelo de evaluación y priorización de riesgos

6.1 Escalas de probabilidad e impacto

El modelo de riesgos utiliza una matriz de probabilidad e impacto de 5 × 5 como recurso de comunicación. Dado que las matrices cualitativas de riesgo pueden crear una falsa precisión, compresión de rangos y ordenación ambigua, la puntuación numérica no debe utilizarse como único fundamento para las decisiones de remediación (Cox, 2008). Por eso, el ARTTF combina la puntuación base con factores explícitos de escalamiento, criticidad de los servicios, relevancia regulatoria y juicio profesional.

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

Tabla 6. Escala de probabilidad

Puntuación	**Nivel**	**Interpretación**
1	Rara	No se espera en condiciones normales; controles preventivos sólidos y exposición limitada.
2	Improbable	Plausible pero infrecuente; la exposición es limitada o los controles son generalmente eficaces.
3	Posible	Podría ocurrir en condiciones realistas; existen debilidades o dependencias conocidas.
4	Probable	Se espera que ocurra o se repita sin remediación; hay pruebas de debilidad de controles o eventos repetidos.
5	Casi segura	Activa, recurrente, muy expuesta o con pruebas sólidas de ser inminente/persistente.

Tabla 7. Escala de impacto

Puntuación	**Nivel**	**Interpretación**
1	Limitado	Efecto localizado; sin consecuencias materiales para clientes, regulación, finanzas o servicios críticos.
2	Moderado	Interrupción o falla de control manejable, con impacto empresarial contenido.
3	Significativo	Impacto operativo, sobre clientes, datos, auditoría, finanzas o gestión que requiere una respuesta coordinada.
4	Grave	Impacto serio sobre servicios críticos, datos sensibles, postura regulatoria, pérdidas financieras u operaciones sostenidas.
5	Severo / Crítico	Potencial de interrupción amplia o prolongada, daño importante a clientes/datos, exposición regulatoria significativa o amenaza a servicios esenciales.

6.2 Mapa de calor de riesgos y bandas base de prioridad

La puntuación base de riesgo se calcula como Probabilidad × Impacto y genera un valor de 1 a 25. Las bandas de prioridad predeterminadas son Baja (1-4), Moderada (5-9), Alta (10-14) y Crítica (15-25). Estas bandas son puntos de partida y deben calibrarse al apetito de riesgo y a la política de gestión de problemas de la institución. La matriz no debe prevalecer sobre requisitos obligatorios de remediación, compromisos de auditoría, hallazgos regulatorios o vulnerabilidades críticas conocidas.

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

Figura 1. Mapa de calor de riesgos del ARTTF (puntuación base)

Impact → Likelihood ↓	**1**	**2**	**3**	**4**	**5**
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Nota. Bandas base: Baja = 1-4; Moderada = 5-9; Alta = 10-14; Crítica = 15-25. Las puntuaciones son un recurso de priorización, no una estimación cuantitativa de la pérdida esperada.

6.3 Factores cualitativos de escalamiento

Tabla 8. Factores de escalamiento de la prioridad de riesgo

Factor de escalamiento	**Desencadenante**	**Tratamiento**
Importancia regulatoria o de supervisión	El hallazgo se relaciona con un compromiso regulatorio, hallazgo de examen, requisito legal, problema formal de auditoría o expectativa material de supervisión.	Elevar la prioridad cuando el retraso pueda crear exposición regulatoria, jurídica o de examen.
Dependencia de servicio crítico	El hallazgo afecta pagos, depósitos, préstamos, acceso de clientes, identidad, seguridad, procesamiento central u otro servicio esencial.	Elevar cuando la falla pueda perjudicar un producto/servicio crítico o una dependencia de recuperación.
Datos sensibles / impacto sobre clientes	El hallazgo podría exponer de forma material datos confidenciales, de clientes, financieros, de autenticación o regulados.	Elevar cuando la sensibilidad, escala o potencial de uso indebido de los datos sea material.
Exposición externa / explotabilidad	La debilidad está expuesta a internet, se explota activamente, es fácil de abusar o está conectada con credenciales débiles o acceso privilegiado.	Elevar según inteligencia de amenazas, pruebas de vulnerabilidad o exposición.
Concentración de terceros / sustituibilidad	Un proveedor crítico tiene sustitutos limitados, dependencias opacas, capacidad de salida inadecuada o riesgo de concentración.	Elevar cuando la institución tenga control limitado o pocas alternativas de recuperación.
Fragilidad de recuperación	Los controles no se han probado, la restauración es incierta, no pueden demostrarse RTO/RPO o permanecen puntos únicos de falla.	Elevar cuando la falla pueda prolongar la interrupción o volver incierta la recuperación.
Problema recurrente / vencido	El mismo problema se repitió, superó fechas objetivo o permaneció abierto durante revisiones anteriores.	Elevar para reflejar una gobernanza de remediación ineficaz y exposición acumulada.

Una práctica recomendada es preservar la puntuación base original y registrar por separado la prioridad final de gestión. Por ejemplo, una puntuación base de 12 puede

designarse Crítica porque se trata de un hallazgo regulatorio vencido que afecta un servicio crítico de pagos. Este enfoque mantiene la transparencia de la puntuación y evita manipular la probabilidad o el impacto únicamente para alcanzar la prioridad deseada.

7. Panel ejecutivo de riesgos tecnológicos

7.1 Diseño del panel

El panel ejecutivo traduce los detalles de la evaluación en un conjunto limitado de indicadores relevantes para la decisión. Debe responder cuatro preguntas: ¿cuál es la postura actual de madurez y riesgo? ¿Qué riesgos requieren decisiones ejecutivas? ¿La remediación avanza al ritmo necesario? ¿Las iniciativas de modernización están mejorando o aumentando la resiliencia? Por lo tanto, el panel debe combinar indicadores de madurez, riesgo, remediación, resiliencia, arquitectura, terceros y auditoría en lugar de informar solamente actividades de ciberseguridad.

Las métricas deben definirse con responsable, lógica de cálculo, fuente de datos, umbral, frecuencia y vía de escalamiento. Un panel sin umbrales puede convertirse en un artefacto de reporte en vez de un control de gestión. Del mismo modo, una cantidad excesiva de métricas puede ocultar los pocos problemas que requieren acción. El ARTTF recomienda una visión ejecutiva compacta respaldada por desgloses operativos más profundos.

Tabla 9. Medidas recomendadas para el panel ejecutivo

Indicador	**Definición**	**Frecuencia**	**Uso ejecutivo**
Madurez tecnológica general	Puntuación media de madurez de los dominios más nivel de confianza de las pruebas.	Trimestral	Tendencia y objetivo por ciclo de evaluación.
Madurez de los dominios	Puntuaciones de madurez D1-D6.	Trimestral	Destacar dominios por debajo del objetivo o en declive.
Riesgos tecnológicos Críticos / Altos	Cantidad y tendencia de elementos Críticos y Altos abiertos.	Mensual	Escalar inmediatamente nuevos elementos Críticos.
Remediación vencida	Número y porcentaje de problemas más allá de la fecha objetivo aprobada.	Mensual	Escalar elementos materiales vencidos y prórrogas repetidas.
Hallazgos regulatorios / de auditoría	Hallazgos abiertos por gravedad, antigüedad, fecha límite y estado de validación.	Mensual	Separar compromisos que requieren pruebas formales de cierre.
Exposición crítica a sistemas heredados	Servicios críticos dependientes de tecnología sin soporte o de alto riesgo.	Trimestral	Rastrear hitos de retiro, contención y desacoplamiento.
Terceros de alto riesgo	Proveedores materiales con problemas abiertos de controles, desempeño, resiliencia o contrato.	Mensual	Incluir estado de concentración y plan de salida.
Excepciones de acceso privilegiado	Cuentas/excepciones de alto riesgo fuera de políticas o requisitos de recertificación.	Mensual	Escalar privilegios sin responsable, obsoletos, compartidos o excesivos.

Indicador	Definición	Frecuencia	Uso ejecutivo
Cumplimiento del SLA de parches / vulnerabilidades	Porcentaje de vulnerabilidades materiales remediadas dentro del SLA definido en función del riesgo.	Mensual	Segmentar por exposición y criticidad empresarial.
Éxito de pruebas de copia de seguridad / recuperación	Servicios críticos con pruebas exitosas y documentadas de restauración/conmutación por error.	Trimestral	Rastrear pruebas fallidas y dependencias de recuperación no demostradas.
Preparación para ejercicios de incidentes / crisis	Estado y cierre de lecciones de ejercicios de mesa o recuperación.	Trimestral / Semestral	Escalar hallazgos no resueltos y de alto impacto de los ejercicios.
Tasa de cierre de remediación	Elementos cerrados y validados independientemente frente a los abiertos durante el período.	Mensual	Supervisar crecimiento de la cartera y recurrencia.
Estado de los hitos de modernización	Hitos críticos de la hoja de ruta en plazo, en riesgo o retrasados.	Mensual	Vincular retrasos con exposición de riesgo y decisiones ejecutivas.
Decisiones ejecutivas requeridas	Decisiones abiertas sobre financiación, aceptación de riesgos, secuenciación, proveedores o alcance.	Mensual	Mantener registro de decisiones con responsable y fecha límite.

7.2 Cadencia de gobernanza

Una cadencia práctica de gobernanza combina revisiones mensuales de remediación y transformación, revisiones trimestrales de riesgos ejecutivos e informes periódicos al consejo o a comités del consejo según el modelo de gobernanza de la institución. Los riesgos críticos no deben esperar una reunión programada. El panel debe preservar el historial de decisiones, la aceptación aprobada de riesgos, los cambios en fechas objetivo y la justificación de decisiones materiales de secuenciación. Esto crea un vínculo auditable entre los hallazgos de la evaluación y la responsabilidad ejecutiva.

8. Hoja de ruta de remediación y modernización

8.1 Principios de la hoja de ruta

La hoja de ruta convierte los hallazgos de riesgo y madurez en acciones secuenciadas. El orden no debe estar determinado únicamente por la puntuación numérica de riesgo más alta. Algunas acciones son requisitos previos de otras: una institución puede necesitar establecer la propiedad de las aplicaciones y el mapeo de dependencias antes de racionalizarlas de forma segura; puede necesitar estabilizar la recuperación de copias de seguridad antes de iniciar una migración de infraestructura de alto riesgo; y puede necesitar propiedad y clasificación de datos antes de implementar analítica avanzada a escala.

Por este motivo, el ARTTF utiliza tres horizontes de planificación. Los primeros 0-90 días enfatizan gobernanza, pruebas, reducción urgente de la exposición y logros rápidos. El horizonte de 3-12 meses institucionaliza controles y ejecuta modernización de complejidad

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 22/08/2026 | aceito: 25/08/2026 | publicação: 28/08/2026

media. El horizonte de 12-24 meses aborda transformación estructural, grandes cambios de plataforma, arquitectura de datos, ingeniería de resiliencia y mejora continua. El cronograma debe adaptarse al perfil de riesgo de la institución, capacidad de recursos, restricciones de proveedores y compromisos regulatorios.

Tabla 10. Hoja de ruta por fases de remediación y modernización

Horizonte	**Acciones prioritarias**	**Entregables representativos**	**Resultado de gestión esperado**
0-90 días - Estabilizar y establecer control	Confirmar gobernanza ejecutiva y responsables; validar inventarios de servicios críticos y tecnología; identificar activos críticos sin soporte; cerrar brechas urgentes de acceso privilegiado y autenticación; validar copia de seguridad/restauración de servicios críticos; clasificar proveedores materiales; crear registro unificado de problemas; establecer plan de cierre regulatorio y de auditoría; definir principios de decisión del estado objetivo.	Estatuto de gobernanza; responsables/RACI; inventario crítico; registro de riesgos principales; logros rápidos validados; línea de base del panel ejecutivo; plan de remediación de 90 días.	Los riesgos desconocidos o sin responsable se vuelven visibles; se contiene la exposición inmediata; los ejecutivos disponen de una base factual común.
3-12 meses - Institucionalizar y modernizar	Implementar arquitectura objetivo y oleadas de modernización; formalizar gobernanza de datos; reforzar IAM/PAM y recertificación de accesos; mejorar prácticas de vulnerabilidad y observabilidad; establecer gobernanza de nube y proveedores; probar BCP/DR y respuesta a incidentes; mejorar el ciclo de vida de políticas; automatizar pruebas cuando sea práctico; ejecutar remediación de alta prioridad.	Arquitectura objetivo; cartera de modernización; modelo operativo de gobernanza de datos; seguimiento de proveedores; pruebas de recuperación verificadas; controles mejorados; tendencia de remediación mensurable.	Los controles se vuelven repetibles y mensurables; la deuda técnica crítica y las brechas de resiliencia comienzan a disminuir.
12-24 meses - Transformar y optimizar	Ejecutar una gran modernización de sistemas heredados/core; desacoplar integraciones y reforzar la arquitectura de API/plataformas; modernizar la arquitectura de datos; implementar ingeniería de resiliencia y pruebas de dependencias; optimizar el modelo operativo de nube; automatizar gobernanza e informes; preparar casos de analítica avanzada/IA sobre bases controladas; incorporar la reevaluación continua.	Plataformas modernizadas; arquitectura resiliente; mejores bases de datos; métricas continuas; gobernanza optimizada; reevaluación que muestra mejora de madurez.	Se reduce el riesgo estructural; modernización y resiliencia se refuerzan mutuamente; la mejora continua se institucionaliza.

8.2 Reglas de priorización y secuenciación

1. Abordar las exposiciones inmediatas de seguridad, clientes, regulación y servicios críticos antes del trabajo de optimización.

2. Establecer responsabilidades y pruebas antes de utilizar las puntuaciones de madurez para decisiones de inversión.

3. Resolver brechas fundamentales de identidad, recuperación, inventario y dependencias que puedan socavar la modernización posterior.

4. Secuenciar la modernización por capacidad empresarial y dependencia, no solamente por la antigüedad de la aplicación.

5. Utilizar contención cuando la sustitución inmediata sea impracticable, pero definir un hito explícito de salida o modernización.

6. Tratar las dependencias de proveedores y nube como parte de la arquitectura del servicio, incluida la planificación de recuperación y salida.

7. Integrar los compromisos de auditoría y regulatorios en la misma hoja de ruta utilizada para la transformación tecnológica.

8. Exigir decisiones ejecutivas para riesgos aceptados, prórrogas repetidas de plazos, reducciones materiales de alcance y cambios que afecten servicios críticos.

9. Reevaluar la madurez y el riesgo residual después de remediaciones materiales o grandes oleadas de modernización.

10. Preservar la trazabilidad desde el hallazgo hasta el riesgo, la acción, las pruebas, la validación y el cierre.

9. Aplicación ilustrativa

9.1 Institución hipotética y alcance

El caso siguiente es ficticio y se presenta exclusivamente para demostrar la mecánica del framework. No representa un cliente, institución financiera, evaluación o conclusión regulatoria real.

HarborView Community Bank (HCB) se modela como un banco comunitario regional hipotético con aproximadamente 3.000 millones de dólares en activos, un modelo operativo mixto de sucursales y canales digitales, varios cientos de empleados y una dependencia material de un proveedor de core bancario, aplicaciones de clientes alojadas en la nube, proveedores de pagos y servicios tecnológicos externalizados. La dirección planea un programa plurianual de modernización digital, pero ha acumulado problemas de auditoría abiertos, integraciones punto a punto, propiedad de datos inconsistente y varias relaciones de alta dependencia con proveedores. El alcance de la evaluación abarca los seis dominios del ARTTF y se centra en servicios críticos de depósitos, pagos, canales digitales, información de clientes e informes financieros.

9.2 Resultados ilustrativos de madurez

Tabla 11. Resultados ilustrativos de madurez para HCB

Dominio	Descripción	Puntuación	Interpretación ilustrativa
D1	Gobernanza tecnológica y responsabilidad ejecutiva	2,8	Existen foros de gobernanza definidos, pero la propiedad y los umbrales de KRI son inconsistentes.
D2	Sistemas heredados y arquitectura tecnológica	1,8	Varios componentes críticos están envejeciendo; la arquitectura objetivo y el mapeo de dependencias están incompletos.

Dominio	Descripción	Puntuación	Interpretación ilustrativa
D3	Gobernanza de datos, identidad y gestión de accesos	2,2	Existen controles de acceso, pero deben reforzarse la propiedad de datos, gobernanza de accesos privilegiados y recertificación.
D4	Nube, proveedores y riesgo de terceros	2,0	Se conocen los proveedores materiales, pero la concentración, planificación de salida y seguimiento continuo son inconsistentes.
D5	Ciberseguridad, continuidad del negocio y recuperación	2,4	Las operaciones de seguridad están establecidas, pero las pruebas de recuperación y de resiliencia entre proveedores están incompletas.
D6	Auditabilidad, preparación regulatoria y gobernanza de la remediación	2,6	Existe seguimiento de problemas, pero los hallazgos vencidos y la calidad de las pruebas requieren una gobernanza ejecutiva más sólida.
General	Madurez con ponderación igual	2,3	Clasificación general: En desarrollo.

La puntuación general ilustrativa de 2,3 indica que HCB estableció varias prácticas fundamentales, pero carece de una institucionalización consistente en arquitectura, gobernanza de terceros, gestión de datos y accesos y recuperación. La observación más importante no es el promedio en sí, sino el perfil desigual de madurez. Un banco puede mantener operaciones de ciberseguridad relativamente maduras y aun así asumir un riesgo material debido a tecnología sin soporte, una planificación deficiente de salida de proveedores o dependencias de recuperación no probadas.

9.3 Riesgos prioritarios ilustrativos

Tabla 12. Registro y priorización ilustrativos de riesgos

ID	Riesgo	P	I	Prioridad base / final	Justificación del escalamiento	Tratamiento inmediato
R1	Middleware sin soporte que sostiene integraciones críticas de pagos	4	5	20 - Crítica	Dependencia conectada externamente, experiencia interna limitada, servicio crítico de pagos.	Contener exposición; confirmar opciones de proveedor/soporte; acelerar plan de desacoplamiento/sustitución.
R2	Cuentas privilegiadas con recertificación incompleta y propiedad inconsistente	4	4	16 - Crítica	Alto privilegio y acceso a sistemas sensibles; relevancia de auditoría.	Recertificación de emergencia; eliminar accesos obsoletos; implementar gobernanza y seguimiento de PAM.
R3	La restauración de servicios críticos no se ha demostrado de extremo a extremo entre proveedores clave	3	5	15 - Crítica	Fragilidad de recuperación y dependencia de terceros.	Ejecutar prueba de restauración/conmutación por error; validar RTO/RPO y dependencias de proveedores; cerrar brechas de evidencia.
R4	El acuerdo con un proveedor material de nube carece de disposiciones suficientemente detalladas de salida/transición	3	4	12 - Alta	Inquietudes de concentración y sustituibilidad.	Revisar contrato y plan de salida; definir requisitos de portabilidad de datos y transición.
R5	Un hallazgo de auditoría de alta gravedad superó la fecha objetivo después de dos prórrogas	3	4	12 - Crítica (escalada)	Factor de gobernanza recurrente/vencido y compromiso de auditoría.	Escalamiento ejecutivo; plan de recuperación; validación independiente antes del cierre.

ID	Riesgo	P	I	Prioridad base / final	Justificación del escalamiento	Tratamiento inmediato
R6	Los elementos de datos críticos carecen de responsables y umbrales de calidad asignados formalmente	3	3	9 - Moderada	Afecta la confiabilidad de informes y la preparación para modernización/analítica.	Establecer propiedad y modelo operativo de calidad de datos en el horizonte de 3-12 meses.

9.4 Vista ilustrativa del panel ejecutivo

Tabla 13. Panel ejecutivo ilustrativo

Indicador	Estado actual	Objetivo	Estado	Comentario ejecutivo
Madurez general	2,3 - En desarrollo	Objetivo 3,0 en 12 meses	Ámbar	Arquitectura y TPRM son los dominios más bajos.
Riesgos críticos	4	Objetivo ≤ 1 en 90 días	Rojo	R1, R2, R3 y R5 requieren seguimiento ejecutivo.
Riesgos altos	1	Tendencia decreciente	Ámbar	R4: riesgo de salida de la nube.
Remediación vencida	7 elementos; 2 materiales	Ningún elemento material vencido	Rojo	R5 requiere plan de recuperación y acción de gobernanza.
Exposición crítica a sistemas heredados	3 servicios críticos	Todos con plan financiado de modernización/contención	Rojo	El middleware de pagos es la máxima prioridad.
Terceros de alto riesgo	6; 2 con problemas abiertos	Todos con seguimiento activo y postura de salida	Ámbar	Se requiere revisión contractual y de concentración.
Excepciones de acceso privilegiado	14	Cero excepciones de alto riesgo sin responsable u obsoletas	Rojo	Recertificación inmediata en curso.
Pruebas de recuperación	3 de 5 servicios críticos probados de extremo a extremo	5 de 5	Ámbar	Debe completarse la restauración entre proveedores.
Hitos de modernización	2 en riesgo	Ningún hito crítico sin decisión ejecutiva	Ámbar	El mapeo de dependencias retrasa la secuenciación de arquitectura.

9.5 Hoja de ruta ilustrativa

En los primeros 90 días, HCB establecería un único foro ejecutivo de remediación, validaría el inventario de servicios críticos, aplicaciones y proveedores, completaría la recertificación de accesos privilegiados, realizaría una prueba integral de recuperación para los servicios de mayor criticidad, establecería un plan de recuperación para problemas de auditoría vencidos y definiría hitos de contención y sustitución para el middleware de pagos sin soporte. Estas acciones reducirían la exposición inmediata y mejorarían la base de pruebas para la modernización de más largo plazo.

Durante los meses 3-12, HCB ejecutaría la primera oleada de modernización de la arquitectura, formalizaría la propiedad de los datos y los umbrales de calidad, mejoraría la gestión de accesos privilegiados, reforzaría el seguimiento de la nube y los proveedores, completaría las pruebas de continuidad del negocio y recuperación ante desastres de servicios

críticos y racionalizaría los procesos de gestión de problemas y pruebas de controles. El objetivo sería alcanzar un nivel Definido en todos los dominios y establecer prácticas Gestionadas en las áreas de mayor riesgo.

Durante los meses 12-24, HCB continuaría desacoplando integraciones heredadas, implementaría la arquitectura objetivo de plataformas y datos, mejoraría la ingeniería de resiliencia y las pruebas de dependencias, automatizaría determinadas pruebas e informes de riesgos y establecería un modelo operativo para analítica responsable y preparación para IA. Una reevaluación formal compararía la madurez de los dominios, el riesgo residual, problemas vencidos, pruebas de recuperación y resultados de modernización con la línea de base original.

10. Discusión

La proposición central del ARTTF es que el riesgo tecnológico y la modernización tecnológica deben gestionarse mediante una perspectiva ejecutiva común. Las instituciones financieras suelen organizar responsabilidades por funciones especializadas: ciberseguridad, infraestructura, arquitectura, datos, gestión de proveedores, cumplimiento, auditoría interna y ejecución de programas. La especialización es necesaria, pero puede fragmentar la responsabilidad cuando la institución debe decidir qué acciones de transformación son más importantes. El framework crea un vocabulario compartido sin exigir que estas funciones se fusionen en un único equipo.

Una segunda contribución es la separación explícita entre madurez y riesgo. La madurez pregunta con qué consistencia y eficacia se institucionaliza una capacidad. El riesgo pregunta qué podría ocurrir, qué probabilidad tiene, qué gravedad puede alcanzar el impacto y qué contexto adicional modifica la prioridad. Una puntuación baja de madurez puede no crear un riesgo alto inmediato cuando el proceso sustenta un servicio de baja criticidad y exposición limitada. A la inversa, una organización generalmente madura puede tener una única vulnerabilidad crítica o dependencia de recuperación no probada que requiera acción inmediata. Tratar madurez y riesgo como conceptos separados pero conectados ayuda a evitar interpretaciones simplistas.

Una tercera contribución es el uso de la confianza de las pruebas. Las evaluaciones tecnológicas dependen con frecuencia de entrevistas con líderes que entienden los procesos previstos, pero pueden no percibir excepciones locales. Registrar la confianza de las pruebas hace visible la incertidumbre y orienta pruebas de seguimiento. También permite una

reevaluación más creíble, porque las mejoras pueden evaluarse mediante pruebas operativas y no solo por cambios de percepción.

El framework también destaca la relación entre modernización y resiliencia operativa. La modernización puede reducir el riesgo al eliminar sistemas sin soporte, reducir procesos manuales, mejorar la observabilidad, reforzar la identidad y simplificar integraciones. También puede aumentar el riesgo cuando la migración introduce nuevas dependencias, debilita el diseño de recuperación, crea concentración o cambia responsabilidades operativas más rápido de lo que la gobernanza puede adaptarse. Por lo tanto, una hoja de ruta basada en riesgos trata la resiliencia como requisito de diseño de la modernización y no como control posterior a la implementación.

Para instituciones pequeñas y medianas, la proporcionalidad es especialmente importante. El objetivo no es reproducir el modelo de personal, documentación o herramientas de un gran banco global. Consiste en demostrar que la gobernanza y los controles son adecuados al tamaño, complejidad, productos, datos, dependencia tecnológica y perfil de riesgo de la institución. La misma pregunta diagnóstica puede llevar, por lo tanto, a expectativas de pruebas diferentes en un banco comunitario, una plataforma fintech y una gran empresa de pagos.

El framework también puede favorecer la transferencia de conocimiento. Como los dominios, preguntas, definiciones de puntuación, enfoque del mapa de calor, medidas del panel y horizontes de la hoja de ruta están documentados, los equipos internos pueden reutilizar el método durante reevaluaciones periódicas, gobernanza de proyectos, revisiones de proveedores y planificación ejecutiva. Esta repetibilidad puede reducir la dependencia de evaluaciones puntuales y ayudar a las instituciones a desarrollar una capacidad interna de gestión de riesgos tecnológicos.

11. Limitaciones e investigaciones futuras

El ARTTF tiene varias limitaciones. Primero, el artículo actual presenta una metodología conceptual y aplicada, no un modelo predictivo validado empíricamente. La escala de cinco niveles y las preguntas diagnósticas aún no se han sometido a pruebas de confiabilidad estadística en una población representativa de instituciones financieras. Segundo, la puntuación cualitativa de riesgos depende del juicio del evaluador. Aunque los requisitos de evidencia y los factores de escalamiento reducen la subjetividad, diferentes evaluadores pueden alcanzar puntuaciones distintas. Tercero, las obligaciones jurídicas y

regulatorias específicas de cada institución varían según licencia, regulador, producto, geografía, datos y actividad; un framework generalizado no puede sustituir un análisis jurídico, de cumplimiento o de supervisión adaptado.

Cuarto, el framework utiliza deliberadamente un conjunto compacto de 30 preguntas. Esto favorece la facilidad de uso ejecutivo, pero implica que un trabajo completo debe ampliar las preguntas en procedimientos detallados y pruebas de evidencia. Quinto, el riesgo tecnológico cambia rápidamente. Las condiciones de amenaza, expectativas regulatorias, arquitecturas de nube, casos de uso de IA, dependencias de proveedores y productos evolucionan, por lo que los criterios diagnósticos deben revisarse periódicamente y someterse a control de versiones.

Las investigaciones futuras deben evaluar el framework mediante múltiples estudios de caso en bancos comunitarios, cooperativas de crédito, empresas fintech y organizaciones de pagos. Las preguntas de investigación útiles incluyen la consistencia entre evaluadores, la relación entre mejoras de madurez y cierre de problemas, el efecto de la confianza de las pruebas en la precisión de la puntuación, el valor de diferentes ponderaciones de los dominios y si la secuenciación de la hoja de ruta mejora el tiempo del ciclo de remediación o reduce hallazgos recurrentes. El trabajo futuro también podría desarrollar extensiones específicas para procesamiento de pagos, Banking-as-a-Service, gestión patrimonial y adopción responsable de IA.

12. Consideraciones finales

Las organizaciones financieras reguladas deben modernizarse preservando control, seguridad, auditabilidad y continuidad. Estos objetivos suelen gestionarse mediante programas separados, aunque las dependencias tecnológicas subyacentes sean compartidas. El Agility Regulated Technology Transformation Framework proporciona un método integrado para conectar estas preocupaciones mediante seis dominios, un modelo de madurez de cinco niveles, un diagnóstico de 30 preguntas, priorización de riesgos, informes ejecutivos y planificación de la transformación por fases.

El framework es intencionalmente práctico. Comienza con alineación ejecutiva y pruebas, distingue madurez de riesgo y concluye con una hoja de ruta que asigna responsabilidades y secuenciación. El caso ilustrativo muestra cómo una institución puede pasar de observaciones fragmentadas a una visión consolidada del riesgo tecnológico y las prioridades de modernización. El resultado más importante no es una puntuación numérica de

madurez, sino una narrativa de gestión defendible que explique qué es material, por qué importa, quién es responsable, qué pruebas sustentan la conclusión y qué acción debe ocurrir a continuación.

Utilizada adecuadamente, la metodología puede respaldar la preparación regulatoria, remediación de auditorías, modernización de sistemas, gobernanza de datos y accesos, supervisión de terceros, ciberseguridad y resiliencia operativa. Está diseñada para complementar —no sustituir— frameworks reconocidos y orientaciones de supervisión. Su valor reside en traducir esos principios en un proceso ejecutivo repetible para priorizar y gobernar la transformación tecnológica en entornos financieros regulados.

13. Declaraciones

Conflicto de intereses: el autor es fundador y propietario de Agility Digital Technologies, LLC., y desarrolló el framework descrito en este artículo. Se declara esta afiliación porque el framework lleva el nombre de la empresa.

Financiación: no se recibió financiación externa para la elaboración de este artículo metodológico.

Declaración ética: este artículo no involucra participantes humanos, animales ni datos confidenciales de clientes. El caso ilustrativo es completamente hipotético.

Disponibilidad de datos: no se creó ni analizó ningún conjunto de datos empíricos. Todos los datos y puntuaciones del caso presentados con fines demostrativos son hipotéticos.

14. Referencias

Cox, L. A., Jr. (2008). What's wrong with risk matrices? Risk Analysis, 28(2), 497-512. https://doi.org/10.1111/j.1539-6924.2008.01030.x

Federal Deposit Insurance Corporation, Board of Governors of the Federal Reserve System, & Office of the Comptroller of the Currency. (2023). Interagency guidance on third-party relationships: Risk management. https://www.fdic.gov/news/financial-institution-letters/2023/fil23029.html

Federal Financial Institutions Examination Council. (2019). Business Continuity Management booklet. FFIEC Information Technology Examination Handbook. https://www.ffiec.gov/news/press-releases/2019/pr-11-14

Federal Financial Institutions Examination Council. (2021a). Architecture, Infrastructure, and Operations booklet. FFIEC Information Technology Examination Handbook. https://www.ffiec.gov/news/press-releases/2021/pr-06-30

Federal Financial Institutions Examination Council. (2021b). Authentication and Access to Financial Institution Services and Systems guidance. https://www.ffiec.gov/news/press-releases/2021/pr-08-11

Financial Stability Board. (2024). The financial stability implications of artificial intelligence. https://www.fsb.org/2024/11/the-financial-stability-implications-of-artificial-intelligence/

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105. https://aisel.aisnet.org/misq/vol28/iss1/6/

Khatri, V., & Brown, C. V. (2010). Designing data governance. Communications of the ACM, 53(1), 148-152. https://doi.org/10.1145/1629175.1629210

National Credit Union Administration. (2026). 2025 cybersecurity and credit union system resilience report. https://ncua.gov/news/publication-search/cybersecurity/2025-cybersecurity-and-credit-union-system-resilience-report

Office of the Comptroller of the Currency. (2026). 2026 cybersecurity and financial system resilience report. https://www.occ.treas.gov/publications-and-resources/publications/cybersecurity-and-financial-system-resilience/index-cybersecurity-and-financial-system-resilience-report.html

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302

Quinn, S., Pascoe, C., Barrett, M., Scarfone, K., & Witte, G. (2024). NIST Cybersecurity Framework 2.0: Quick-start guide for using the CSF Tiers (NIST SP 1302). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1302

Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

U.S. Department of the Treasury. (2024a, December 19). Treasury releases report on the uses, opportunities, and risks of artificial intelligence in financial services. https://home.treasury.gov/news/press-releases/jy2760

U.S. Department of the Treasury. (2024b, July 17). Treasury and the Financial Services Sector Coordinating Council publish new resources on effective practices for secure cloud adoption. https://home.treasury.gov/news/press-releases/jy2467

U.S. Department of the Treasury. (2026, February 19). Treasury releases two new resources to guide AI use in the financial sector. https://home.treasury.gov/news/press-releases/sb0401

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems, 28(2), 118-144. https://doi.org/10.1016/j.jsis.2019.01.003