Análisis sobre la centralización de funciones de Transformación Digital del Estado y Protección de Infraestructura Crítica en Guatemala

Análisis sobre la centralización de funciones de Transformación Digital del Estado y Protección de Infraestructura Crítica en Guatemala

"Guatemala No se Detiene"
Sylvia María Campos Verdesia
9 de mayo 2025

I. Introducción

La infraestructura crítica (IC) abarca los sistemas, activos y servicios esenciales cuya interrupción comprometería la seguridad nacional, el desarrollo económico y el bienestar social. Incluye sectores como energía, agua, transporte, telecomunicaciones, salud y finanzas. Su protección es una prioridad estratégica, especialmente en países como Guatemala, donde estas infraestructuras presentan vulnerabilidades severas. Paralelamente, la Transformación Digital del Estado (TDE) busca modernizar la gestión pública mediante el uso intensivo de tecnologías digitales, con el propósito de mejorar servicios, promover la transparencia y dinamizar la economía digital. No obstante, el país enfrenta limitaciones estructurales significativas en ambos ámbitos: el 35% de la población no tiene acceso a internet y Guatemala ocupa el puesto 134 de 141 en conectividad vial según el Foro Económico Mundial.

En este contexto, surge una interrogante crucial para el diseño institucional: ¿Debe un solo ente asumir las funciones de transformación digital y protección de infraestructuras críticas? Aunque ambas son áreas estratégicas, difieren sustancialmente en objetivos, marcos normativos y requerimientos técnicos. Resolver esta cuestión exige un análisis integral que considere factores operativos, jurídicos y de gobernanza.

Algunos países han optado por centralizar ambas funciones en una sola entidad, buscando sinergias y eficiencia. Sin embargo, la mayoría, incluyendo miembros de la OCDE y varias naciones latinoamericanas, han optado por mantenerlas separadas, articuladas mediante mecanismos de coordinación estratégica. Esta separación favorece la especialización técnica, una mejor gestión de riesgos y una mayor adaptabilidad institucional.

Este documento examina las ventajas, desventajas y riesgos de ambos modelos, presenta un análisis comparativo de experiencias internacionales y propone un enfoque adaptado a las condiciones de Guatemala. Se argumenta que, dada la inmadurez del ecosistema digital, las brechas normativas y las limitaciones institucionales, entre otras, la opción más viable es mantener funciones separadas pero coordinadas. Esto permite desarrollar capacidades específicas sin comprometer la eficiencia operativa, a la vez que se fortalece la resiliencia nacional frente a amenazas tanto físicas como digitales.

II. Modelos internacionales comparados

El siguiente cuadro comparativo analiza la gestión de la transformación digital y la protección de infraestructuras críticas en 12 países, seleccionados por su diversidad en niveles de desarrollo, contextos institucionales y enfoques estratégicos. Incluye casos de América Latina (México, Colombia, Uruguay, Perú, Chile, Costa Rica, Argentina), referentes globales en digitalización (Estonia, Singapur), y modelos de resiliencia en seguridad (Estados Unidos, España, Israel). La tabla examina los entes responsables, la unificación o separación de funciones, y los mecanismos de coordinación, proporcionando una base técnica para evaluar modelos aplicables a Guatemala. Este análisis identifica patrones exitosos, como la especialización y coordinación

estratégica en España y Costa Rica, y destaca desafíos en contextos con recursos limitados, señalando las propuestas para abordar las limitaciones institucionales, normativas y digitales de Guatemala.

País	Ente encargado de la transformación digital del Estado	Ente responsable de la infraestructura crítica	Funciones: Unificadas o Separadas	Coordinación entre entidades
México	Coordinación de Estrategia Digital Nacional (Presidencia de la República) y Agencia Digital de Innovación Pública (ADIP, Ciudad de México): Implementan la Agenda Digital Nacional para digitalizar servicios públicos, promover interoperabilidad y mejorar conectividad. La ADIP lidera iniciativas como Llave CDMX para trámites digitales.	Centro Nacional de Control de Energía (CENACE) y Secretaría de Seguridad y Protección Ciudadana (SSPC): CENACE protege infraestructura energética crítica; SSPC coordina seguridad general, incluyendo ciberseguridad, vía el Centro Nacional de Ciberseguridad. El INIFED gestiona infraestructura escolar. No hay ente único centralizado.	**Separadas:** Transformación digital y protección de infraestructuras críticas están divididas entre entidades federales y locales, con enfoques sectoriales.	Coordinación moderada: La Guardia Nacional y el CSIRTmx (OEA) facilitan colaboración en ciberseguridad, pero la descentralización y falta de un marco unificado limitan la integración.
Colombia	Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC): Lidera la Estrategia de Gobierno Digital y el Plan Nacional de Conectividad para digitalizar servicios, mejorar acceso a internet y fomentar innovación.	Unidad de Gestión del Riesgo de Desastres (UNGRD) y Ministerio de Defensa: UNGRD protege infraestructuras críticas frente a desastres naturales; el Comando Conjunto Cibernético (CCOC) aborda ciberamenazas a sectores como energía y telecomunicaciones.	**Separadas:** Digitalización a cargo de MinTIC; protección de infraestructuras críticas por entidades de seguridad y gestión de riesgos.	Coordinación alta: El CSIRT Colombiano (ColCERT), bajo MinTIC, colabora con CCOC y UNGRD en ciberseguridad, integrando esfuerzos vía la Política Nacional de Ciberseguridad.
Perú	Secretaría de Gobierno y Transformación Digital (Presidencia del Consejo de Ministros): Lidera el Laboratorio de Gobierno y Transformación Digital y la Estrategia Nacional de Gobierno Digital, impulsando plataformas como GEOPERÚ y Participa Perú. Perú está en el puesto 58 global en EGDI 2024.	Ministerio del Interior y Autoridad Nacional del Agua (ANA): Ministerio del Interior supervisa seguridad de infraestructuras críticas; ANA protege recursos hídricos. El Centro Nacional de Seguridad Digital (CNSD) aborda ciberamenazas. No hay ente único.	**Separadas:** Transformación digital centralizada en la Secretaría; protección de infraestructuras críticas fragmentada entre ministerios y entidades sectoriales.	Coordinación moderada: CNSD y CSIRT.pe facilitan colaboración en ciberseguridad, pero la falta de un ente unificado limita la integración. La Plataforma Nacional de Interoperabilidad apoya la coordinación digital.
Estados Unidos	Oficina de Estrategia Digital Nacional (Casa Blanca) y Departamento de Comercio (NTIA): Gestionan la Estrategia Nacional de Tecnología y digitalización de servicios federales.	Departamento de Seguridad Nacional (DHS, vía CISA): Protege 16 sectores críticos (energía, transporte, comunicaciones). Otros departamentos (Defensa, Energía) supervisan sectores específicos.	**Separadas**: Transformación digital y protección de infraestructuras críticas divididas entre agencias federales con roles especializados.	Coordinación alta: CISA colabora con NTIA y otras agencias en ciberseguridad mediante consejos sectoriales y el Centro Nacional de Coordinación de Ciberseguridad. La colaboración público-privada es clave.
Chile	División de Gobierno Digital (Ministerio de Hacienda): Lidera el Plan de Transformación Digital del Estado, digitalizando servicios públicos (ej., ClaveÚnica) y promoviendo interoperabilidad.	Ministerio de Defensa y Agencia Nacional de Ciberseguridad (ANCI): La Ley N° 21.542 (2023) asigna a las Fuerzas Armadas la protección de infraestructuras críticas (energía, agua, telecomunicaciones). ANCI,	**Separadas:** Transformación digital a cargo de Hacienda; protección de infraestructuras críticas dividida entre Defensa (seguridad	Coordinación alta: ANCI y el CSIRT Nacional coordinan ciberseguridad entre entidades públicas y privadas, apoyados por el Consejo Multisectorial sobre Ciberseguridad.

País	Ente encargado de la transformación digital del Estado	Ente responsable de la infraestructura crítica	Funciones: Unificadas o Separadas	Coordinación entre entidades
		creada en 2024, protege infraestructuras digitales críticas y coordina ciberseguridad.	física) y ANCI (ciberseguridad).	
España	Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA, Ministerio para la Transformación Digital y de la Función Pública): Implementa el Plan España Digital 2025, digitalizando servicios, promoviendo IA y extendiendo banda ancha.	Centro Nacional de Protección de Infraestructuras Críticas (CNPIC, Ministerio del Interior): Protege 12 sectores críticos (energía, transporte, TIC) bajo la Ley 8/2011, elaborando el Catálogo Nacional de Infraestructuras Estratégicas.	**Separadas:** SEDIA lidera digitalización; CNPIC se enfoca en protección de infraestructuras críticas, con roles claramente definidos.	Coordinación alta: El Instituto Nacional de Ciberseguridad (INCIBE) actúa como puente, coordinando ciberseguridad entre SEDIA, CNPIC y operadores privados, bajo la Estrategia Nacional de Ciberseguridad.
Costa Rica	Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT): Lidera el Plan Nacional de Desarrollo de las Telecomunicaciones, conectando el 95% de las escuelas a banda ancha y promoviendo la Identidad Digital Nacional.	Ministerio de Seguridad Pública y CSIRT-CR: Ministerio de Seguridad protege infraestructuras críticas (energía, agua, telecomunicaciones); CSIRT-CR aborda ciberamenazas, apoyado por el ICE para redes eléctricas.	**Separadas**: MICITT se enfoca en digitalización; Seguridad Pública y CSIRT-CR gestionan protección de infraestructuras críticas.	Coordinación alta: El Consejo Nacional de Telecomunicaciones y CSIRT-CR facilitan colaboración en ciberseguridad, integrando esfuerzos entre sectores públicos y privados.
Argentina	Secretaría de Innovación Pública (Jefatura de Gabinete de Ministros): Lidera la Estrategia Nacional de Transformación Digital, implementando plataformas como Mi Argentina y promoviendo interoperabilidad y datos abiertos.	Ministerio de Seguridad y Agencia Nacional de Seguridad: Ministerio de Seguridad protege infraestructuras críticas (energía, transporte, comunicaciones); la Agencia Nacional de Seguridad, creada en 2023, aborda ciberseguridad para sectores críticos.	**Separadas**: Transformación digital a cargo de la Secretaría; protección de infraestructuras críticas dividida entre Seguridad y la Agencia Nacional.	Coordinación moderada: El CERT Nacional (AR-CERT) coordina ciberseguridad, pero la reciente creación de la Agencia Nacional limita la integración. La Plataforma Nacional de Interoperabilidad apoya la coordinación digital.
Singapur	Ministerio de Comunicaciones e Información (MCI) y Agencia GovTech: Lideran la iniciativa Smart Nation, digitalizando servicios (ej., Singpass, usado por 70% de la población) y promoviendo conectividad y adopción de IA.	Agencia de Ciberseguridad de Singapur (CSA): Protege infraestructuras críticas de información (CII) en sectores como energía y transporte, bajo el Código de Práctica de Ciberseguridad (CCoP2.0, 2022).	**Separadas**: MCI y GovTech lideran digitalización; CSA se enfoca en protección de CII, con roles especializados.	Coordinación alta: CSA colabora con MCI y operadores privados mediante el Centro Nacional de Ciberseguridad y consejos sectoriales, asegurando alineación en la Estrategia Nacional de Ciberseguridad.
Uruguay	Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC): Implementa la Agenda Uruguay Digital 2025, liderando digitalización de servicios, participación ciudadana y ciberseguridad. Uruguay es líder regional en gobierno digital (EGDI 2024: puesto 22 global).	AGESIC y Ministerios (Transporte y Obras Públicas, Interior, Energía): AGESIC gestiona ciberseguridad para infraestructuras críticas (CERTuy); el Ministerio del Interior supervisa seguridad física de sectores como energía y transporte, con apoyo de ANP y UTE.	**Parcialmente unificadas**: AGESIC centraliza transformación digital y ciberseguridad de infraestructuras críticas; seguridad física está separada.	Coordinación alta: AGESIC coordina ciberseguridad y digitalización mediante CERTuy y la Estrategia Nacional de Ciberseguridad, con apoyo del Consejo Asesor para la Sociedad de la Información.

País	Ente encargado de la transformación digital del Estado	Ente responsable de la infraestructura crítica	Funciones: Unificadas o Separadas	Coordinación entre entidades
Estonia	Ministerio de Asuntos Económicos y Comunicaciones: Lidera la transformación digital a través de iniciativas como e-Estonia, con 99% de servicios gubernamentales en línea y el programa de e-residencia. Es líder global en gobierno digital (EGDI 2024: puesto 2).	Autoridad de Sistemas de Información (RIA): Coordina la protección de infraestructuras críticas de información (CII) bajo la Ley de Ciberseguridad, gestionando el CERT-EE y supervisando sectores esenciales (energía, transporte, salud).	**Parcialmente unificadas**: El Ministerio lidera digitalización y ciberseguridad; RIA se enfoca en protección de CII, pero la seguridad física es gestionada por otros ministerios (Interior, Defensa).	Coordinación alta: El Consejo de Ciberseguridad, RIA y CERT-EE coordinan esfuerzos, apoyados por la Estrategia de Ciberseguridad 2024-2030. La cooperación con NATO y la UE refuerza la integración.
Israel	Oficina Nacional de Transformación Digital (Ministerio de Economía): Lidera la digitalización de servicios públicos y la adopción de tecnologías avanzadas (ej., IA, blockchain).	Dirección Nacional de Ciberseguridad (INCD, Ministerio de Defensa): Protege infraestructuras críticas (energía, agua, comunicaciones) y coordina ciberseguridad nacional, apoyada por el CERT-IL y unidades militares (IDF).	**Parcialmente unificadas**: INCD centraliza ciberseguridad para digitalización e infraestructuras críticas; la transformación digital está separada, pero coordinada.	Coordinación alta: INCD, CERT-IL y el Ministerio de Defensa integran esfuerzos con el sector privado y agencias digitales, apoyados por una robusta colaboración público-privada y R&D.

El análisis comparativo demuestra una tendencia clara hacia la separación de funciones entre los entes encargados de la transformación digital y los responsables de la protección de infraestructuras críticas. Este modelo es adoptado por la mayoría de los países revisados -incluidos México, Colombia, Perú, Estados Unidos, España y Costa Rica- y se caracteriza por una mayor especialización técnica, una gestión diferenciada de riesgos físicos y digitales, y estructuras de gobernanza más adaptables. Por otro lado, países como Uruguay, Estonia e Israel aplican modelos de unificación parcial, centrados en la ciberseguridad, pero con marcos normativos sólidos y alta madurez digital. Este último modelo parece tener limitada sus aplicabilidad de forma directa en contextos con menor capacidad institucional, como el guatemalteco.

III. Ventajas y Desventajas

A continuación, se analizan ventajas y desventajas de aplicar un modelo institucional de manejo conjunto de la transformación digital y las infraestructuras críticas, con ejemplos internacionales y su aplicabilidad a Guatemala.

Ventajas

1. **Sinergia en la gestión de la ciberseguridad**: La transformación digital del Estado implica modernizar sistemas tecnológicos, implementar servicios digitales y proteger datos sensibles. Dado que muchas infraestructuras críticas (como redes eléctricas, sistemas de transporte o telecomunicaciones) dependen de tecnologías digitales, un ente conjunto podría alinear las estrategias de ciberseguridad para ambos ámbitos. Por ejemplo: un solo organismo podría estandarizar protocolos de seguridad para plataformas gubernamentales y sistemas críticos, reduciendo vulnerabilidades comunes.
2. **Optimización de recursos**: Unificar ambos roles en un solo ente podría reducir costos operativos al evitar la duplicación de funciones, como la gestión de equipos de

ciberseguridad, infraestructura tecnológica o auditorías de seguridad. Se podrían compartir recursos humanos y tecnológicos, como centros de operaciones de seguridad (SOC) o herramientas de monitoreo, para proteger tanto los servicios digitales del Estado como las infraestructuras críticas.

3. **Coordinación integral**: La transformación digital y la protección de infraestructuras críticas requieren colaboración entre sectores públicos y privados. Un ente unificado podría facilitar la comunicación y la implementación de estándares comunes, asegurando una visión holística de la seguridad y la modernización tecnológica. Ejemplo: En España, el CNPIC colabora con operadores privados; un ente similar podría integrar esfuerzos de digitalización y protección en un solo marco.
4. **Aceleración de la modernización**: La experiencia en transformación digital podría aplicarse para actualizar sistemas obsoletos en infraestructuras críticas (como redes SCADA[1] en energía o transporte), mejorando su resiliencia frente a ciberataques. Un enfoque combinado podría priorizar la adopción de tecnologías emergentes (como IA o blockchain) para ambas áreas.
5. **Gestión unificada de datos**: Ambos roles implican manejar grandes volúmenes de datos sensibles. Un solo ente podría implementar políticas de gobernanza de datos coherentes, asegurando la privacidad y seguridad tanto en servicios digitales como en sistemas críticos.

Desventajas

1. **Sobrecarga operativa**: La protección de infraestructuras críticas y la transformación digital son tareas complejas y de gran escala. Unificarlas en un solo ente podría saturar su capacidad operativa, dificultando la atención adecuada a cada área. Ejemplo: En Chile, la Ley N° 21.542 asigna roles específicos a las Fuerzas Armadas para infraestructuras críticas, mientras que la transformación digital suele recaer en ministerios como el de Hacienda o Tecnología. Combinarlas podría generar conflictos de prioridades.
2. **Falta de especialización**: La protección de infraestructuras críticas requiere conocimientos específicos en seguridad física, ciberseguridad industrial y gestión de riesgos en sectores como energía o transporte. La transformación digital, en cambio, se centra en servicios ciudadanos, identidad digital, interoperabilidad y modernización administrativa. Un ente conjunto podría diluir la experiencia técnica en uno u otro ámbito. Ejemplo: En España, el CNPIC se dedica exclusivamente a infraestructuras críticas, mientras que la transformación digital está liderada por la Secretaría de Estado de Digitalización e Inteligencia Artificial. Esta separación permite enfoques especializados.
3. **Riesgo de centralización excesiva**: Concentrar ambas responsabilidades en un solo ente podría crear un punto único de fallo. Un error, un ciberataque o una mala gestión en el ente afectaría tanto la infraestructura crítica como los servicios digitales del Estado. También podría generar dependencias excesivas de un solo organismo, reduciendo la resiliencia del sistema.

[1] Sistema SCADA (Supervisory Control and Data Acquisition, por sus siglas en inglés) es una tecnología utilizada para monitorear, controlar y gestionar procesos industriales e infraestructuras críticas en tiempo real. Combina hardware y software para recopilar datos de sensores y dispositivos, supervisar operaciones y enviar comandos a equipos en sectores como energía, agua, transporte, manufactura o puertos.

4. **Conflictos de objetivos**: La transformación digital prioriza la accesibilidad, la innovación y la experiencia del usuario, mientras que la protección de infraestructuras críticas se centra en la seguridad, la resiliencia y la confidencialidad. Estos objetivos pueden entrar en conflicto, por ejemplo, al implementar sistemas abiertos para ciudadanos que podrían ser vulnerables para infraestructuras críticas. Ejemplo: Un sistema digital ciudadano podría requerir acceso público, mientras que un sistema crítico (como el control de una presa) necesita aislamiento total.
5. **Desafíos de gobernanza y regulación**: Las infraestructuras críticas suelen involucrar a múltiples sectores (energía, transporte, salud) y operadores privados, con regulaciones específicas. La transformación digital, en cambio, se centra más en el sector público. Un ente conjunto podría enfrentar dificultades para coordinar normativas y actores claves con intereses diversos. Ejemplo: En la UE, la Directiva (UE) 2022/2557 establece requisitos estrictos para entidades críticas, mientras que la transformación digital sigue marcos como el Reglamento eIDAS. Unificar estas responsabilidades podría complicar el cumplimiento normativo.
6. **Riesgo político y de percepción pública**: Un ente con tanto poder (controlando infraestructuras críticas y servicios digitales) podría ser percibido como una amenaza a la privacidad o una herramienta de control estatal, especialmente en contextos donde la confianza en las instituciones es baja. Ejemplo: En Chile, la participación de las Fuerzas Armadas en la protección de infraestructuras críticas ya ha generado críticas por posibles implicaciones en derechos ciudadanos.

IV. Conclusión

A partir del análisis nacional e internacional se identifican cuatro ejes fundamentales que sustentan la recomendación para Guatemala de ***optar por una separación funcional entre la transformación digital del Estado y la protección de infraestructuras críticas con mecanismos eficaces de coordinación estratégica***. Esta opción permite:

- **La especialización técnica de los entes.** La transformación digital del Estado y la protección de infraestructuras críticas requieren conocimientos, capacidades y culturas organizativas distintas. La digitalización implica interoperabilidad, experiencia de usuario, plataformas accesibles y protección de datos, mientras que la gestión de infraestructuras críticas involucra seguridad física, continuidad operativa, supervisión de activos estratégicos y análisis de riesgos sistémicos. Intentar fusionar estas competencias en un solo ente comprometería la calidad técnica de ambas agendas, reduciendo su eficacia operativa. La especialización garantiza un enfoque experto, con mandatos y equipos dedicados a los desafíos particulares de cada función.

- **La resiliencia operativa frente a riesgos sistémicos**. La existencia de dos entes diferenciados permite diseñar respuestas adaptadas a distintos tipos de amenazas, desde ciberataques hasta desastres naturales o fallas físicas. En contextos complejos como el guatemalteco, donde la infraestructura es frágil y la respuesta ante crisis aún limitada, es preferible que cada entidad desarrolle protocolos, capacidades de monitoreo y alertas tempranas para su ámbito específico. Esta división mejora la redundancia, reduce el riesgo de fallos institucionales y aumenta la capacidad de adaptación frente a crisis multidimensionales.

- **La inclusión digital como prioridad diferenciada**. La inclusión digital requiere políticas activas que aborden desigualdades históricas en el acceso a internet, dispositivos y competencias digitales, especialmente en zonas rurales, comunidades indígenas y grupos vulnerables. Un ente centrado exclusivamente en esta agenda podrá movilizar recursos, articular políticas educativas y promover alianzas para expandir la conectividad sin que se vean relegadas frente a prioridades de infraestructura crítica, usualmente asociadas a seguridad y defensa.

- **La necesidad de una gobernanza interinstitucional robusta**. La separación funcional exige mecanismos efectivos de coordinación para asegurar coherencia, evitar duplicidades y garantizar una visión nacional compartida. Esto implica crear instancias como un *Consejo Nacional de Ciberseguridad y Digitalización*, con representación de múltiples sectores y poderes del Estado. La gobernanza colaborativa es especialmente importante en países con baja confianza institucional, ya que permite mayor control público, auditoría social y legitimidad democrática de las políticas implementadas.

Esta conclusión también tiene fundamento en tres desafíos clave que enfrenta Guatemala: la brecha digital estructural, la alta vulnerabilidad física de las infraestructuras nacionales y las limitaciones institucionales, económicas y normativas que dificultan una gobernanza integrada eficaz.

La experiencia internacional muestra que los países que han optado por modelos parcialmente unificados -como Israel o Estonia- cuentan con capacidades tecnológicas, normativas y presupuestarias que Guatemala aún no ha desarrollado. En cambio, los modelos de separación con coordinación estratégica, como los aplicados en Costa Rica, España y Colombia, permiten avanzar en digitalización e inclusión sin descuidar la resiliencia frente a amenazas físicas o cibernéticas. Guatemala puede adoptar un esquema similar, fortaleciendo capacidades específicas en cada función y estableciendo mecanismos claros de coordinación interinstitucional, con participación pública y privada. Esta vía maximiza la eficiencia operativa y facilita la inversión de cooperación internacional y alianzas público-privadas.

V. Recomendaciones para Guatemala

A partir del diagnóstico técnico y la comparación internacional, se recomienda que Guatemala adopte un modelo institucional con **entes separados** para la transformación digital del Estado y la protección de infraestructuras críticas, articulados mediante una **coordinación estratégica robusta**. Esta propuesta se basa en la evidencia de que los modelos unificados, como se mencionó antes, solo funcionan en países con alta madurez normativa, digital y operativa, condiciones que Guatemala aún no cumple. En ese sentido, se proponen avanzar en tres ejes complementarios:

Ejes	Planteamiento
1. **Estructura institucional especializada**	• **Agencia Nacional de Transformación Digital (ANTD).** Encargada, bajo la Presidencia o un Ministerio específico, de la conectividad, digitalización de servicios públicos, interoperabilidad, identidad digital y alfabetización digital. Esta entidad deberá priorizar la inclusión de zonas rurales e indígenas, alineándose con los esfuerzos de conectividad y alfabetización digital. • **Ente Nacional de Protección de Infraestructuras Críticas (ENPIC).** Adscrito al Ministerio de Gobernación o Defensa, será responsable de mapear, clasificar y proteger activos estratégicos (agua, transporte, energía, salud), mediante planes de resiliencia y

	gestión de riesgos físicos y digitales, en articulación con instituciones como INSIVUMEH y la CONRED, entre otras.
2. Mecanismos de coordinación y gobernanza	• **Consejo Nacional de Ciberseguridad y Digitalización.** Órgano colegiado con participación de los diferentes organismos del Estado, sector privado, sociedad civil y cooperación internacional, que garantizará coherencia interinstitucional, transparencia y legitimidad democrática en las decisiones estratégicas. • **Centro Nacional de Ciberseguridad (CNC).** Unidad técnica que operará el CERT nacional, emitirá estándares de seguridad digital, apoyará a los dos entes en respuesta a incidentes y formación de capacidades. Se inspira en modelos como el INCIBE (España) o el CSIRT-CR (Costa Rica).
3. Reforma del marco normativo	• **Ley de Transformación Digital del Estado.** Establecerá principios de interoperabilidad, protección de datos personales, estándares digitales obligatorios y disposiciones sobre ciberseguridad aplicables a los servicios públicos, garantizando coherencia con los ODS, marcos de la OCDE y buenas prácticas internacionales. • **Ley de Protección de Infraestructuras Críticas.** Definirá responsabilidades institucionales, criterios de clasificación, requisitos mínimos de seguridad y planes sectoriales obligatorios. Incluirá elementos de ciberseguridad aplicados a infraestructuras críticas, sin requerir una ley adicional específica. **Nota:** se plantea que ambas leyes incluyan los elementos de ciberseguridad según corresponda, sin embargo podrá optarse por desarrollar una Ley específica en Ciberseguridad.

Las propuestas planteadas responden directamente a las limitaciones estructurales, normativas y operativas que enfrenta Guatemala, y se basan en lecciones aprendidas de países con trayectorias exitosas en transformación digital y protección de infraestructuras críticas. A continuación, se justifica cada componente clave con base en desafíos identificados:

1. **Brecha digital estructural.** La brecha digital en Guatemala es un obstáculo crítico para el desarrollo inclusivo. Esta disparidad limita el acceso a educación, salud y servicios públicos digitales, perpetuando desigualdades socioeconómicas. La creación de la Agencia Nacional de Transformación Digital (ANTD) responde a esta problemática al centralizar y priorizar políticas de inclusión digital, enfocándose en conectividad rural, alfabetización digital y acceso equitativo a plataformas públicas. Ejemplos como Costa Rica, donde el programa "Comunidades Conectadas" logró que el 95% de las escuelas tengan internet de banda ancha, o Uruguay, con su Plan Ceibal que asegura conectividad y dispositivos en el 91% de los hogares, demuestran que una entidad especializada con un mandato claro puede articular recursos y políticas para cerrar brechas. La ANTD, al coordinar esfuerzos entre el gobierno, el sector privado y la cooperación internacional, podría implementar programas similares, como subsidios para infraestructura en zonas rurales o alianzas con proveedores de telecomunicaciones, garantizando un impacto sostenible y medible en la inclusión digital.

2. **Vulnerabilidad de infraestructura crítica.** Las infraestructuras críticas de Guatemala, como puertos, redes eléctricas y sistemas de transporte son altamente vulnerables a ciberataques, desastres naturales y fallos operativos, en parte debido a la falta de un marco coordinado de protección. Por ejemplo, el puerto de Quetzal, clave para el comercio regional, ha enfrentado interrupciones por fallos técnicos y desastres climáticos. El Esquema Nacional de Protección de Infraestructuras Críticas (ENPIC) aborda esta vulnerabilidad al establecer un sistema de identificación, monitoreo y protección de activos estratégicos, articulando esfuerzos con entidades como INSIVUMEH (para riesgos climáticos) y operadores públicos/privados. Modelos internacionales, como el

Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) en España, que coordina la ciberseguridad de sectores clave, o la Agencia Nacional de Ciberseguridad e Infraestructura (ANCI) en Chile, que protege redes energéticas y de transporte, muestran que una gestión especializada reduce riesgos y mejora la resiliencia. En Guatemala, el ENPIC podría priorizar la modernización de sistemas SCADA en energía o la implementación de protocolos de ciberseguridad en puertos, fortaleciendo la seguridad nacional y la continuidad operativa.

3. **Limitaciones institucionales.** Las instituciones guatemaltecas enfrentan restricciones técnicas y humanas que limitan su capacidad para liderar procesos complejos de transformación digital. El CIV, SEGEPLAN o la GAE, por ejemplo, carecen del expertise necesario en ciberseguridad o interoperabilidad digital, lo que genera cuellos de botella en la ejecución de proyectos. Separar funciones mediante la creación de entidades especializadas, como la ANTD y el ENPIC, permite asignar mandatos claros a organismos con personal técnico capacitado, evitando la sobrecarga de instituciones con prioridades múltiples. Este enfoque ha sido exitoso en Costa Rica, donde el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) delega tareas técnicas a entidades como el ICE para conectividad, o en España, donde el Instituto Nacional de Ciberseguridad (INCIBE) se enfoca exclusivamente en ciberseguridad. En Guatemala, esta separación incrementaría la eficiencia, permitiendo que instituciones específicas como la ANTD y el ENPIC lideran la digitalización y la protección de activos críticos.

4. **Débil marco normativo.** El marco legal de Guatemala para la transformación digital y la ciberseguridad es fragmentado y obsoleto, careciendo de regulaciones específicas sobre interoperabilidad, protección de datos o ciberseguridad en infraestructuras críticas. Esto genera inseguridad jurídica para inversionistas y operadores, además de exponer al país a riesgos crecientes de ciberataques (como el aumento global de ransomware, que creció un 80% entre 2020 y 2023 según Chainalysis). Inspirándose en marcos robustos como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, la Ley de Ciberseguridad de Chile o la Ley de Protección de Infraestructuras Críticas de España, Guatemala necesita leyes que establezcan estándares claros de ciberseguridad, interoperabilidad entre sistemas gubernamentales y protección de datos personales. Estas normas no solo fortalecerían la confianza en los servicios digitales, sino que también facilitarían la atracción de inversión extranjera en tecnología, al garantizar un entorno regulatorio predecible y alineado con estándares internacionales.

5. **Necesidad de transparencia y control democrático.** La baja confianza en las instituciones públicas guatemaltecas, agravada por casos de corrupción y falta de rendición de cuentas, exige mecanismos que garanticen legitimidad y participación ciudadana en la transformación digital. El Consejo Nacional de Ciberseguridad y Digitalización, con representación de gobierno, sector privado, academia y sociedad civil, responde a esta necesidad al promover un enfoque multisectorial y transparente. Este modelo, inspirado en organismos como el Consejo Nacional de Ciberseguridad de España o el Consejo Consultivo de Transformación Digital de Chile, asegura que las políticas digitales reflejen las necesidades de diversos actores y estén sujetas a escrutinio público. En Guatemala, el Consejo podría supervisar la implementación de la ANTD y el ENPIC, publicar informes de progreso y organizar foros ciudadanos, fortaleciendo la legitimidad de las iniciativas en un contexto de escepticismo institucional.

6. **Recursos financieros y humanos limitados.** Guatemala enfrenta restricciones presupuestarias y una escasez de profesionales capacitados en ciberseguridad y

tecnologías digitales, lo que limita la implementación de proyectos de transformación digital. El Centro Nacional de Ciberseguridad (CNC) aborda este desafío al desarrollar capacidades nacionales mediante programas de formación especializada en ciberseguridad, protección de infraestructuras críticas y gestión de sistemas digitales. Este enfoque reduce la dependencia de consultorías externas, que suelen ser costosas y no siempre se adaptan al contexto local. Por ejemplo, países como Colombia han implementado iniciativas como "Talento Digital", formando a 100,000 personas en habilidades tecnológicas entre 2020 y 2023, lo que demuestra el impacto de invertir en capital humano local. Además, el CNC puede fomentar la cooperación internacional, aprovechando alianzas con organismos internacionales, y promover alianzas público-privadas para financiar infraestructura y transferencia tecnológica. Estas estrategias garantizarán la sostenibilidad financiera y técnica de las iniciativas de transformación digital, fortaleciendo la resiliencia de Guatemala frente a amenazas cibernéticas y operativas.

Estas recomendaciones están diseñadas para ser implementables, escalables y sostenibles, permitiendo a Guatemala avanzar hacia una transformación digital inclusiva, segura y soberana, sin comprometer la protección de los activos que sustentan su seguridad, economía y desarrollo.

Listado de Acrónimos y Significados

Acrónimo	Significado
ADIP	Agencia Digital de Innovación Pública (México)
AGESIC	Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Uruguay)
ANA	Autoridad Nacional del Agua (Perú)
ANCI	Agencia Nacional de Ciberseguridad (Chile)
ANTD	Agencia Nacional de Transformación Digital (propuesta para Guatemala)
AR-CERT	Equipo de Respuesta ante Emergencias Informáticas de Argentina
CENACE	Centro Nacional de Control de Energía (México)
CERT	Computer Emergency Response Team
CERTuy	Equipo de Respuesta ante Incidentes de Seguridad Informática de Uruguay
CISA	Cybersecurity and Infrastructure Security Agency (EE.UU.)
CCOC	Comando Conjunto Cibernético (Colombia)
CNC	Centro Nacional de Ciberseguridad (propuesta para Guatemala)
CNPIC	Centro Nacional de Protección de Infraestructuras Críticas (España)
CONRED	Coordinadora Nacional para la Reducción de Desastres (Guatemala)
CSIRT	Computer Security Incident Response Team
CSIRTmx	Equipo CSIRT de México
CSIRT-CR	Equipo CSIRT de Costa Rica
EGDI	E-Government Development Index
ENPIC	Ente Nacional de Protección de Infraestructuras Críticas (propuesta para Guatemala)
IDF	Israel Defense Forces (Fuerzas de Defensa de Israel)
INCIBE	Instituto Nacional de Ciberseguridad (España)
INCD	Dirección Nacional de Ciberseguridad (Israel)
INIFED	Instituto Nacional de Infraestructura Física Educativa (México)
INSIVUMEH	Instituto Nacional de Sismología, Vulcanología, Meteorología e Hidrología (Guatemala)
KSI	Keyless Signature Infrastructure (Estonia)
MCI	Ministry of Communications and Information (Singapur)
MICITT	Ministerio de Ciencia, Tecnología y Telecomunicaciones (Costa Rica)
MinTIC	Ministerio de Tecnologías de la Información y las Comunicaciones (Colombia)
NTIA	National Telecommunications and Information Administration (EE.UU.)
OEA	Organización de los Estados Americanos
OCDE	Organización para la Cooperación y el Desarrollo Económicos
ODS	Objetivos de Desarrollo Sostenible
RIA	Autoridad de Sistemas de Información (Estonia)
SEDIA	Secretaría de Estado de Digitalización e Inteligencia Artificial (España)
SOC	Security Operations Center
SSPC	Secretaría de Seguridad y Protección Ciudadana (México)
TDE	Transformación Digital del Estado
UNGRD	Unidad Nacional para la Gestión del Riesgo de Desastres (Colombia)
UTE	Administración Nacional de Usinas y Transmisiones Eléctricas (Uruguay)
CIV	Ministerio de Comunicaciones, Infraestructura y Vivienda (Guatemala)
CERT-EE	Equipo de Respuesta ante Emergencias Informáticas de Estonia
eIDAS	Electronic Identification, Authentication and Trust Services Regulation (Reglamento de la UE)
GEOPERÚ	Plataforma de servicios digitales del Gobierno de Perú
Mi Argentina	Plataforma digital de servicios ciudadanos en Argentina
Participa Perú	Plataforma de participación ciudadana digital en Perú
Smart Nation	Iniciativa nacional de digitalización de Singapur
Singpass	Sistema nacional de identidad digital en Singapur
Llave CDMX	Plataforma de identidad digital y trámites en línea en Ciudad de México
Plan España Digital 2025	Estrategia nacional de digitalización de España
UE	Unión Europea