**UNIVERSIDAD PRIVADA DE TACNA**

**FACULTAD DE INGENIERÍA**

**Escuela Profesional de Ingeniería de Sistemas**



**ARTÍCULO TECNOLÓGICO:**

“Propuesta de políticas de gobernanza de red en instituciones públicas en línea con el ODS 16”

**Curso: REDES Y COMUNICACIÓN DE DATOS I**

**Docente:**

ALCANTARA MARTINEZ, HUGO MARTIN

**Estudiante:**

LEYVA SARDON, ELVIS RONALD (2021072614)

**Tacna – Perú**

**2025**

# ABSTRACT

La gobernanza de redes en instituciones públicas es un pilar fundamental para garantizar servicios digitales seguros, transparentes y accesibles, en línea con el Objetivo de Desarrollo Sostenible (ODS) 16: "Paz, justicia e instituciones sólidas". Este artículo propone un marco de políticas de gobernanza de red orientado a fortalecer la eficiencia, la seguridad cibernética y la rendición de cuentas en el sector público, abordando desafíos como la fragmentación de sistemas, la vulnerabilidad ante ciberataques y las brechas en el acceso a la información. A través de una metodología basada en revisión documental y análisis comparativo de buenas prácticas internacionales, se identifican cuatro ejes clave: seguridad de datos bajo estándares internacionales, interoperabilidad institucional, transparencia mediante tecnologías abiertas, e inclusión digital para reducir desigualdades. La propuesta demuestra cómo estas políticas no solo optimizan la infraestructura tecnológica gubernamental, sino que también contribuyen directamente a las metas del ODS 16, particularmente a la creación de instituciones eficaces (meta 16.6) y al acceso público a la información (meta 16.10). Se concluye con recomendaciones para su implementación, destacando la necesidad de marcos normativos adaptativos y cooperación multiacto.

# INTRODUCCIÓN

En la era de la transformación digital, las instituciones públicas enfrentan el desafío de modernizar sus infraestructuras de red para garantizar servicios eficientes, seguros y accesibles a la ciudadanía. Sin embargo, la falta de políticas robustas de gobernanza de redes puede generar problemas críticos, como vulnerabilidades en ciberseguridad, fragmentación de sistemas, opacidad en la gestión de datos y exclusión digital. Estos desafíos no solo limitan la eficacia gubernamental, sino que también obstaculizan el cumplimiento del Objetivo de Desarrollo Sostenible (ODS) 16, que promueve "paz, justicia e instituciones sólidas" mediante metas como la transparencia, el acceso a la información y la reducción de la corrupción.

En este contexto, la gobernanza de redes emerge como un factor estratégico para alinear las capacidades tecnológicas del sector público con los principios del ODS 16. A nivel global, organismos como la ONU y la UIT han destacado la necesidad de marcos normativos que aseguren redes interoperables, protegidas y abiertas. No obstante, muchas instituciones especialmente en países en desarrollo carecen de políticas integrales, lo que incrementa riesgos como ciberataques a infraestructuras críticas o la desconfianza ciudadana en servicios digitales estatales.

Este artículo propone un modelo de políticas de gobernanza de red para instituciones públicas, diseñado bajo tres pilares: seguridad, transparencia e inclusión. A través de un análisis cualitativo de estándares internacionales y casos de éxito, se definen lineamientos prácticos para fortalecer la infraestructura digital estatal. La relevancia de esta investigación radica en su enfoque dual: (1) resolver problemas técnicos de gestión de redes y (2) contribuir a los indicadores del ODS 16, demostrando cómo la tecnología puede ser un habilitador de instituciones más justas y eficaces.

# DESARROLLO

## Definición y componentes de la gobernanza de red

La gobernanza de red es el conjunto de políticas, normas, procesos y estructuras organizativas que regulan el diseño, operación, monitoreo y mejora de las redes digitales estatales. Esta gobernanza no se limita al aspecto técnico, sino que abarca decisiones estratégicas sobre seguridad, interoperabilidad, transparencia, ética digital y equidad en el acceso.

La gobernanza de la red interorganizacional proporciona un conjunto de principios compartidos conjuntamente que afectan la interacción entre los actores de la red y, en última instancia, el valor creado en la red. (Clauss & Ritala, 2023)

En el contexto gubernamental, las redes no solo conectan dispositivos, sino que constituyen infraestructuras críticas para el funcionamiento del Estado moderno, permitiendo desde la gestión de servicios ciudadanos (salud, educación, justicia) hasta la administración financiera, electoral y documental.

La gobernanza en red en las instituciones públicas coordina y gestiona eficazmente la red de cooperación entre los diferentes niveles de gobierno y los diversos departamentos, promoviendo el interés público y abordando cuestiones complejas. (Zhang, H. & Teo, B., 2023)

## Seguridad de redes públicas: estándares internacionales y desafíos emergentes

### Amenazas actuales en redes estatales

La seguridad de redes en instituciones públicas se ha convertido en una prioridad estratégica, considerando que los gobiernos dependen cada vez más de infraestructuras digitales para operar servicios esenciales como salud, justicia, educación y finanzas. Sin una protección adecuada, estas redes son blanco frecuente de ciberataques que comprometen la estabilidad institucional, la privacidad ciudadana y la continuidad operativa del Estado.

Entre las amenazas más frecuentes que enfrentan las redes gubernamentales se encuentran:

* Ransomware dirigido: es un tipo de malware que bloquea o cifra la información de una red institucional, exigiendo un rescate económico para recuperar el acceso a los datos.
* Phishing institucional: consiste en ataques de suplantación de identidad que buscan engañar a funcionarios o usuarios para obtener credenciales de acceso o información mediante correos o sitios falsos.
* Ataques de denegación de servicio (DDoS): intentan saturar un sistema o servicio digital mediante múltiples solicitudes simultáneas.

Las principales amenazas cibernéticas para las instituciones de educación superior en 2020 son los ataques de malware, los ataques DoS/DDos y los ataques de phishing, que representan un desafío para los especialistas en este campo. (Arina, A., 2022)

### Normas internacionales y estrategias de protección

Para mitigar estas amenazas, los gobiernos han adoptado marcos normativos y estándares reconocidos a nivel internacional, entre los que destacan:

* ISO/IEC 27001: Es el estándar internacional más reconocido en la gestión de seguridad de la información. Proporciona un marco sistemático para identificar riesgos, implementar controles y establecer políticas de protección.
* Estrategias Nacionales de Ciberseguridad (ENC): Son instrumentos de planificación que permiten a los Estados definir prioridades, responsabilidades y marcos legales para proteger su ecosistema digital.
* Directiva NIS y NIS2 (UE): Obliga a las entidades públicas y operadores críticos a adoptar medidas técnicas y organizativas robustas y a notificar incidentes graves.
* Guías y marcos del NIST (EE. UU.): Proporciona directrices para identificar, proteger, detectar, responder y recuperar ante ciberataques.

ISO/IEC 27001 es una norma internacional que proporciona orientación para construir y mantener un sistema de gestión de seguridad de la información (SGSI) y aumenta la confianza entre las partes interesadas. (Putra, D. y otros, 2021).

Las Estrategias Nacionales de Ciberseguridad (ECN) son planes que consideran la visión financiera, las cualidades sociales y culturales de un país y apuntan a construir órdenes sociales seguros, fuertes y mejorados mediante las TIC. (Alghamdi, 2021)

## Integración de políticas: propuesta de un marco adaptativo y transversal

Se propone un modelo basado en cuatro ejes interdependientes: seguridad, interoperabilidad, transparencia e inclusión. Estos pilares permiten construir una arquitectura institucional que sea técnica y socialmente sólida, en línea con las metas del ODS 16.

|  |  |
| --- | --- |
| **Seguridad:** Prioriza la protección de datos, la integridad de la información y la continuidad operativa. Las políticas deben adoptar estándares como ISO/IEC 27001 y garantizar planes de gestión de incidentes, formación del personal y auditorías periódicas. La ciberseguridad debe estar integrada desde el diseño (“security by design”). | **Interoperabilidad:** Busca garantizar que los sistemas y plataformas de diferentes entidades públicas se comuniquen entre sí de manera fluida. Esto implica usar estándares abiertos, servicios web normalizados y catálogos de datos comunes. La interoperabilidad reduce la redundancia administrativa y mejora la eficiencia y la experiencia del ciudadano. |
| **Transparencia:** Implica políticas que promuevan la apertura de datos, el acceso a la información pública y el monitoreo ciudadano. La implementación de portales de datos abiertos y plataformas de rendición de cuentas son claves para fortalecer la confianza pública y combatir la corrupción. | **Inclusión digital:** Se refiere a garantizar que todos los ciudadanos, sin importar su ubicación geográfica, edad, nivel educativo o condición económica, puedan acceder y beneficiarse de los servicios digitales. Esto incluye la accesibilidad para personas con discapacidad y alfabetización digital. |

## Sugerencias de lineamientos generales y adaptabilidad

Para que este modelo sea efectivo, se sugiere establecer lineamientos generales que puedan ser adaptados a las realidades locales de cada institución, región o país. Algunas recomendaciones clave incluyen:

* **Diagnóstico inicial participativo:** Realizar evaluaciones técnicas y sociales de la infraestructura y capacidades existentes, incorporando la visión de usuarios, técnicos y tomadores de decisiones.
* **Normativas marco flexibles:** Crear leyes o reglamentos que establezcan principios y objetivos generales, permitiendo que cada institución defina mecanismos específicos según su tamaño, nivel de digitalización y sector.
* **Gobernanza multiactor:** Fomentar la colaboración entre organismos públicos, sector privado, sociedad civil y academia para co-crear políticas tecnológicamente viables y socialmente aceptables.
* **Planes de acción escalables:** Diseñar políticas que puedan implementarse en fases, priorizando componentes críticos, con metas de corto, mediano y largo plazo, según los recursos y capacidades institucionales.
* **Evaluación continua y retroalimentación:** Incorporar sistemas de monitoreo y evaluación que permitan ajustar las políticas en tiempo real, basándose en evidencia y nuevas amenazas tecnológicas.

## Cómo estas políticas permiten cumplir con las metas 16.6 y 16.10 de la ODS.

### ODS 16.6: Crear instituciones eficaces, responsables y transparentes

El eje de interoperabilidad mejora la eficiencia operativa al reducir la duplicación de datos, agilizar procesos administrativos y facilitar la coordinación entre entidades estatales. Plataformas interoperables permiten la automatización de trámites, el seguimiento en tiempo real de expedientes y una administración orientada al servicio ciudadano.

La seguridad fortalece la confianza en las instituciones, al proteger la integridad de los servicios digitales, prevenir interrupciones críticas y garantizar la confidencialidad de la información.

Asimismo, la inclusión digital extiende la cobertura de los servicios públicos digitales, especialmente en zonas rurales, con poblaciones vulnerables o históricamente excluidas. Esto permite construir instituciones representativas y con legitimidad social.

### ODS 16.10: Garantizar el acceso público a la información y proteger las libertades fundamentales

Las políticas basadas en el eje de transparencia permiten cumplir directamente esta meta. La implementación de portales de datos abiertos, sistemas de trazabilidad digital y mecanismos de rendición de cuentas facilita el acceso ciudadano a información pública clara, oportuna y verificable.

Además, el enfoque “gobierno abierto” permite que la ciudadanía participe activamente en la supervisión de las instituciones, fortaleciendo así la democracia digital y la lucha contra la corrupción. Esto se alinea con los principios promovidos por iniciativas internacionales como la Alianza para el Gobierno Abierto (OGP) y la Declaración de Derechos Digitales de la ONU.

# CONCLUSIONES

**La gobernanza de red fortalece la institucionalidad pública y promueve la eficiencia del Estado (ODS 16.6):** Un marco de políticas integradas basado en seguridad, interoperabilidad, transparencia e inclusión permite construir instituciones más eficaces, responsables y tecnológicamente resilientes. Esto mejora la gestión de recursos públicos, optimiza servicios y genera confianza ciudadana en la administración estatal.

**La transparencia digital impulsa el acceso a la información y combate la corrupción (ODS 16.10):** La implementación de plataformas de datos abiertos, trazabilidad digital y rendición de cuentas fortalece la democracia participativa, promueve la vigilancia ciudadana y protege el derecho fundamental de acceso a la información pública.

**La inclusión digital reduce desigualdades y promueve sociedades más justas (ODS 10 y 16):** Al garantizar acceso universal a servicios digitales incluyendo zonas rurales, personas con discapacidad y sectores vulnerables se democratiza la tecnología y se avanza hacia una gobernanza más representativa, equitativa y sostenible.

**La ciberseguridad, clave para la paz digital y la protección de derechos (ODS 16 y 9):** Integrar la seguridad desde el diseño de los sistemas públicos no solo previene ataques y protege la privacidad, sino que asegura la continuidad de servicios esenciales como salud, educación o justicia, fortaleciendo el rol del Estado en la era digital.

**La gobernanza multiactor fortalece la legitimidad y responsabilidad institucional (ODS 16.7):** Incorporar a diversos actores en el diseño, implementación y evaluación de políticas de red promueve procesos más participativos, representativos y responsables. Esto permite construir instituciones más inclusivas, alineadas con las necesidades reales de la sociedad.

# OBJETIVO DE DESAROLLO SOSTENIBLE 2025

Promover sociedades pacíficas e inclusivas para el desarrollo sostenible, facilitar el acceso a la justicia para todos y crear instituciones eficaces, responsables e inclusivas a todos los niveles.

# REFERENCIAS BIBLIOGRÁFICAS

Alghamdi, M. (2021). Guide to developing a National Cyber Security Strategy. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.02.613

Arina, A. (2022). Network Security Threats to Higher Education Institutions. *Central and Eastern European eDem and eGov Days.* https://doi.org/10.24989/ocg.v341.24

Clauss, T., & Ritala, P. (2023). Network governance institutionalization: Creating mutual value by harnessing and avoiding conflicts in interorganizational networks. *Journal of Business Research*. https://doi.org/10.1016/j.jbusres.2023.113880

Putra, D., Tistiyani, S., & Sunaringtyas, S. (2021). The Use of ISO/IEC 27001 Family of Standards in Regulatory Requirements in Some Countries. *2021 2nd International Conference on ICT for Rural Development (IC-ICTRuDev)*, 1-6. https://doi.org/10.1109/IC-ICTRuDev50538.2021.9656529

Zhang, H., & Teo, B. (2023). Literature Review on the Construction of Service-Oriented Government in China from the Perspective of Network Governance. *Frontiers in Humanities and Social Sciences.* https://doi.org/10.54691/fhss.v3i2.4129.