# Análisis de necesidades de fortalecimiento tecnológico

## PLATAFORMA TECNOLÓGICA INTEROPERABLE DEL SISTEMA NACIONAL DE SEGURIDAD

La Secretaría Técnica del Consejo Nacional de Seguridad como órgano técnico, profesional y especializado, y en su función de mantener activos los mecanismos de comunicación e intercambio de información del Sistema Nacional de Seguridad, y en el marco de los instrumentos de Seguridad de la Nación, desarrolla el proyecto de la Plataforma Tecnológica Interoperable del Sistema Nacional de Seguridad.

## ANTECEDENTES

La transformación digital en el gobierno ha sido una prioridad en diversos países de la región, considerando los avances en los sistemas de e-Gobierno, que es un mecanismo que demuestra un compromiso hacia la mejora de los procesos que se llevan a cabo en las instituciones públicas. El Gobierno de Guatemala, ha tomado decisiones que apoyan el fortalecimiento de instituciones por medio de portales tecnológicos que fomenten la participación ciudadana, impulsando la adhesión a la Alianza para el Gobierno Abierto en 2011. Al respecto, las instituciones fueron comprometidas a buscar mecanismos que faciliten el intercambio de información para producir conocimiento y auditar sus procesos.

La Organización de Estados Americanos (OEA) bajo el cargo del Departamento para la Gestión Pública Efectiva (DGPE) y la Secretaría de Asuntos Hemisféricos, publicaron en el año 2016 el informe sobre la Situación y Retos del Gobierno Abierto en Guatemala en donde se detalla el análisis que se llevó a cabo para mejorar las prácticas de traslado de información y comunicación entre instituciones. Resultando lo anterior, en recomendaciones para la implementación efectiva de una estrategia de datos abiertos, dentro de las cuales se encuentra la necesidad de crear sistemas interoperables entre las instituciones del Estado, indicando que existen algunas en Guatemala como lo son SICOINGL, Guatecompras, SNIP, SIGES o GuateNóminas; no obstante, sigue existiendo la necesidad de abarcar más campos de acción tales como la seguridad, ambiente, procesos electorales, etc. Lo anterior permite establecer un precedente en cuanto a la transformación tecnológica que está sufriendo el Gobierno de Guatemala.

Bajo el tema de la seguridad, la Ley Marco del Sistema Nacional de Seguridad del año 2008 promueve la creación de mecanismos de comunicación entre instituciones miembros del Sistema Nacional de Seguridad (SNS) asignando esta función a la Secretaría Técnica del Consejo Nacional de Seguridad (STCNS) la cual, desde su institucionalización en 2012 ha trabajado en la creación, mantenimiento, alimentación y mejora continua de una Plataforma de Monitoreo y Estadística con

objetivo de contar con una herramienta centralizadora de datos para generar información que proporcione valor para la toma de decisiones del Consejo Nacional de Seguridad (CNS).

Dicha plataforma tecnológica ha coadyuvado a las funciones de la STCNS proporcionando un panorama certero de la situación de Guatemala con información estadística, gráficas, mapas de calor y capas situacionales para correlación de variables en materia de seguridad abarcando tres ámbitos de Seguridad de la Nación: Seguridad Interior, Seguridad Exterior, y Gestión de Riesgos.

La STCNS en el marco del Cuarto Plan Nacional de Gobierno Abierto asume el compromiso del fortalecimiento de la coordinación interinstitucional y fomento de la transparencia y la participación ciudadana en el sector seguridad. Se propone la creación de marcos de trabajo y establecimiento de estándares para sistemas interoperables dentro del SNS basado en la experiencia de otros países y regiones del mundo donde la integración de sistemas informáticos ha resultado en beneficio del gobierno y la transparencia. Se cuenta como precedente los esfuerzos de la Unión Europea que, a través de investigaciones exploratorias sobre modelos de gobernanza emergentes basados en las tecnologías de información desarrolló un Marco de Interoperabilidad para instituciones públicas que presentaba las normas y directrices en el intercambio de información y conocimiento, debiendo respetar las cualidades básicas de los datos tales como ser: Primarios, Accesibles, Completos, Procesables por máquinas y No discriminados. Este marco proporciona un modelo de referencia que se pretende trasladar, adaptar y replicar para el SNS.

## CONDICIÓN DE NECESIDAD

El análisis realizado para la construcción del Libro Blanco de Seguridad, permitió identificar las principales expresiones de los desafíos que enfrenta el Estado en materia de seguridad; entre ellos, se identifica la investigación científica y tecnológica, específicamente en cuanto a la sistematización y optimización de la tecnología para la seguridad, desarrollar programas de investigación con estándares internacionales e implementar plataformas tecnológicas.

Asimismo, la visión de futuro, tazada en dicho instrumento plantea la disponibilidad funcional de oferta tecnológica como un producto de seguridad, derivado de la inversión en los componentes técnicos y organizativos que intervienen en la gestión y estrategia de seguridad.

La interoperabilidad de tecnologías y sistemas de información es necesaria para coadyuvar a la institucionalidad de procesos y la integración de capacidades de las

instituciones que conforman el Sistema Nacional de Seguridad, en la toma de decisiones, así como en el diseño y gestión de programas mayores de seguridad, para obtener los resultados previstos con los menores costos de transacción.

La caracterización político-estratégica de la Política Nacional de Seguridad, expresa que el uso de la tecnología en el ámbito de seguridad, es fundamental para mejorar las capacidades institucionales de prevención y respuesta. Se constituye en una herramienta que al hacerla interoperable, favorece la coordinación, colaboración y cooperación para la identificación y evaluación de los riesgos, amenazas y vulnerabilidades a la Seguridad de la Nación, facilitando la toma de decisiones en función de la seguridad y el desarrollo.

Bajo la perspectiva del Programa Estratégico de Gestión Integral de la Seguridad de la Nación (GISEG), la Política Nacional de Seguridad comunica la importancia del fortalecimiento de las capacidades y competencias sistémicas de las instituciones que conforman el Sistema Nacional de Seguridad, para generar una adecuada actuación interinstitucional, mejorar los procesos de decisión y la calidad de respuesta a la formación dinámica de necesidades de seguridad.

Por su parte, la Estrategia Nacional de Seguridad Cibernética reconoce que la dependencia de plataformas digitales y la necesidad de mecanismos de intercambio de información de manera rápida y segura, hacen que garantizar la disponibilidad, integridad y confidencialidad de las mismas se convierta en una prioridad nacional. De igual forma, identifica la necesidad de fortalecer los mecanismos de colaboración, cooperación y coordinación intersectorial, requeridos para para asegurar la plena integración tecnológica en los ámbitos de funcionamiento del Sistema Nacional de Seguridad.

En el Cuarto Plan de Acción Nacional de Gobierno Abierto, se asume el compromiso de “Fortalecer la coordinación interinstitucional y fomentar la transparencia y la participación ciudadana en el sector seguridad.” Al respecto, entre los hitos relativos a dicho compromiso, se comprende el “Fortalecimiento de las unidades de informática y tecnología para desarrollar y optimizar las plataformas tecnológicas institucionales interoperables del sector seguridad”.

## DIAGNÓSTICO DE BRECHAS TECNOLÓGICAS EN EL SISTEMA NACIONAL DE SEGURIDAD

La condición de necesidad planteada anteriormente hace importante analizar el estado actual de las capacidades tecnológicas de las instituciones que conforman el Sistema Nacional de Seguridad, en lo relacionado a criterios de interoperabilidad entre sistemas informáticos. Tiene como objetivo identificar los desafíos que existen realizando para ello un diagnóstico de brechas tecnológicas e

institucionales, analizando un estudio de la información existente proporcionada por cada institución. Para este efecto se evaluaron cuatro características consideradas para la factibilidad del proyecto: infraestructura; políticas y procedimientos; sistemas de información; y estructura organizacional, el análisis de resultados es representado de forma estadística en base a las respuestas de los participantes de la mesa técnica interinstitucional.

La implementación de las Tecnologías de la Información (TIC) dentro de las instituciones públicas logra resultados positivos en cuanto a la mejora de procesos administrativos gubernamentales, reducción de costos y aumento en la eficiencia de los servicios transaccionales que brinda el gobierno para cumplir sus objetivos de nación, así como el aumento de la legitimidad democrática y de la transparencia. La identificación de los factores que han permitido el fortalecimiento de las instituciones a través de medios tecnológicos es vital para llevar a cabo estrategias que logren la integración de estas herramientas para la generación de conocimiento en materia de seguridad, estos factores identificados son: La infraestructura tecnológica manejada por cada institución, la capacidad y conocimiento tecnológico del recurso humano así como la información que procesa

## INFRAESTRUCTURA

La infraestructura tecnológica se entiende como el conjunto de hardware, software y telecomunicaciones que la institución necesita para realizar y apoyar sus operaciones, funciona como base para la gestión y traslado de la información.

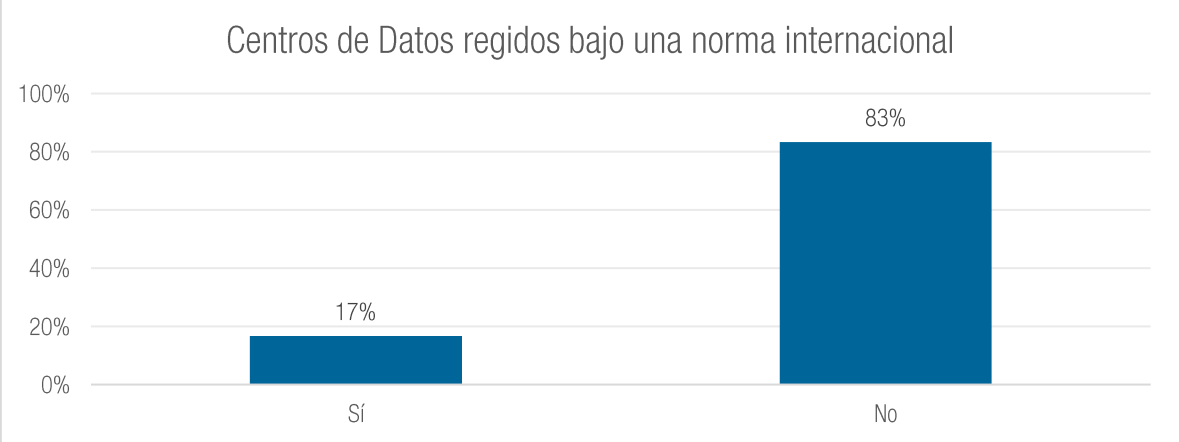
La infraestructura tecnológica para las instituciones públicas en Guatemala no se encuentra regida por ninguna normativa específica en cuanto a tecnologías que debieran utilizarse ni protocolos para la comunicación interna y externa, por lo que se interpreta que cada institución ha sido equipada conforme a su presupuesto y a la dependencia digital en sus procedimientos.

### 1. CENTRO DE DATOS

El centro de datos es un espacio físico tal y como su nombre lo indica es un centro de procesamiento de datos. Esta definición engloba las dependencias y los sistemas asociados gracias a los cuales los datos pueden ser almacenados, tratados y distribuidos.

Para el desarrollo de una plataforma interoperable se han estudiado las capacidades tecnológicas de las instituciones y el vínculo que poseen con el tratamiento de datos estadísticos. Los cuestionamientos planteados en la temática de infraestructura, hacen referencia a servicios tecnológicos implementados en la institución brindando un panorama de los mecanismos apropiados para la comunicación interinstitucional deseada.

A pesar que una gran mayoría de instituciones afirma poseer un Centro de Datos para sus gestiones informáticas, se identifica en este tema una brecha tecnológica ya que mucha de la infraestructura tecnológica de los centros de datos es destinada actualmente a labores administrativas como gestión de ordenadores, telefonía, correo institucional, administración de redes, por tal motivo la generación sistemática de datos estratégicos en materia de seguridad no está ligada directamente al uso del centro de datos, dificultando la gestión para el traslado de información.

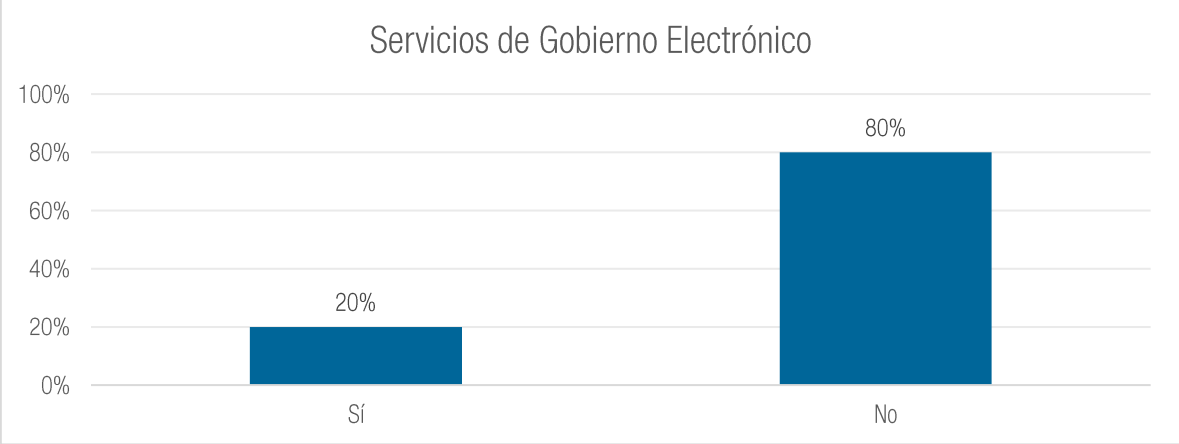



*Instituciones y dependencias del Sistema Nacional de Seguridad*

La anterior gráfica denota la falta de una normativa que estandarice la inversión en tecnología en la administración pública, resultando en un desafío para la implementación de medidas de comunicación efectivas utilizando los sistemas de información.

## 2. GOBIERNO ELECTRÓNICO

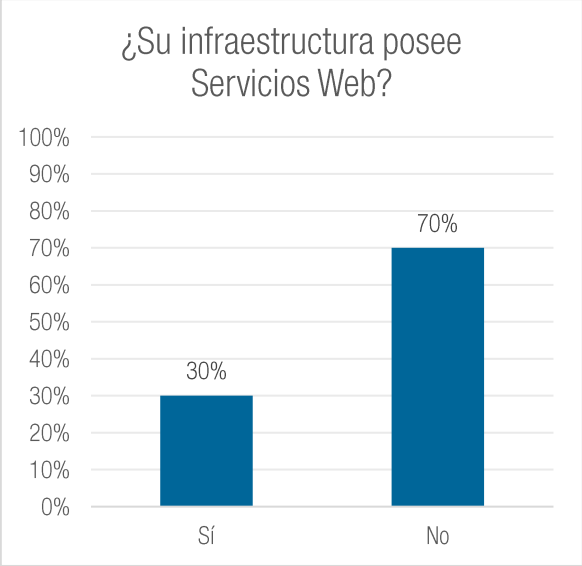
Los servicios de e-Gobierno o Gobierno Electrónico son la aplicación de las tecnologías de la información y la comunicación al funcionamiento del sector público, con el objetivo de brindar mejores servicios al ciudadano e incrementar la eficiencia, la transparencia y la participación ciudadana. Los servicios digitales que una institución pública brinda de forma externa a través de internet señalan facultades de interconexión y la sistematización tecnológica en sus procesos. Sin embargo, dentro del Sistema Nacional de Seguridad el estudio resulta en la existencia de instituciones que no cuentan con las condiciones para el establecimiento, operatividad y funcionalidad del Gobierno Electrónico.

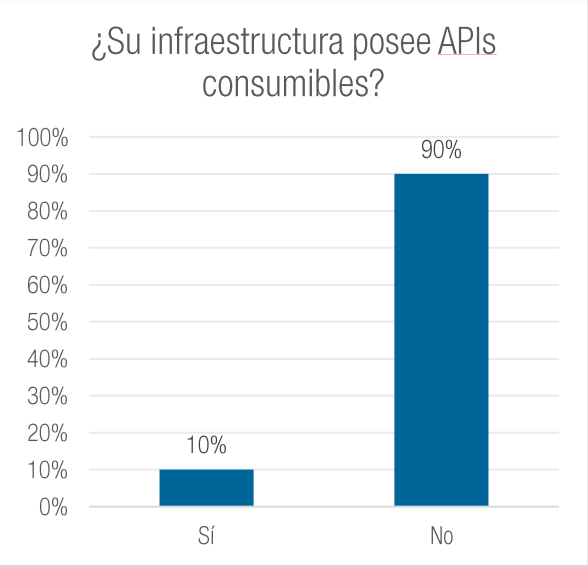



## 3. SERVICIOS WEB

Los Servicios Web son sistemas diseñados para soportar la interoperabilidad máquina-máquina, a través de una red. Este tiene una interfaz que descripta en un formato que puede ser procesado por una máquina. Siendo un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones de software desarrolladas en lenguajes de programación diferentes.

Se han identificado únicamente cuatro instituciones dentro del Sistema Nacional de Seguridad que han desarrollado servicios web para que sean consumibles por otros sistemas de forma interna y externa, siendo esta una brecha que indica la necesidad de dotar de experiencia en el intercambio de información a las unidades de informática respectivas para que sean capaces de brindar la información en la forma que se requiere



El análisis inicial sobre las necesidades de fortalecimiento institucional da como resultado una directriz clara por orientar a los participantes al uso de mecanismos de comunicación tales como los Servicios Web y APIs. La Secretaría Técnica del Consejo Nacional de Seguridad en base a la indicación de los participantes considera que los principales retos que enfrentará el Sistema Nacional de Seguridad para hacer interoperables sus infraestructuras tecnológicas son:

1. Diseñar un catálogo de estándares, entre los cuales se definan las vías de comunicación bidireccional dentro del SNS.
2. Continuación del proyecto con el cambio de gobierno.
3. Fomento del desarrollo tecnológico e inversión para las instituciones.
4. Marco normativo necesario para fundamentar las acciones de centralización de la información para Seguridad de la Nación.

## CONCLUSIÓN

Según la participación en las mesas de discusión acorde a los resultados obtenidos del formulario para diagnóstico de necesidades tecnológicas en las instituciones del sector seguridad, se concluye que se debe priorizar el factor de interoperabilidad entre las instituciones, ya que cada una trabaja de forma independiente según la naturaleza de sus actividades, sin embargo existe una oportunidad de crecimiento tecnológico para este sector de la administración pública, si existe un mecanismo para compartir información de forma fluida y sin trabas burocráticas, de esta manera se podrá tener un amplio panorama de la temática de Seguridad de la Nación en todos sus ámbitos.