Plan de Tecnología, Información y Comunicaciones de la Secretaría de Estado en el Despacho de Seguridad

Tegucigalpa, M.D.C., Marzo de 2024

Elaboración del Documento

Elaborado por:	Cargo	Área de Trabajo	Fecha	Firma
Leonel Canales	Soporte SAP	Departamento Sistema Integrado de Gestión	Marzo 2024	
Nahun Pacheco	Soporte SAP	Departamento Sistema Integrado de Gestión	Marzo 2024	

Revisión del Documento

Revisado por:	Cargo	Área de Trabajo	Fecha	Firma
Msc. Abner Villanueva	Encargado del Sistema Integrado de Gestión	Departamento Sistema Integrado de Gestión	Marzo 2024	

Verificación del Documento

Verificado por:	Cargo	Área de Trabajo	Fecha	Firma
Msc. Mariela García	Coordinadora COCOIN-SEDS	UPEG	Marzo 2024	

Aprobación del Documento

Aprobado por:	Cargo	Área de Trabajo	Fecha	Firma
Dr. Héctor Gustavo Sánchez Velásquez	Secretario de Seguridad	Secretaría de Seguridad	Marzo 2024	

Tabla de contenido Plan de Tecnología, Información y Comunicaciones de la Secretaría de Estado en el Despacho de Seguridad

1. INTRODUCCIÓN

La Secretaría de Seguridad, consciente de la importancia crítica que las Tecnologías de la Información y Comunicación (TIC) desempeñan en la eficacia y eficiencia de las operaciones de seguridad pública, ha desarrollado un plan integral de TIC con el objetivo de modernizar y optimizar sus sistemas y procesos. Este plan estratégico se centra en la adopción de tecnologías avanzadas, la mejora de la infraestructura de TI existente, y la implementación de sistemas de información seguros y resilientes.

Busca no solo fortalecer la capacidad operativa y la respuesta ante incidentes de la Secretaría, sino también promover la transparencia, la colaboración interinstitucional y la confianza pública. Al alinear sus objetivos tecnológicos con las necesidades de seguridad nacional, este plan marca un paso adelante en el compromiso de la Secretaría por proporcionar un entorno más seguro y pacífico para la sociedad, mediante el uso estratégico y efectivo de las TIC.

2. ANTECEDENTES

Para el año 2015 la Secretaría de Seguridad presentaba obsolescencia en sus procesos, controles y tecnología, enfrentándose principalmente a las siguientes situaciones:

a) Información desactualizada, disgregada y centralizada en unas pocas personas que eran indispensables donde se dependía de la disponibilidad de estas para revisar y proporcionar los datos solicitados.
b) Capacidades limitadas para ejecutar reportes personalizados debido a la falta de procesos definidos, desintegrados y desvinculados.
c) La elaboración de informes era tardía, por lo que la toma de decisiones resultaba ineficaz y poco oportuna.
d) Existía una cantidad significante de trabajo manual y duplicación de esfuerzos en procesos básicos.
e) Los sistemas operacionales y financieros no estaban integrados impidiendo obtener datos oportunos y precisos.
f) Y los tiempos de respuesta eran excesivos en la realización de tareas diarias. g) La contabilidad a nivel de Policía Nacional era manejada en programas básicos como Excel y Fox Pro del año 1998 para el pago de nómina.

g) No se aprovechaban las herramientas tecnológicas disponibles en el mercado.

Dichas situaciones evidenciaron la imperante necesidad de modernizar, actualizar y optimizar el sistema administrativo de la Secretaría de Seguridad.

A través de la adquisición e implementación de herramientas tecnológicas confiables y seguras por parte del Sistema Integrado de Gestión (SIG), se ha logrado obtener resultados en los siguientes aspectos:

a) Modernización, simplificación y estandarización de los procesos, tales como: generación de planilla de pago, gestión de compras de bienes y suministros, abastecimiento de combustible, gestión de mantenimientos de flota vehicular, gestión de solicitudes de viáticos, entre otros.
b) Minimizar las interrupciones y maximizar la productividad.
c) Eliminar la duplicidad de funciones y esfuerzos.
d) Fortalecimiento de los mecanismos de Control Interno, registro y monitoreo.
e) Consolidación de la información de la fuerza laboral.
f) Generación de información precisa, oportuna y actualizada en tiempo real.
g) Mantenimiento del flujo ininterrumpido de información, ejecución y seguimiento al Plan de Mejora elaborado en cumplimiento del Convenio de Transparencia, para la optimización de los procesos de gestión de resultados, talento humano y compras y contrataciones, a través de la sistematización.

3. OBJETIVOS

- Implementar el uso de nuevas tecnologías informáticas que garanticen la gestión eficiente de los recursos humanos, materiales, presupuestarios y financieros de la Institución.

- Establecer protocolos y procesos que aseguren la correcta administración de los recursos y faciliten la toma de decisiones, garantizando la transparencia y rendición de cuentas.

- Planificar y gestionar los equipos y herramientas tecnológicas e informáticas necesarias para el cumplimiento de los objetivos estratégicos de la Secretaría de Estado en el Despacho de Seguridad.

4. ALCANCE DEL DOCUMENTO

El documento del plan de Tecnologías de la Información y Comunicación (TIC) de la Secretaría de Seguridad establece un marco estratégico integral destinado a revolucionar las operaciones de seguridad a través de la modernización tecnológica. Su alcance se extiende desde la actualización de la infraestructura tecnológica y la implementación de sistemas avanzados de gestión de información y comunicaciones, hasta el fortalecimiento de las medidas de ciberseguridad para proteger datos sensibles y sistemas críticos. Prioriza la capacitación del personal en herramientas tecnológicas emergentes, promoviendo una cultura de innovación y mejora continua.

Este plan es un pilar fundamental en la estrategia de la Secretaría para alcanzar una gestión de seguridad más eficiente, transparente y adaptada a los desafíos contemporáneos.

5. MARCO METODOLÓGICO

El marco metodológico del Plan de Tecnologías de la Información y Comunicación (TIC) de la Secretaría de Seguridad se estructura en torno a un enfoque sistemático y estratégico para la identificación, implementación y gestión de tecnologías críticas que respalden los objetivos de seguridad. Se priorizan proyectos según su impacto en la mejora de la seguridad y la eficiencia operativa. La metodología incluye la planificación detallada de la implementación, con especial énfasis en la gestión del cambio y la seguridad de la información, se asegura una revisión continua y la adaptación de la estrategia de TIC para alinearla con los cambiantes requisitos de seguridad y las innovaciones tecnológicas. Este enfoque garantiza que el Plan de TIC sea dinámico, escalable y capaz de responder efectivamente a las necesidades de la Secretaría de Seguridad.

6. MARCO NORMATIVO

El marco normativo por el cual se rige la Secretaría de Estado en el Despacho de Seguridad (SEDS) se basa en las siguientes leyes:

- Constitución de la República de Honduras
- Ley de Transparencia y Acceso a la Información Pública
- Reglamento de Ejecución General de la Ley Orgánica del Presupuesto

- Ley de Contratación del Estado
- Ley de Procedimiento Administrativos
- Ley Orgánica de la Secretaría de Seguridad y Policía Nacional
- Reglamento General de la Ley Orgánica de la Secretaría de Seguridad y Policía Nacional
- Ley de Administración Pública
- Y otras leyes que apliquen

7. ANÁLISIS DE LA SITUACIÓN ACTUAL

a) Situación actual de la estrategia de las TI

La situación actual de las Tecnologías de la Información (TI) en la Secretaría de Estado en el Despacho de Seguridad (SEDS) y la Policía Nacional de Honduras ha experimentado un notable progreso en los últimos años. Este avance ha sido fundamental para la transformación y modernización de los procesos internos, mejorando significativamente la eficiencia y eficacia en las operaciones de seguridad. La implementación de sistemas de información y la digitalización de procedimientos han permitido una mejor gestión de datos y una respuesta más rápida ante incidentes.

Por otro lado, pese a estos avances, aún persisten desafíos significativos que necesitan atención. La brecha tecnológica entre diferentes áreas y la necesidad de capacitación continua del personal en nuevas tecnologías son aspectos críticos para mantener y mejorar los niveles de seguridad. Además, la ciberseguridad emerge como un campo de atención prioritaria, dado el incremento en la dependencia de las operaciones sobre plataformas digitales, lo que hace imprescindible fortalecer las defensas contra ataques cibernéticos. En este contexto, la SEDS y la Policía Nacional están enfocadas en continuar su camino hacia la innovación tecnológica, asegurando un marco seguro y actualizado que responda de manera efectiva a las demandas de seguridad del país.

b) Impacto del uso y apropiación de las TI

i. Principales actividades llevadas a cabo

- Administración de sistema de recursos empresariales (SAP)
- Administración y control del abastecimiento de combustible mediante RFID y tarjeta con banda magnética
- Desarrollo de aplicaciones
- Gestión del correo electrónico institucional
- Gestión del sitio web institucional
- Gestión de endpoint

ii. Productos o servicios prestados

- Soporte técnico
- Capacitaciones
- Administración de sistemas

iii. Herramientas de TI

- SAP: Sistema de Recursos Empresariales que gestiona e integra los procesos administrativos dentro de la institución; incluyendo las áreas de presupuesto, finanzas, compras, almacenes, recursos humanos.
- Office 365: Suite de programas de ofimática que incluye cuenta de correo electrónico institucional.
- Kaspersky Security Cloud Endpoint: Herramienta para brindar seguridad a los equipos de cómputo de la SEDS.
- Eset Nod Endpoint: Herramienta para brindar seguridad a los equipos de cómputo de la Policía Nacional.
- Servidores de almacenamiento y programas
- Equipo de infraestructura de redes

iv. Actividades sin apoyo de las TI

- Gestión documental del Archivo General

v. Perfil del directivo frente a las TI

El perfil del directivo frente a las Tecnologías de la Información (TI) debe reflejar una combinación de habilidades técnicas, de gestión y estratégicas que le permitan liderar eficazmente en un entorno tecnológicamente avanzado y en constante cambio. A continuación, se enumeran algunas de las características esenciales que debería poseer:

- **Visión estratégica**: Capacidad para entender cómo las TI pueden servir como un habilitador estratégico para lograr los objetivos de la institución.

- **Liderazgo y habilidades de gestión**: Aptitud para liderar equipos multidisciplinarios, gestionar proyectos tecnológicos complejos y fomentar un ambiente de trabajo colaborativo e innovador.

- **Comprensión técnica**: Aunque no necesariamente sea un experto en todos los aspectos técnicos, debe poseer una sólida comprensión de las tecnologías clave que impactan a su organización y la capacidad para tomar decisiones informadas sobre inversiones en TI.

- **Habilidades de comunicación**: Capacidad para comunicarse con las partes interesadas, incluyendo personal técnico y administrativo.

- **Gestión del cambio**: Habilidad para liderar y gestionar el cambio organizacional provocado por la implementación de nuevas tecnologías, minimizando resistencias y maximizando la adopción y el valor aportado.

- **Conciencia sobre ciberseguridad**: Entendimiento profundo de los riesgos de seguridad cibernética y la importancia de implementar políticas y prácticas robustas para proteger los activos de información de la organización.

- **Pensamiento analítico y resolución de problemas**: Capacidad para analizar datos y tendencias complejas para tomar decisiones basadas en evidencias, identificando soluciones efectivas a procesos a través del uso de TI.

- **Aprendizaje continuo**: Compromiso con la actualización constante en conocimientos tecnológicos, tendencias de la industria y prácticas de gestión, para adaptarse a la evolución del entorno digital.

- **Ética y responsabilidad social**: Comprensión de la importancia de gestionar las TI de manera ética y socialmente responsable, considerando la privacidad de datos, la inclusión digital y el impacto ambiental de las tecnologías.

vi. Recursos dedicados a las TI (humanos, financieros y tecnológicos)

- **Recurso Humano**: Se cuenta con el Departamento del Sistema Integrado de Gestión y la Dirección Policial de Telemática, para cumplir con los requerimientos de TI de la institución.

- **Recurso Financiero**: Dada la naturaleza sensible de la información manejada por nuestra institución, su divulgación queda estrictamente restringida para asegurar la integridad y seguridad tanto de nuestras operaciones como del personal involucrado. Esta medida obedece a protocolos de confidencialidad y seguridad nacional, esenciales para preservar los intereses y bienestar colectivo, garantizando así el cumplimiento de nuestras responsabilidades y misiones institucionales de forma segura y efectiva.

- **Recurso tecnológico**: Entre los años 2023 y 2024 se realizó la adquisición del siguiente equipo tecnológico:
  - 40 computadoras portátiles
  - 248 computadoras de escritorio
  - 36 impresoras de flujo continuo

- 200 unidades de sistema de alimentación ininterrumpida (UPS)

c) Situación actual de los SI

i. Sistemas de apoyo

Se cuenta con algunos sistemas de apoyo, tales como:

- **SIAFI**: el Sistema de Administración Financiera Integrada (SIAFI) es un conjunto de subsistemas y módulos informáticos integrados, para la planificación, gestión y control de los recursos del Estado.

- **SIREP**: el Sistema de Registro y Control de Servidores (SIREP) es una herramienta informática cuyo fin es lograr un registro de datos del recurso humano de la administración pública.

- **Pagos en Línea ACH**: realizar pagos a proveedores.

- **DET-Live**: Plataforma de Declaración Electrónica de Tributos que permite elaborar las declaraciones juradas y otros documentos fiscales.

- **Sistema de Información de Planificación SEDS**: es un sistema creado a la medida para la UPEG, donde se registran los datos de producción física de las cadenas de valor.

ii. Sistemas misionales

Un sistema misional es un conjunto de procesos y tecnologías de información diseñados específicamente para apoyar la misión principal de una organización.

- **Sistemas misionales de gestión**

    1. **SAP**: Sistema de Planificación de Recursos Empresariales, por medio del cual se integra y se gestiona la parte financiera, presupuestaria, contable, compras, almacenes, logística, transporte y recursos humanos de la institución.

- **Sistemas misionales de prestación**

    1. **NACMIS**: Registro y control de casos, utilizado por la Policía Nacional

    2. **IBIS**: Registro y control de armas balísticas

    3. **AFIS**: Registro de huellas dactilares, utilizado por los entes investigativos de la Policía Nacional

- **Servicios de información digital, incluidos los portales**

    1. **Página web de la Secretaría de Estado en el Despacho de Seguridad**: www.seguridad.gob.hn

    2. **Página web de la Policía Nacional de Honduras**: www.policianacional.gob.hn

    3. **SEPOL**: el Sistema Estadístico Policial en Línea (SEPOL) es un sistema estadístico de acceso inmediato y publico que pertenece a la Policía Nacional de Honduras, donde se registra la incidencia delictiva y el accionar policial, con la finalidad de brindar datos confiables que sirvan como insumo para la elaboración de análisis, estudios e investigaciones, www.sepol.hn

iii. Sistemas de direccionamiento estratégico

1. **SIGPRET**: el Sistema de Gerencia Pública por Resultados y Transparencia es una herramienta de la Dirección de Gestión por

Resultados que apoya la toma de decisiones, realizando tanto el monitoreo como la evaluación de los resultados y logros alcanzados, mediante la identificación temprana de las fortalezas o debilidades institucionales, sectoriales y de impacto, a través de la medición objetiva del cumplimiento de las metas.

2. **Portal Único de Transparencia**: es una plataforma tecnológica gratuita, creada por el Instituto de Acceso a la Información Pública (IAIP) para facilitar a las personas el ejercicio del derecho de acceso a la información completa, veraz, adecuada y oportuna que generan las instituciones que manejan fondos públicos, en los términos definidos por la Ley de Transparencia en sus artículos 4 y 13.

3. **SIELHO**: el Sistema de Información Electrónico de Honduras (SIELHO), es un mecanismo orientado para el manejo de las solicitudes de información e interponer recursos de revisión en línea.

4. **SEN**: el Sistema Estadístico Nacional (SEN) tiene la responsabilidad de recopilar, procesar, analizar y difundir información estadística relacionada con diversos aspectos del país.

d) Situación actual de los servicios tecnológicos

i. Estrategia y gobierno

El departamento Sistema Integrado de Gestión (SIG) es la plataforma administrativa que consolida los recursos humanos, logísticos y financieros para su debido control, con el propósito de transparentar y hacer mas eficientes todos los procesos administrativos de la Secretaría de Estado en el Despacho de Seguridad y la Policía Nacional, mediante la aplicación de tecnologías de información.

La Dirección Policial de Telemática es la responsable de direccionar, asesorar y promover la implementación, administración y soporte de los sistemas de telecomunicaciones e informática de la Policia Nacional, con el fin de establecer políticas y procesos que conduzcan al mejoramiento

en la utilización de las herramientas tecnológicas en la prestación de los servicios policiales.

ii. Administración de sistemas de información

El departamento del Sistema Integrado de Gestión es el encargado de gestionar los usuarios del sistema SAP, creando y asignando roles según las competencias laborales y funciones a realizar por cada empleado, según sea su asignación organizativa; igualmente se lleva un control de los usuarios que muestran un periodo de inactividad dándoles de baja del sistema, con el fin de llevar un control sobre las personas que tienen acceso a la información.

De igual forma, en este departamento se encuentra el gestor institucional de usuarios SIAFI, que se encarga de gestionar la creación de usuarios solicitados por las demás dependencias de la institución, así como la solicitud de modificación de perfiles, cancelación y solicitud de reinicio de contraseñas.

También se administran las cuentas de Microsoft 365, Kaspersky Security Cloud Plus Endpoint. Y se administra el dominio seguridad.gob.hn

La Dirección Policial de Telemática se encarga de administrar los usuarios de los sistemas: NACMIS y SEPOL. Además del dominio policianacional.gob.hn

iii. Infraestructura

El departamento del Sistema Integrado de Gestión responsable de administrar y gestionar la infraestructura tecnológica para apoyar los procesos de las demás áreas de la institución, para el almacenaje de información, servidores de aplicaciones o archivos, bases de datos y demás canales de comunicación.

iv. Conectividad

La Dirección Policial de Telemática cuenta con el departamento de Conectividad, que es el encargado de velar por la conexión a internet en todas las unidades y departamentos de la Secretaría de Estado en el Despacho de Seguridad y la Policía Nacional, con el fin de garantizar un acceso ininterrumpido a nivel nacional, para poder cumplir con la alta disponibilidad de todos los servicios.

v. Servicios de operación

En el ámbito de Tecnologías de la Información (TI), los servicios de operación se refieren a las actividades y procedimientos diarios necesarios para gestionar y mantener la infraestructura tecnológica de una organización en funcionamiento óptimo. Estos servicios son cruciales para asegurar que todos los sistemas, aplicaciones, redes y servicios de TI apoyen de manera efectiva los procesos empresariales y satisfagan las necesidades de los usuarios finales. Tales como:

- **Gestión de incidentes**: Se enfoca en la restauración rápida de los servicios de TI después de una interrupción, minimizando el impacto negativo en las operaciones de la institución.

- **Gestión de problemas**: Busca identificar y resolver las causas raíz de uno o más incidentes para prevenir su recurrencia.

- **Gestión de cambios**: Proceso para asegurar que todos los cambios en la infraestructura de TI se realicen de manera controlada, minimizando el riesgo de impactar negativamente la disponibilidad y calidad de los servicios.

- **Cumplimiento y seguridad**: Incluye la implementación y el monitoreo de políticas de seguridad para proteger los datos y los sistemas de TI contra accesos no autorizados, ataques cibernéticos y otras amenazas.

- **Soporte técnico y mesa de ayuda**: Proporciona asistencia directa a los usuarios finales para resolver incidencias y problemas relacionados con el uso de los servicios y recursos de TI.

vi. Mesa de servicios especializados

En el departamento de Sistema Integrado de Gestión se cuenta con personal capacitado y certificado en los diferentes módulos de SAP, mismos que se encargan de dar soporte de nivel 1 a los usuarios a nivel nacional, así como de realizar las configuraciones necesarias en el sistema para cumplir con las necesidades que surjan en el día a día.

De igual forma, la Dirección Policial de Telemática cuenta con un departamento de soporte técnico para atender las necesidades de los funcionarios a nivel nacional.

e) Situación actual de la gestión de la información

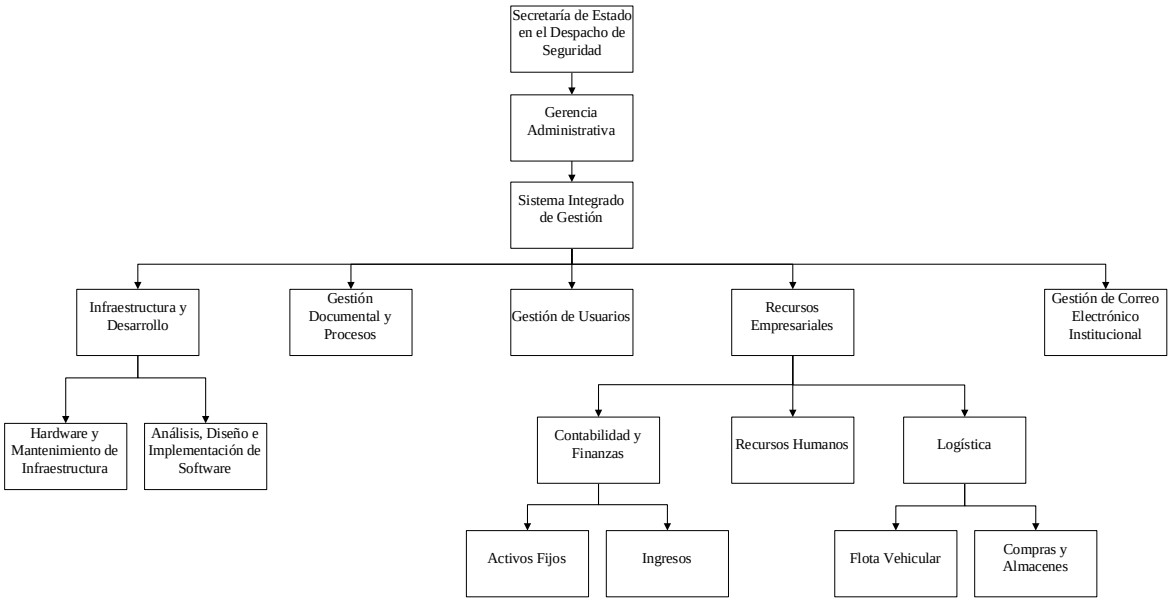
La situación actual de la gestión de la información en la Secretaría de Seguridad y Policía Nacional enfrenta desafíos complejos y dinámicos, enmarcados por la creciente necesidad de adaptarse a las tecnologías avanzadas y a las cambiantes demandas de seguridad. En este contexto, la institución se esfuerza por mejorar sus sistemas de información y comunicación para garantizar una gestión eficaz y eficiente de los datos críticos relacionados con la seguridad pública.

La implementación de plataformas tecnológicas modernas y la integración de bases de datos interinstitucionales son pasos clave para fortalecer la capacidad de respuesta ante el crimen y mejorar la coordinación entre diferentes entidades gubernamentales. Sin embargo, persisten retos significativos en términos de ciberseguridad y la necesidad de capacitación continua del personal para manejar tecnologías emergentes.

A pesar de estos desafíos, la Secretaría de Seguridad y Policía Nacional avanza hacia una gestión de la información más robusta y segura, lo que es fundamental para la prevención del delito y la protección de la ciudadanía.

f) Situación actual del gobierno de las TI (estructura organizacional y talento humano)

Organigrama del Departamento Sistema Integrado de Gestión



g) Análisis financiero del área de TI

Dada la naturaleza sensible de la información manejada por nuestra institución, su divulgación queda estrictamente restringida para asegurar la integridad y seguridad tanto de nuestras operaciones como del personal involucrado. Esta medida obedece a protocolos de confidencialidad y seguridad nacional, esenciales para preservar los intereses y bienestar colectivo, garantizando así el cumplimiento de nuestras responsabilidades y misiones institucionales de forma segura y efectiva.

8. ENTENDIMIENTO ESTRATÉGICO

a) Modelo operativo de la organización

i. Análisis del entorno

Análisis de factores internos y externos que intervienen en la operatividad de la institución:

Fortalezas

- Experiencia y conocimiento especializado: La Secretaría cuenta con personal experimentado en seguridad y aplicación de la ley, acumulando un conocimiento profundo sobre las dinámicas de seguridad locales.
- Cobertura nacional: Posee una amplia presencia en todo el territorio, lo que le permite responder a incidentes en diversas ubicaciones.
- Apoyo internacional: Recibe apoyo, en términos de financiamiento y entrenamiento, de organismos internacionales y países cooperantes en la lucha contra el crimen organizado.

Oportunidades

- Tecnologías emergentes: La adopción de nuevas tecnologías, como sistemas de vigilancia avanzados y software de análisis de datos, ofrece la posibilidad de mejorar la eficiencia y efectividad en la prevención y combate al crimen.
- Colaboración interinstitucional: Fortalecer las alianzas con otras entidades gubernamentales, organizaciones no gubernamentales y la sociedad civil puede mejorar la inteligencia de seguridad y la eficacia de las operaciones.
- Iniciativas de reforma: Existen oportunidades para implementar reformas estructurales que mejoren la eficacia, transparencia y rendición de cuentas de la institución.

Debilidades

- Limitaciones de recursos: Restricciones presupuestarias y falta de equipamiento moderno pueden limitar la capacidad de respuesta y operación.
- Percepción pública y confianza: Desafíos en la percepción pública y la confianza hacia la policía debido a acusaciones de corrupción y abusos en el pasado.
- Formación y retención de personal: Dificultades en la atracción, formación y retención de personal calificado, especialmente ante desafíos de seguridad complejos.

Amenazas

- Crimen organizado y narcotráfico: Honduras enfrenta desafíos significativos relacionados con el crimen organizado, incluido el narcotráfico, que amenazan la seguridad y estabilidad.
- Corrupción e infiltración: La corrupción y la posible infiltración de criminales en las fuerzas de seguridad representan riesgos serios para la integridad y efectividad de la institución.
- Cambio político y estabilidad institucional: Cambios en el entorno político pueden influir en la estabilidad y dirección estratégica de la Secretaría, afectando su capacidad para implementar políticas de largo plazo.

ii. Estrategia institucional

El Plan Estratégico Institucional define el curso de acción que la institución debe seguir en el mediano y largo plazo para cerrar la brecha entre la situación actual y la situación deseada, es decir la visión, en el marco de su misión y los valores institucionales.

A razón de lo anterior, la Secretaría de Seguridad y Policía Nacional han replanteado su visión para el año 2030, la cual permitirá garantizar una mejora sustancial en la reducción de la incidencia criminal en el país. La eficiencia en el uso de los recursos, la transparencia, la credibilidad nacional e internacional, la reforma institucional, los procesos de reconstrucción, la reducción en los índices de criminalidad son frutos de

la planificación estratégica implementada por las máximas autoridades policiales.

La misión de la Secretaría de Seguridad es: "Somos la institución del Estado que promueve la convivencia, protege la vida y bienes de las personas, mediante la prevención, disuasión y control del delito, con estricto apego a la ley, respeto y garantía de los derechos humanos."

La nueva visión institucional es: "Para el 2030, seremos una institución cercana a la comunidad, profesional, confiable y respetada, que garantice la convivencia y contribuya a posicionar a Honduras entre los países más seguros."

Dicha visión pretende ser alcanzada por medio de seis grandes objetivos estratégicos como ser:

1. Reducir la siniestralidad vial en el país para prevenir pérdidas de vidas, lesiones, discapacidades y daños a la propiedad.

2. Mejorar el perfil profesional de los egresados de las academias policiales para responder a las demandas del servicio policial.

3. Fortalecer el Sistema de Inteligencia Policial para prevenir, disuadir y controlar el delito, así como la violencia.

4. Aumentar la capacidad de respuesta en la investigación criminal para coadyuvar a la disminución de la impunidad.

5. Mejorar la capacidad de prevención, disuasión y control de la violencia, así como el delito para contribuir articuladamente a la seguridad pública.

6. Institucionalizar un Modelo Integral de Gestión por Resultados.

iii. Modelo operativo

El modelo operativo de la Secretaría de Seguridad de Honduras es un marco estratégico que define cómo la institución lleva a cabo sus funciones y actividades para garantizar la seguridad pública en el país. Incluye los siguientes componentes:

- **Misión y visión** (enunciado en el ítem anterior)

- **Objetivos estratégicos** (enunciados en el ítem anterior)

- **Estructura organizativa**: la Secretaría de Seguridad y la Policía Nacional de Honduras se encuentran conformadas por diferentes unidades, departamentos, direcciones y divisiones debidamente jerarquizadas.

- **Procesos y procedimientos**: actualmente la Secretaría de Seguridad y la Policía Nacional se encuentran en proceso de diseñar los manuales de procesos y procedimientos de cada una de sus unidades, con el fin de contar con una base para el actuar policial.

- **Recursos Humanos**: la administración del personal se rige por las leyes del país, incluyendo la Ley de Servicio Civil, la Ley y Reglamento de la Carrera Policial. Así como también se cuenta con centros educativos policiales para la captación de personal operativo a nivel de escala básica y oficiales.

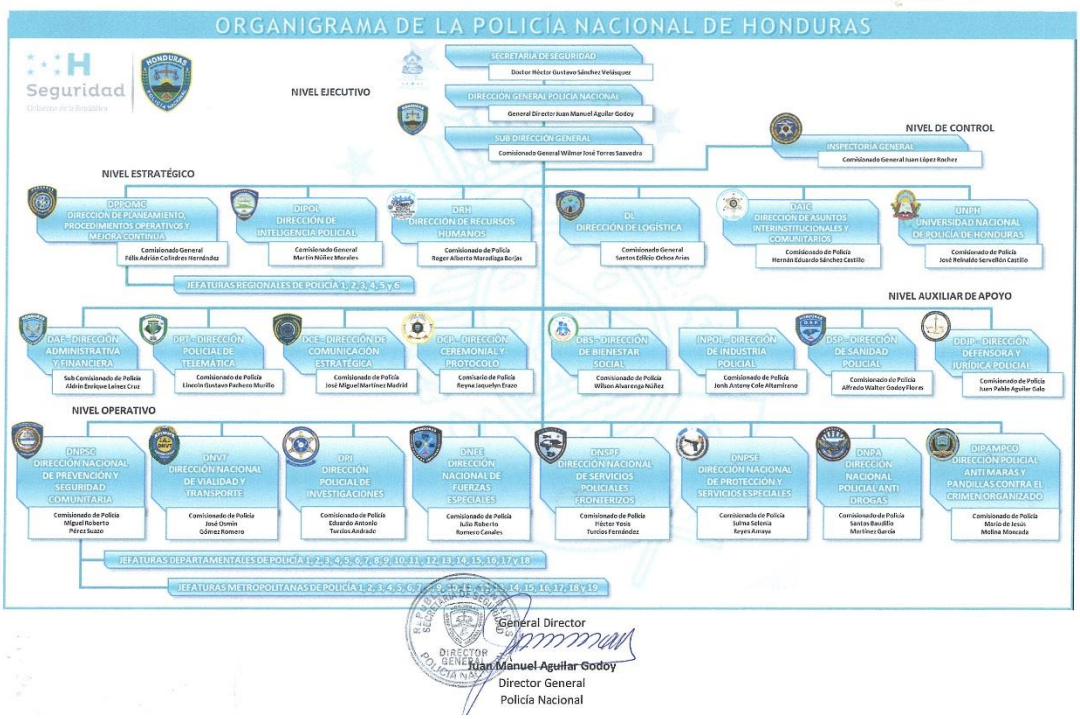
- **Recursos Tecnológicos**: son todos los recursos a nivel de hardware y software con que cuenta la institución. Se incluyen todos los sistemas de apoyo que son de uso interinstitucional con otras entidades del Estado, así como los sistemas adquiridos por la institución y los sistemas desarrollados internamente. Todos ellos con la finalidad de cumplir con los objetivos de la institución.

- **Evaluación y mejora continua**: en el caso de la Policía Nacional se cuenta con la Dirección de Planeamiento, Procedimientos Operativos y Mejora Continua, quienes se encargan de desarrollar los lineamientos operacionales de planeación del servicio policial, a través de estrategias, planes y programas que concentren los componentes de prevención, disuasión y control de los delitos y faltas.

iv. Estructura de la organización

Organigrama de la Secretaría de Estado en el Despacho de Seguridad

Organigrama de la Policía Nacional de Honduras



b) Descripción del flujo y necesidades de información

En la institución varios procesos cuentan con apoyo de las TIC, entre ellos podemos mencionar los siguientes:

1. Creación de número de equipo para un vehículo

   Inicio
   Dirección/Unidad Solicitante
   1. El proceso inicia en la con la solicitud de la creación del número de equipo vía correo electrónico al Sistema Integrado de Gestión por medio del formato FCNE-001.

Sistema Integrado de Gestión (SIG)

2. El Usuario Técnico procede a validar que se haya remitido el número de activo fijo y copia de factura, de no contar con los mismos se notifica a la Dirección de Logística para que pueda remitirla.

3. Una vez se cuenta con la documentación necesaria, el usuario técnico del SIG procede con la actualización del activo fijo en el sistema SAP.

4. Seguidamente se crea el número de equipo y se remite vía correo electrónico a la Dirección/Unidad solicitante.

Dirección de Logística

5. El Departamento de Transporte de la Dirección de Logística procede a elaborar la Boleta de Circulación y entrega el vehículo a la Unidad de Asignación.

Sistema Integrado de Gestión (SIG)

6. Finalmente, el usuario técnico del Sistema Integrado de Gestión procede a instalar la viñeta con el número de equipo y se actualiza el nombre del Conductor en el sistema SAP.

Fin

2. Creación/Modificación de centro logístico y almacén

Inicio
Dirección/Unidad Solicitante

1. La Dirección/Unidad Policial solicita mediante oficio al Departamento de Sistema Integrado de Gestión (SIG) la creación/modificación de centros/almacenes.

Sistema Integrado de Gestión

2. Determina si el requerimiento es procedente. En caso afirmativo, el Usuario Técnico del SIG procede a crear el solicitante de acuerdo al nombre oficial de la Dirección/Unidad.

3. Prosigue a realizar la creación del centro de acuerdo al mismo criterio.

4. Se crea el Almacén y se extienden los materiales de acuerdo a la naturaleza o propósito del mismo.

5. Finalmente, se remite mediante oficio el código de solicitante, centro, Almacén y lista de materiales extendidos a la Dirección/Unidad solicitante.

6. En caso de que la solicitud no sea procedente; el departamento SIG procede a remitir oficio especificando la causa del desistimiento de la solicitud y/o la corrección en caso que sea aplicable.

Fin

3. Creación/Modificación de usuario SAP

Inicio
Dirección/Unidad Solicitante

1. El proceso comienza con la Unidad Solicitante que remite mediante oficio solicitud para crear o modificar un usuario del sistema SAP al Departamento del Sistema Integrado de Gestión (SIG).

Sistema Integrado de Gestión

2. El SIG revisa la solicitud de creación o modificación de usuario, el Usuario técnico verifica si existe disponibilidad

de cuentas para asignar (en el caso de las solicitudes de creación); de no haberlas se contesta a la unidad solicitante que no hay cuentas disponibles para creación de usuarios.

3. El Usuario Técnico del SIG crea/modifica el usuario con los roles correspondientes.

4. Una vez creado/modificado el Usuario se notifica por escrito a través de un oficio a la Unidad Solicitante.

Fin

4. Creación/Modificación de centro logístico y almacén

Inicio
Dirección/Unidad Solicitante

1. La Dirección/Unidad o Departamento solicitante, envía un oficio de solicitud al Departamento del Sistema Integrado de Gestión (SIG) solicitando el desarrollo de un nuevo sistema informático, para cubrir alguna necesidad en específico.

Sistema Integrado de Gestión

2. El programador determina si el requerimiento es procedente; en caso afirmativo, el Programador de sistemas procede a levantar los requerimientos entrevistando a los futuros Usuarios finales.

3. A partir de los requerimientos, el Programador procede a modelar la estructura de la base de datos.

4. Una vez concluido procede a diseñar los prototipos de la interfaz gráfica de usuario.

5. Concluida la etapa de análisis y diseño, se procede a desarrollar el código fuente del software con el lenguaje de

programación más conveniente de acuerdo con la naturaleza del requerimiento.

6. Posteriormente, se procede a realizar pruebas unitarias para identificar incidencias relacionadas a funcionalidad técnicas y validaciones.

7. Al concluir, se realizan pruebas integrales junto con el/los solicitantes para identificar incidencias relacionadas al funcionamiento del software.

8. En caso de no existir incidencias respecto a la funcionalidad, el solicitante procederá a firmar el acta de aceptación del proyecto, dando fe que el software desarrollado cumple con el alcance definido. Por otro lado, en caso de identificar incidencias, el programador de sistemas procede nuevamente a la actividad de desarrollo de código fuente y actividades subsiguientes.

9. Finalmente, el Departamento del SIG designa al programador de sistemas a realizar monitoreo y soporte técnico a usuarios finales, así como, verificar el rendimiento, disponibilidad y consistencia de la información; para determinar si el software efectivamente fortalece el proceso administrativo en cuestión.

Fin

5. Creación de correo electrónico institucional

Inicio
Dirección/Unidad solicitante

1. La Unidad Solicitante remite oficio de solicitud de creación de correo electrónico al Departamento del Sistema Integrado de Gestión (SIG).

Sistema Integrado de Gestión

2. Procede a verificar la disponibilidad de licencias para determinar si el trámite es procedente o retenido.

3. En caso de existir disponibilidad de licencia, el Usuario Técnico del Sistema Integrado de Gestión procede a crear la cuenta de correo electrónico conforme a los parámetros establecidos y se remiten las credenciales de acceso a la cuenta.

Fin

6. Creación de tarjeta para abastecimiento de combustible

Inicio
Dirección/Unidad Solicitante

1. El procedimiento inicia con la necesidad de un Departamento de abastecer combustible a las Unidades, ya sean operativas o de servicio administrativo, la cual elabora una solicitud mediante un oficio a la Unidad correspondiente si es la Policía Nacional será a la Dirección de Logística y si pertenece a la parte administrativa a la Sub Gerencia de Recursos Materiales.

Sistema Integrado de Gestión

2. La solicitud deberá ser remitida a la Gerencia Administrativa para su aprobación y Vo.Bo Posteriormente la validación por parte del Usuario Técnico del SIG si la solicitud procede o no procede, si procede continua con el proceso si no procede fin de proceso.

3. Con las validaciones respectivas aprobadas se solicita al proveedor la tarjeta magnética mediante correo electrónico.

4. Cuando se recibe la tarjeta el Usuario Técnico del SIG realiza la entrega al solicitante por medio de un acta la cual es firmada de recibida.

Fin

c) Alineación de las TI con los procesos

En la Secretaría de Estado en el Despacho de Seguridad y la Policía Nacional, varios de los procesos se han automatizado, haciendo uso de las Tecnologías de Información, con el fin de realizar de manera más eficiente y eficaz los mismos.

Entre los procesos que han adoptado las TI en su desarrollo se encuentran:

- Gestión de compras por parte de las diferentes unidades
- Gestión y control de abastecimiento de combustible para la flota vehicular por medio de RFID y tarjetas de cinta magnética
- Gestión del personal
- Generación de boucher y constancias para el personal de la institución
- Control de vacaciones y permisos
- Generación en línea de constancia de antecedentes policiales
- Pago directo en bancos de infracciones de tránsito
- Gestión de la flota vehicular de la institución
- Generación de planilla de pago

9. MODELO DE GESTIÓN DE LAS TI

a) Estrategia de las TI

i. Definición de los objetivos estratégicos de las TI

1. Mejorar la infraestructura tecnológica para fortalecer la capacidad de respuesta y coordinación en situaciones de emergencia y operativos de seguridad.

2. Implementar sistemas de información y comunicación eficientes y seguros para facilitar el intercambio de información entre las distintas entidades de seguridad y agilizar la toma de decisiones.

3. Promover la capacitación y actualización constante del personal en el uso de tecnologías de la información, con el fin de optimizar su desempeño y aprovechar al máximo las herramientas disponibles.

4. Desarrollar e implementar soluciones tecnológicas innovadoras para la prevención y combate del delito, que permitan anticiparse a situaciones de riesgo y mejorar la eficacia de las operaciones de seguridad.

5. Garantizar la seguridad y protección de la información a través de la implementación de medidas de ciberseguridad y el fortalecimiento de políticas y procedimientos internos.

6. Fomentar la colaboración y el intercambio de información con organismos internacionales y otras instituciones de seguridad, para fortalecer la cooperación en materia de seguridad a nivel regional e internacional.

7. Evaluar periódicamente el desempeño de los sistemas de información y comunicación, con el fin de identificar oportunidades de mejora y garantizar su adecuado funcionamiento.

8. Promover la incorporación de tecnologías emergentes, como la inteligencia artificial y el análisis de big data, para mejorar la capacidad predictiva y analítica en materia de seguridad.

ii. Alineación de la estrategia de las TI con la estrategia de la institución

La alineación de las Tecnologías de la Información y Comunicación (TIC) con las estrategias y objetivos de la Secretaría de Seguridad es un aspecto crucial para garantizar la efectividad, eficiencia y seguridad en la gestión y operaciones de esta entidad. En este contexto, la implementación de

sistemas avanzados como SAP, Microsoft 365 y Kaspersky juega un papel fundamental en la modernización y fortalecimiento de las capacidades de la Secretaría para enfrentar los desafíos actuales en materia de seguridad.

- ***Infraestructura***

  La alineación de las estrategias de Tecnologías de la Información (TI) con la estrategia general de la Secretaría de Seguridad y de la Policía Nacional es fundamental para garantizar una respuesta efectiva y eficiente ante los retos de seguridad actuales. En este contexto, la infraestructura tecnológica desempeña un papel crucial, no solo como soporte para las operaciones diarias, sino también como un facilitador para el logro de los objetivos estratégicos de la institución.
  Un aspecto especialmente crítico en este alineamiento es asegurar que las necesidades de conexión de los funcionarios de la institución estén plenamente cubiertas, permitiéndoles acceder a recursos críticos y comunicarse de manera efectiva, independientemente de su ubicación geográfica.

  Para alinear eficazmente la estrategia de TI con los objetivos de la Secretaría de Seguridad y la Policía Nacional, se deben considerar varios aspectos clave:

  - **Conectividad ininterrumpida y segura**
    La implementación de una red robusta y segura que garantice conectividad ininterrumpida para todos los funcionarios, independientemente de si se encuentran en oficinas centrales, estaciones locales o en el campo. Esto incluye el uso de tecnologías de red privada virtual (VPN) para asegurar la transmisión de datos y el acceso remoto a sistemas internos de manera segura.

  - **Movilidad y Acceso Remoto**
    Facilitar dispositivos móviles y soluciones de acceso remoto seguras para permitir que los funcionarios realicen

tareas críticas y accedan a la información necesaria desde cualquier lugar. Esto es crucial para las operaciones de campo y para una respuesta rápida en situaciones de emergencia.

- **Capacitación y Soporte Técnico**
  Proporcionar formación continua a los funcionarios sobre el uso eficiente de la tecnología y garantizar que exista un soporte técnico disponible 24/7 para resolver cualquier incidencia que pueda afectar la conectividad o el acceso a los sistemas.

- **Infraestructura como Servicio (IaaS) y Plataforma como Servicio (PaaS)**
  Considerar la adopción de infraestructura y plataformas en la nube para mejorar la escalabilidad y flexibilidad de los servicios TI. Esto permite a la institución adaptarse rápidamente a las cambiantes necesidades de seguridad y operativas, asegurando al mismo tiempo la continuidad del servicio.

- **Seguridad de la Información**
  Implementar soluciones de seguridad avanzadas, incluyendo la encriptación de datos, firewalls, sistemas de detección y prevención de intrusiones, y políticas estrictas de control de acceso para proteger la información sensible contra amenazas internas y externas.

- **Colaboración y Herramientas de Comunicación**
  Utilizar plataformas de colaboración en línea que faciliten la comunicación interna y el trabajo en equipo, como Microsoft Teams o similares, asegurando que estas herramientas cumplan con los estándares de seguridad requeridos.

Al cubrir estas necesidades de conexión y alinear las estrategias de TI con los objetivos de la Secretaría de

Seguridad y la Policía Nacional, se puede mejorar significativamente la capacidad de respuesta ante incidentes, optimizar los recursos disponibles y garantizar una gestión de la seguridad pública más efectiva y eficiente. Esta integración estratégica asegura no solo el cumplimiento de los objetivos a corto plazo sino también la sostenibilidad y adaptabilidad de las operaciones de seguridad a largo plazo, en un entorno cada vez más digitalizado y desafiante.

- ***Servicios***

La integración y alineación de las estrategias de Tecnologías de la Información (TI) con la estrategia global de la Secretaría de Seguridad y la Policía Nacional son fundamentales para mejorar los servicios ofrecidos a la ciudadanía, como la emisión de licencias de conducir, permisos de portación de armas y la emisión de constancias de antecedentes policiales. La eficacia, eficiencia, seguridad y accesibilidad de estos servicios son cruciales para el fortalecimiento de la confianza pública en las instituciones de seguridad y en los procesos administrativos gubernamentales.

A continuación, se detallan algunos enfoques clave para alinear las estrategias de TI con los objetivos de servicio al ciudadano:

- **Digitalización y Automatización de Servicios**
  La digitalización de trámites permite una gestión más ágil y menos propensa a errores, mejorando significativamente la experiencia del usuario. Implementar sistemas informáticos que automatizan la recepción, procesamiento y emisión de documentos como licencias de conducir y permisos de portación de armas agiliza los tiempos de respuesta y reduce las cargas operativas.

- **Plataformas en Línea y Servicios de Autoatención**
  Desarrollar e implementar plataformas en línea accesibles para que los ciudadanos puedan realizar solicitudes, tramitar renovaciones, pagar tasas y obtener documentos sin necesidad de desplazarse físicamente. Esto incluye la creación de portales seguros para la consulta de antecedentes policiales, con medidas robustas de verificación de identidad para proteger la privacidad y seguridad de la información.

- **Integración de Bases de Datos y Sistemas Interinstitucionales**
  La interoperabilidad entre diferentes sistemas y bases de datos gubernamentales facilita una verificación más rápida y fiable de la información. Esto es esencial para validar antecedentes, cotejar datos y expedir permisos de manera eficiente. Una estrategia de TI bien alineada aboga por una arquitectura tecnológica que permita esta integración, asegurando al mismo tiempo la seguridad y confidencialidad de los datos personales.

- **Seguridad de la Información y Protección de Datos**
  Implementar políticas de seguridad de la información y soluciones tecnológicas avanzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos manejados. Esto es crucial no solo para proteger la información sensible de los ciudadanos sino también para preservar la confianza en las instituciones que gestionan estos procesos.

- **Facilitación de Acceso y Equidad**
  Hay que asegurar que los servicios en línea sean accesibles para todos los segmentos de la población, incluyendo aquellos con limitado acceso a internet o con discapacidades, mediante la implementación de soluciones tecnológicas inclusivas y la provisión de alternativas para el acceso a los servicios.

- **Capacitación y Sensibilización**
  Capacitar al personal sobre las nuevas tecnologías y procesos digitales para mejorar la eficiencia operativa y la calidad del servicio al ciudadano. Igualmente, realizar campañas de sensibilización para los ciudadanos sobre cómo utilizar los servicios digitales disponibles.

- ***Aplicaciones***

A nivel de aplicaciones de software, esta alineación implica el desarrollo, implementación y uso eficiente de soluciones tecnológicas que respondan directamente a los desafíos operativos, tácticos y estratégicos enfrentados por estas entidades.
A continuación, se explora cómo esta alineación puede optimizar los procesos, mejorar la eficiencia y fortalecer la seguridad pública.

- **SAP**
  En la Secretaría de Seguridad se utiliza para optimizar los recursos y mejorar los procesos internos. A través de su sistema ERP (Planificación de Recursos Empresariales), SAP ayuda a integrar y gestionar de manera centralizada las diversas áreas de la organización, como finanzas, recursos humanos, logística y compras. Esto permite una mejor asignación de recursos, una mayor transparencia en la gestión financiera y una optimización de las cadenas de suministro, lo cual es esencial para el funcionamiento efectivo de cualquier organismo de seguridad.

- **Microsoft 365**
  Ofrece una suite de herramientas colaborativas y de productividad que pueden transformar la forma en que la Secretaría de Seguridad realiza sus operaciones diarias. Con aplicaciones como Teams, Outlook, Word, Excel y

PowerPoint, facilitadas en la nube, el personal puede colaborar en tiempo real, acceder a documentos y comunicarse de manera eficiente, independientemente de su ubicación geográfica. Esto es particularmente relevante para operaciones de seguridad que requieren una coordinación y comunicación rápidas y efectivas. Además, Microsoft 365 incluye funcionalidades de seguridad y cumplimiento avanzadas, que son esenciales para proteger la información sensible manejada por la Secretaría.

- **Kaspersky**
  Conocido por sus soluciones de seguridad informática, es vital para proteger la infraestructura de TI de la Secretaría de Seguridad contra una amplia gama de amenazas cibernéticas, incluyendo virus, malware, ransomware y ataques de phishing. La implementación de Kaspersky garantiza la integridad, confidencialidad y disponibilidad de los datos críticos, un aspecto esencial para mantener la operatividad y la confianza en las operaciones de seguridad. Además, las soluciones de Kaspersky ofrecen gestión de vulnerabilidades, seguridad móvil y control de acceso a internet, proporcionando una protección integral en todos los frentes.

La alineación estratégica de las TIC, mediante la adopción de sistemas como SAP, Microsoft 365 y Kaspersky, permite a la Secretaría de Seguridad mejorar su eficiencia operativa, fomentar la colaboración interna y asegurar sus operaciones y datos contra amenazas cibernéticas. Este enfoque integrado y tecnológicamente avanzado es esencial para afrontar los desafíos de seguridad del siglo XXI, marcando un paso adelante en la modernización y profesionalización de las fuerzas de seguridad.

- ***Usuarios***

A nivel de usuario implica una integración profunda entre las tecnologías disponibles y las necesidades diarias de los funcionarios, así como de los ciudadanos a quienes sirven. Esta alineación busca no solo mejorar la eficiencia operativa y la efectividad de las respuestas de seguridad, sino también fortalecer la transparencia, accesibilidad y confianza pública en estas instituciones.

A continuación, se destacan varios aspectos clave:

- **Facilidad de Uso y Accesibilidad**
  Las aplicaciones y sistemas TIC deben ser intuitivos y fáciles de usar para los funcionarios de todos los niveles, desde la alta dirección hasta el personal operativo. Esto incluye interfaces de usuario claras, capacitación adecuada y soporte técnico accesible para asegurar que todos puedan aprovechar plenamente las herramientas a su disposición. Para los ciudadanos, la accesibilidad se refiere a la capacidad de interactuar con la Secretaría y la Policía a través de múltiples canales digitales, como sitios web, aplicaciones móviles y redes sociales, de manera sencilla y desde cualquier dispositivo.

- **Personalización y Respuesta**
  Los sistemas TIC deben ser capaces de adaptarse a las necesidades específicas de diferentes usuarios. Para los funcionarios, esto puede significar la personalización de dashboards o paneles de control, notificaciones y herramientas de análisis en función de sus roles específicos y responsabilidades. Para los ciudadanos, la personalización mejora la relevancia y el tiempo de respuesta de los servicios ofrecidos, como la emisión de documentos o la respuesta a consultas y denuncias.

- **Seguridad y Privacidad**
  La seguridad de la información y la protección de la privacidad son preocupaciones centrales para usuarios tanto internos como externos. Las TIC deben incorporar mecanismos avanzados de seguridad para proteger la información sensible y personal contra el acceso no autorizado, la manipulación o el robo. Esto incluye la encriptación de datos, autenticaciones robustas y protocolos de seguridad para el intercambio de información.

- **Integración y Colaboración**
  Las herramientas TIC deben fomentar la integración y la colaboración tanto interna como externamente. Internamente, esto significa sistemas que faciliten la comunicación y el trabajo conjunto entre diferentes departamentos y niveles de la Secretaría y la Policía. Externamente, la colaboración con otras agencias gubernamentales, organizaciones internacionales y la comunidad en general es crucial para una gestión eficaz de la seguridad. Las plataformas de colaboración en línea y las redes de comunicación seguras son fundamentales en este aspecto.

- **Capacitación y Desarrollo**
  Para asegurar una alineación efectiva a nivel de usuario, es esencial ofrecer programas de capacitación y desarrollo continuo que permitan a los funcionarios mantenerse actualizados con las últimas tecnologías y prácticas. Esto incluye no solo el uso de software y hardware, sino también la comprensión de los aspectos de ciberseguridad, protección de datos y uso ético de la tecnología.

- **Retroalimentación y Mejora Continua**
  Finalmente, establecer mecanismos de retroalimentación donde los usuarios puedan reportar problemas, sugerir mejoras y compartir experiencias con las herramientas TIC

es vital para el ciclo de mejora continua. Esto asegura que los sistemas evolucionen de acuerdo con las necesidades reales de los usuarios y los desafíos emergentes en el ámbito de la seguridad.

b) Gobierno de las TI

i. Cadena de valor de las TI

Fuente: Tomado de MinTIC, 2015. Basado en: Guide to Measuring the Information Society (2011). OECD; Clasificación Central de Productos -CPC Vers. 2 A.C. Dane; CRC (2010). Análisis del sector TIC en Colombia: evolución y desafíos, Raúl Katz (2015). El ecosistema y la economía digital en América Latina.

ii. Indicadores y riesgos en los procesos de las TI

Indicadores Clave de Rendimiento (KPIs) en TI

1. **Disponibilidad del Sistema**: Mide el tiempo que los sistemas de TI están operativos y disponibles para los usuarios. Es crucial para evaluar la confiabilidad de las infraestructuras de TI.

2. **Tiempo de Respuesta**: Evalúa la rapidez con la que los sistemas y aplicaciones responden a las solicitudes de los usuarios. Un

tiempo de respuesta bajo es indicativo de un buen rendimiento del sistema.

3. **Tiempo de Resolución de Incidentes**: Mide el tiempo que tarda el equipo de TI en resolver un incidente desde que se reporta hasta su conclusión. Es un indicador de la eficiencia del soporte técnico.

4. **Satisfacción del Usuario:** A través de encuestas y feedback directo, este indicador evalúa hasta qué punto los usuarios están satisfechos con los servicios de TI.

5. **Costo por Ticket de Soporte:** Calcula el costo promedio de gestionar y resolver un ticket de soporte, ayudando a evaluar la eficiencia económica del soporte de TI.

6. **Porcentaje de Cumplimiento de Acuerdos de Nivel de Servicio (SLAs)**: Mide la proporción de veces que el equipo de TI cumple con los estándares de servicio acordados, un indicador clave de la fiabilidad y calidad del servicio.

Riesgos en los procesos de TI

1. **Ciberseguridad**: La vulnerabilidad a ataques cibernéticos es uno de los mayores riesgos, pudiendo resultar en la pérdida o compromiso de datos críticos.

2. **Obsolescencia Tecnológica**: El rápido avance de la tecnología puede hacer que los sistemas se vuelvan obsoletos rápidamente, lo que aumenta el riesgo de incompatibilidades y fallas de seguridad.

3. **Fallos del Sistema**: Los errores de software o hardware pueden llevar a la caída de sistemas críticos, afectando la operatividad de la organización.

4. **Pérdida de Datos**: Riesgos asociados a la pérdida de información importante debido a fallos de hardware, errores humanos o ciberataques.

5. **Incumplimiento de Normativas**: El incumplimiento de leyes y regulaciones sobre protección de datos y privacidad puede resultar en sanciones legales y daño reputacional.

6. **Dependencia de Proveedores**: La excesiva dependencia de servicios externos o proveedores de tecnología puede ser un riesgo si estos enfrentan problemas operativos o de seguridad.

7. **Gestión del Cambio**: La implementación de nuevos sistemas o procesos puede enfrentar resistencia interna o fallas debido a una gestión del cambio inadecuada.

Para mitigar estos riesgos, es esencial implementar una sólida gestión de riesgos en TI, que incluya la identificación proactiva de vulnerabilidades, la implementación de medidas de seguridad adecuadas, el mantenimiento regular de sistemas y la capacitación continua de usuarios y personal de TI. Además, el seguimiento constante de los KPIs permitirá a las organizaciones ajustar sus estrategias y procesos de TI para mejorar continuamente su rendimiento y reducir los riesgos asociados.

iii. Plan de implementación de procesos

Plan de Implementación de Procesos TIC para la Secretaría de Seguridad y Policía Nacional

Objetivo:
Implementar procesos TIC eficientes y seguros que mejoren la capacidad operativa y la respuesta a las demandas de seguridad nacional.

1. **Evaluación de la Infraestructura Existente:**
   Realizar un análisis exhaustivo de la infraestructura TIC actual de la Secretaría, identificando áreas de mejora y posibles puntos de vulnerabilidad.
   Evaluar la capacidad de los sistemas actuales para satisfacer las necesidades y la misión y visión de la institución.

2. **Definición de Requerimientos:**
   Consultar a los diferentes departamentos y unidades dentro de la Secretaría para comprender sus necesidades específicas en cuanto a procesos TIC.
   Establecer criterios claros para la selección de tecnologías y soluciones que satisfagan los requerimientos identificados.

3. **Diseño de Procesos TIC:**
   Desarrollar un plan detallado para la implementación de procesos TIC, incluyendo la adquisición de hardware y software, la configuración de redes y sistemas, y la capacitación del personal.
   Diseñar protocolos de seguridad robustos para proteger la información sensible y garantizar la integridad de los sistemas.

4. **Implementación Gradual:**
   Priorizar la implementación de procesos TIC según su impacto en las operaciones de seguridad.
   Realizar pruebas piloto antes de desplegar completamente nuevas tecnologías o sistemas.

5. **Capacitación y Entrenamiento:**
   Brindar capacitación adecuada al personal para garantizar una transición suave hacia los nuevos procesos TIC.
   Establecer programas de entrenamiento continuo para mantener al personal actualizado sobre las últimas tecnologías y mejores prácticas en seguridad informática.

6. **Monitoreo y Evaluación:**
   Implementar mecanismos de monitoreo para supervisar el desempeño de los nuevos procesos TIC y detectar posibles problemas o áreas de mejora.
   Realizar evaluaciones periódicas para medir el impacto de las tecnologías implementadas en la eficiencia operativa y la seguridad de la Secretaría.

7. **Mejora Continua:**
   Establecer un ciclo de mejora continua para optimizar constantemente los procesos TIC y adaptarse a las cambiantes necesidades.
   Fomentar la retroalimentación del personal para identificar oportunidades de mejora y resolver posibles obstáculos.

8. **Comunicación y Divulgación:**
   Informar de manera transparente a todo el personal sobre los cambios en los procesos TIC y los beneficios esperados, por medio de circulares, correo electrónico y boletines informativos.
   Promover una cultura de seguridad informática y concientizar sobre la importancia de proteger los activos de información de la Secretaría.

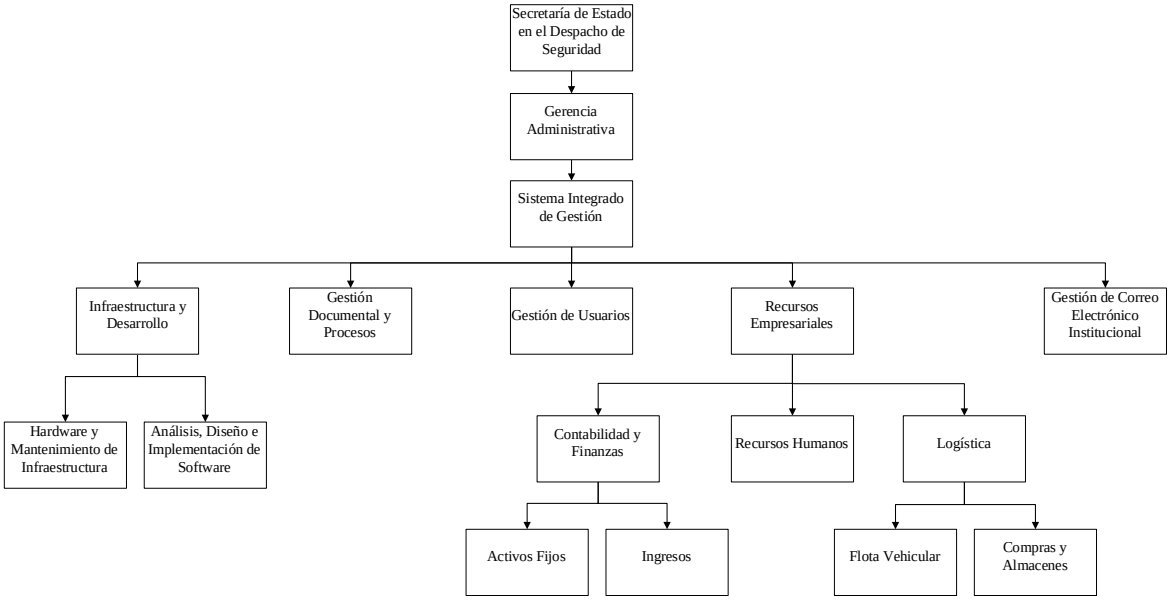
9. **Respaldo y Continuidad del Negocio:**
   Implementar políticas de respaldo de datos y planes de continuidad del negocio para garantizar la disponibilidad y la integridad de la información en caso de incidentes o desastres.

10. **Asignación de Recursos:**
    Destinar los recursos necesarios, tanto humanos como financieros, para asegurar el éxito de la implementación de procesos TIC en la Secretaría de Seguridad y Policía Nacional.

Este plan de implementación de procesos TIC servirá como guía para modernizar y fortalecer la infraestructura tecnológica de la Secretaría, mejorando así su capacidad para garantizar la seguridad y protección de los ciudadanos.

iv. Estructura organizacional del área de TI

Organigrama Sistema Integrado de Gestión



c) Gestión de la información

i. Herramientas de análisis

En aras de optimizar la gestión del recurso humano y la administración de la flota vehicular de la Policía Nacional, se llevará a cabo la implementación de un dashboard utilizando Power BI. Este dashboard ofrecerá una visualización dinámica y en tiempo real del estatus del personal y los vehículos, permitiendo a los responsables de la toma de decisiones tener una visión integral y detallada de la situación operativa en todo momento. Con esta herramienta, será posible monitorear la distribución del personal en diferentes áreas geográficas, identificar posibles desequilibrios en la asignación de recursos y gestionar de manera eficiente la disponibilidad de vehículos para las distintas actividades policiales.

La adopción de este sistema de análisis a través de Power BI conlleva una serie de beneficios significativos para la Policía Nacional. Entre ellos se destacan la capacidad de tomar decisiones más informadas y ágiles basadas en datos en tiempo real, la optimización de la asignación de recursos humanos y vehiculares, la identificación proactiva de áreas de mejora en la gestión operativa y la posibilidad de anticiparse a situaciones que requieran una respuesta rápida y coordinada. Además, al ofrecer una visualización clara y concisa de la información relevante, este dashboard promueve la transparencia y la rendición de cuentas dentro de la institución, fortaleciendo así su capacidad para cumplir con eficacia su misión de proteger y servir a la comunidad.

ii. Arquitectura de Información

La arquitectura de la información es un campo interdisciplinario que se centra en la organización, estructuración y presentación de la información en sistemas de información y medios digitales. En términos generales, la arquitectura de la información se ocupa de diseñar la estructura y la disposición de la información de manera que sea fácil de entender, navegar y encontrar por parte de los usuarios.

En el contexto digital, la arquitectura de la información se refiere a la organización de contenidos en sitios web, aplicaciones móviles, bases de datos y otros entornos digitales. Esto implica definir cómo se clasifican y categorizan los contenidos, cómo se relacionan entre sí, cómo se presentan visualmente al usuario, y cómo se facilita la navegación y la búsqueda.

Para implementar una sólida arquitectura de información en la página web de la Secretaría de Seguridad, es crucial considerar varios aspectos para garantizar una experiencia óptima para los usuarios, todo esto en búsqueda de la mejora continua:

- **Análisis de usuarios y sus necesidades**: Comprender quiénes son los principales usuarios de la página web de la Secretaría de

Seguridad, qué información están buscando y cómo prefieren acceder a ella.

- **Jerarquización de la información**: Organizar la información de manera jerárquica, con los elementos más importantes y relevantes en la parte superior de la estructura. Por ejemplo, secciones como noticias, programas de seguridad, contacto con la policía, deberían estar fácilmente accesibles desde el menú principal.

- **Navegación intuitiva**: Diseñar una navegación clara y fácil de usar que guíe a los usuarios de manera intuitiva a través del sitio web. Esto puede incluir un menú desplegable con categorías bien definidas y enlaces a páginas internas relevantes.

- **Etiquetado consistente**: Utilizar etiquetas y categorías consistentes en todo el sitio para que los usuarios puedan comprender fácilmente la estructura de la información y encontrar lo que están buscando sin confusión.

- **Búsqueda efectiva**: Implementar una función de búsqueda efectiva que permita a los usuarios encontrar rápidamente la información deseada. Esto puede incluir la capacidad de filtrar los resultados de búsqueda por categoría o fecha.

- **Diseño receptivo**: Asegurarse de que el diseño de la página web sea receptivo y se adapte a diferentes dispositivos y tamaños de pantalla, para garantizar una experiencia consistente y satisfactoria en computadoras de escritorio, tabletas y dispositivos móviles.

- **Retroalimentación del usuario**: Facilitar la retroalimentación de los usuarios sobre la navegación y la accesibilidad del sitio web, mediante encuestas, formularios de contacto o herramientas de comentarios, para identificar áreas de mejora y realizar ajustes según sea necesario.

d) Sistemas de información

i. Arquitectura de sistemas de información

La arquitectura de sistemas de información se refiere a la estructura y diseño de los componentes de un sistema de información, incluyendo hardware, software, redes, bases de datos, interfaces de usuario y otros elementos, con el fin de cumplir con los objetivos y requisitos del negocio de manera eficiente y efectiva. Esta arquitectura se basa en principios y estándares que guían la organización y el funcionamiento del sistema en su conjunto.

Algunos aspectos clave de la arquitectura de sistemas de información incluyen:

- **Componentes del sistema**: Identificación de los diferentes componentes que conforman el sistema de información, como servidores, clientes, bases de datos, aplicaciones, etc.

- **Interconexiones**: Definición de cómo se conectan y comunican entre sí los distintos componentes del sistema, ya sea a través de redes locales, nubes, internet u otros medios.

- **Capas de abstracción**: Organización de los componentes del sistema en capas de abstracción, como la capa de presentación (interfaz de usuario), la capa de lógica de negocio (aplicaciones y procesos) y la capa de datos (almacenamiento y gestión de información).

- **Estándares y protocolos**: Establecimiento de estándares y protocolos para la comunicación entre los componentes del sistema, garantizando la interoperabilidad y la compatibilidad entre diferentes tecnologías y plataformas.

- **Seguridad**: Integración de medidas de seguridad para proteger la información y los recursos del sistema contra accesos no autorizados, ataques cibernéticos y otros riesgos.

- **Escalabilidad y rendimiento**: Diseño del sistema de manera que pueda crecer y adaptarse a medida que cambien las necesidades del negocio, y que pueda mantener un rendimiento óptimo incluso bajo cargas de trabajo intensas.

- **Mantenibilidad**: Consideración de la facilidad con la que el sistema puede ser mantenido y actualizado a lo largo del tiempo, minimizando el tiempo de inactividad y los costos asociados.

- **Cumplimiento normativo**: Aseguramiento de que el sistema cumpla con las regulaciones y normativas aplicables en cuanto a privacidad, seguridad, accesibilidad, entre otros aspectos.

ii. Implementación de sistemas de información

La implementación exitosa de SAP en la Secretaría de Seguridad ha generado una serie de beneficios significativos, especialmente en lo que respecta a la estrategia de reducción delictiva. Estos beneficios se extienden a través de varios aspectos clave de la operación de la Secretaría, proporcionando herramientas y capacidades mejoradas para abordar los desafíos de seguridad pública. A continuación, se detallan algunos de los principales beneficios:

- **Mejora en la gestión de recursos humanos**: SAP ha optimizado la gestión del recurso humano dentro de la Secretaría de Seguridad, permitiendo una asignación más eficiente del personal en áreas críticas de intervención delictiva. Esto se logra a través de una mejor gestión de turnos, monitoreo de la disponibilidad del personal y asignación de tareas basada en las habilidades y la ubicación geográfica.

- **Optimización de la logística y el aprovisionamiento**: La implementación de SAP ha mejorado significativamente la gestión de inventarios y suministros dentro de la Secretaría. Esto garantiza que los recursos necesarios para las operaciones policiales estén disponibles de manera oportuna y eficiente, lo que contribuye a una respuesta más rápida y efectiva ante situaciones de emergencia o delictivas.

- **Integración de sistemas y procesos**: La implementación de SAP ha facilitado la integración de sistemas y procesos dentro de la Secretaría de Seguridad, lo que mejora la coordinación y la colaboración entre diferentes unidades y departamentos. Esto permite una respuesta más coordinada y eficaz a situaciones de emergencia y una mejor comunicación entre los diversos actores involucrados en la prevención y el combate del delito.

- **Mayor transparencia y rendición de cuentas**: SAP ha mejorado la transparencia en la gestión de recursos y operaciones dentro de la Secretaría de Seguridad, lo que contribuye a una mayor rendición de cuentas y una mejor supervisión de las actividades policiales. Esto ayuda a prevenir prácticas corruptas y garantiza que los recursos públicos se utilicen de manera eficiente y efectiva en la lucha contra la delincuencia.

En resumen, la implementación de SAP en la Secretaría de Seguridad ha fortalecido significativamente su capacidad para prevenir y combatir la delincuencia, proporcionando herramientas y capacidades mejoradas para la gestión de recursos humanos, la logística, el análisis de datos y la coordinación operativa. Esto ha contribuido de manera tangible a la estrategia de reducción delictiva, permitiendo una respuesta más efectiva y proactiva a los desafíos de seguridad pública.

iii. Servicios de soporte técnico

La Secretaría de Seguridad ha implementado una robusta gama de servicios de soporte técnico para sus usuarios finales, abarcando diversas

áreas críticas que van desde la gestión de sistemas empresariales como SAP hasta el mantenimiento de equipos informáticos y la seguridad de la información con herramientas como Microsoft 365 y Kaspersky Cloud Plus Endpoint. Este enfoque integral no solo garantiza la continuidad operativa, sino que también fortalece las capacidades de respuesta y prevención delictiva de la institución.

En primer lugar, la adopción de SAP ha revolucionado la gestión administrativa y operativa de la Secretaría, proporcionando una plataforma unificada para optimizar procesos, centralizar datos y mejorar la toma de decisiones. Esta solución ha permitido una mejor planificación de recursos, la automatización de tareas rutinarias y la generación de informes precisos y oportunos, lo que ha contribuido a una mayor eficiencia y transparencia en todas las operaciones.

Por otro lado, los servicios de soporte técnico también se extienden a la suite de Microsoft 365, que ofrece herramientas colaborativas y de productividad esenciales para el personal de la Secretaría. La integración de aplicaciones como Outlook, Teams y OneDrive facilita la comunicación interna, la colaboración en proyectos y el acceso seguro a la información desde cualquier lugar y dispositivo, lo que mejora la eficiencia y la capacidad de respuesta ante situaciones críticas.

En cuanto a la seguridad informática, la implementación de Kaspersky Cloud Plus Endpoint ha reforzado las defensas contra amenazas cibernéticas, protegiendo los sistemas y datos sensibles de la Secretaría contra malware, ransomware y otras formas de ataques. Esta solución ofrece una protección proactiva en tiempo real, así como herramientas de gestión centralizada que permiten supervisar y mantener la seguridad de manera eficiente en todos los dispositivos y puntos finales de la red.

Además, los servicios de mantenimiento de equipos informáticos garantizan el correcto funcionamiento y rendimiento de los dispositivos utilizados por el personal, minimizando el tiempo de inactividad y optimizando la productividad. Esta atención proactiva incluye actualizaciones de software, reparaciones de hardware y configuraciones personalizadas según las necesidades individuales de cada usuario.

Finalmente, la gestión de abastecimiento de combustible se ha simplificado y optimizado mediante soluciones tecnológicas que permiten monitorear y controlar el consumo de combustible de la flota vehicular de manera eficiente. Esto no solo reduce los costos operativos, sino que también contribuye a una mejor planificación logística y una mayor disponibilidad de recursos para las operaciones de seguridad y prevención delictiva.

En resumen, los servicios de soporte técnico brindados a los usuarios finales de la Secretaría de Seguridad, que incluyen soluciones como SAP, Microsoft 365, Kaspersky Cloud Plus Endpoint, mantenimiento de equipos informáticos y gestión de abastecimiento de combustible, juegan un papel fundamental en el fortalecimiento de las capacidades operativas y estratégicas de la institución, permitiendo una respuesta más efectiva y eficiente ante los desafíos de seguridad y prevención delictiva.

e) Modelo de gestión de servicios tecnológicos

i. Criterios de calidad y procesos de gestión de servicios de TIC

En la Secretaría de Seguridad, la gestión de servicios de Tecnologías de la Información y Comunicación (TIC) se rige por rigurosos criterios de calidad y procesos diseñados para garantizar la eficiencia, seguridad y confiabilidad de los sistemas y recursos tecnológicos utilizados en las operaciones diarias. Estos criterios y procesos están orientados a cumplir con los objetivos estratégicos de la institución y satisfacer las necesidades tanto internas como externas de manera efectiva.

- **Disponibilidad y fiabilidad**: Se establecen estándares para garantizar que los servicios de TIC estén disponibles cuando se necesiten y que funcionen de manera confiable en todo momento. Esto implica implementar medidas de redundancia, respaldo y recuperación ante desastres para minimizar el tiempo de inactividad y asegurar la continuidad operativa.

- **Seguridad de la información**: Se aplican estrictas políticas y procedimientos de seguridad para proteger los activos de información de la Secretaría, incluyendo datos confidenciales, sistemas críticos y recursos tecnológicos. Esto implica la implementación de medidas de control de acceso, encriptación de datos, monitoreo de amenazas y concientización del personal en materia de seguridad informática.

- **Eficiencia operativa**: Se promueven procesos eficientes y optimizados para maximizar el rendimiento de los sistemas y recursos de TIC, minimizando el tiempo y los recursos necesarios para llevar a cabo tareas y procesos. Esto incluye la automatización de tareas repetitivas, la optimización de recursos de hardware y software, y la adopción de mejores prácticas en la gestión de servicios de TI.

- **Atención al usuario**: Se establecen canales de comunicación eficaces para brindar soporte técnico oportuno y de calidad a los usuarios de los servicios de TIC. Esto implica la implementación de un servicio de mesa de ayuda o centro de atención al usuario, donde se puedan reportar y resolver incidentes y solicitudes de manera rápida y eficiente.

- **Mejora continua**: Se fomenta una cultura de mejora continua en la gestión de servicios de TIC, mediante la evaluación periódica del desempeño, la identificación de áreas de mejora y la implementación de acciones correctivas y preventivas. Esto incluye la retroalimentación del usuario, revisiones de procesos y tecnologías, y la adopción de estándares y marcos de trabajo reconocidos en la industria de las TIC.

- **Cumplimiento normativo**: Se asegura el cumplimiento de las regulaciones y normativas aplicables en materia de tecnologías de la información y protección de datos. Esto implica estar al tanto de las leyes y regulaciones relevantes, implementar controles y procedimientos para garantizar el cumplimiento, y someterse a

auditorías periódicas para verificar el cumplimiento de los requisitos legales y regulatorios.

En resumen, los criterios de calidad y procesos de gestión de servicios de TIC en la Secretaría de Seguridad se centran en garantizar la disponibilidad, seguridad, eficiencia y mejora continua de los sistemas y recursos tecnológicos utilizados para cumplir con la misión de la institución y garantizar la seguridad y protección de los ciudadanos.

ii. Infraestructura

La gestión de la infraestructura de Tecnologías de la Información (TI) en la Secretaría de Seguridad es fundamental para asegurar el funcionamiento eficiente de los sistemas y recursos tecnológicos utilizados en las operaciones diarias. Esta gestión abarca una serie de actividades y procesos destinados a planificar, implementar, monitorear y mantener la infraestructura de TI de manera efectiva, garantizando que cumpla con los objetivos estratégicos de la institución. Algunos aspectos clave de la gestión de la infraestructura de TI en la Secretaría de Seguridad incluyen:

- **Planificación y diseño**: Se realiza una planificación estratégica para determinar las necesidades actuales y futuras de infraestructura de TI de la Secretaría, considerando factores como la capacidad, seguridad, escalabilidad y cumplimiento normativo. Se diseñan arquitecturas de infraestructura que sean adecuadas para soportar las operaciones y aplicaciones críticas de la institución.

- **Implementación y despliegue**: Se lleva a cabo la implementación de la infraestructura de TI de acuerdo con los planes y diseños establecidos, asegurando que los sistemas y recursos sean configurados correctamente y puestos en funcionamiento de manera efectiva. Esto puede incluir la adquisición de hardware y software, la configuración de redes, la instalación de sistemas operativos y la integración de aplicaciones.

- **Monitoreo y mantenimiento**: Se establecen mecanismos de monitoreo para supervisar el rendimiento, disponibilidad y seguridad de la infraestructura de TI de manera continua. Se realizan tareas de mantenimiento preventivo y correctivo para garantizar el funcionamiento óptimo de los sistemas y recursos, y se abordan proactivamente los problemas identificados antes de que afecten las operaciones.

- **Gestión de riesgos y seguridad**: Se implementan medidas de seguridad para proteger la infraestructura de TI contra amenazas y vulnerabilidades, incluyendo la implementación de firewalls, sistemas de detección de intrusiones, encriptación de datos y políticas de acceso. Se lleva a cabo la gestión de riesgos para identificar, evaluar y mitigar los riesgos potenciales que puedan afectar la seguridad y disponibilidad de la infraestructura.

- **Respaldo y recuperación**: Se establecen políticas y procedimientos para realizar copias de seguridad de datos y sistemas de manera regular, garantizando la disponibilidad y la integridad de la información en caso de desastres o incidentes. Se desarrollan planes de recuperación ante desastres para restaurar rápidamente los sistemas y recursos en caso de interrupciones graves.

- **Optimización y mejora continua**: Se realizan evaluaciones periódicas de la infraestructura de TI para identificar áreas de mejora y optimización. Se implementan cambios y actualizaciones de manera planificada para mejorar el rendimiento, la eficiencia y la seguridad de la infraestructura de manera continua.

iii. Conectividad

La gestión de la conectividad TIC en la Secretaría de Seguridad se erige como un pilar fundamental para fortalecer las operaciones y la coordinación en el ámbito de la seguridad pública. A través de una infraestructura tecnológica robusta y eficiente, se promueve la interconexión de sistemas, la recopilación y análisis de datos, así como la comunicación ágil y segura entre las distintas instancias gubernamentales y cuerpos de seguridad. Esta gestión integral de la conectividad TIC permite optimizar la respuesta ante situaciones de emergencia, mejorar la vigilancia y el monitoreo del territorio, y facilitar la toma de decisiones estratégicas basadas en información oportuna y precisa. De esta manera, la Secretaría de Seguridad se posiciona como un actor clave en la aplicación de tecnologías de la información y la comunicación para garantizar la protección y el bienestar de la ciudadanía.

iv. Servicios de operación

La gestión de los servicios de operación de Tecnologías de la Información y Comunicación (TIC) en la Secretaría de Seguridad se caracteriza por su enfoque integral y proactivo para garantizar la continuidad y eficiencia de los sistemas críticos. Desde el monitoreo constante de la infraestructura hasta la respuesta ágil ante incidencias, se prioriza la seguridad y disponibilidad de los recursos digitales. Además, se fomenta la innovación y actualización tecnológica para adaptarse a las demandas cambiantes del entorno, fortaleciendo así la capacidad de respuesta y la coordinación interinstitucional en materia de seguridad.

v. Mesa de servicios

La gestión del servicio de Help Desk en la Secretaría de Seguridad se centra en proporcionar un punto de contacto centralizado y eficiente para resolver consultas, incidencias y solicitudes de soporte relacionadas con tecnologías de la información y comunicación (TIC). Con un equipo especializado y procesos bien definidos, se garantiza una atención rápida y efectiva a los usuarios, ya sean agentes de seguridad, personal

administrativo o ciudadanos. Además, se implementan medidas para registrar, clasificar y dar seguimiento a cada solicitud, asegurando así una gestión transparente y trazable de todas las interacciones. Esta estrategia no solo mejora la productividad y el funcionamiento de los sistemas TIC, sino que también fortalece la confianza y satisfacción de los usuarios con los servicios proporcionados por la Secretaría de Seguridad.

f) Iniciativas de uso y apropiación

Las iniciativas de uso y apropiación de las Tecnologías de la Información (TI) en el ámbito del gobierno digital, especialmente en la Secretaría de Seguridad, se centran en mejorar la eficiencia, transparencia y calidad de los servicios ofrecidos a la ciudadanía. Estas iniciativas pueden incluir la implementación de plataformas en línea para facilitar trámites y consultas, como la solicitud de documentos, denuncias de delitos o seguimiento de procesos judiciales.

Además, se promueve la participación ciudadana a través de herramientas digitales que permiten a los ciudadanos interactuar con las autoridades de seguridad, reportar incidentes y recibir información relevante en tiempo real. Esto puede incluir aplicaciones móviles, portales web y redes sociales que facilitan la comunicación bidireccional entre la comunidad y las fuerzas de seguridad.

Asimismo, se desarrollan proyectos de análisis de datos y sistemas de información que permiten recopilar, procesar y analizar grandes volúmenes de información para mejorar la toma de decisiones y la prevención del delito. Estas iniciativas pueden involucrar el uso de tecnologías como el análisis predictivo, la inteligencia artificial y la minería de datos para identificar patrones, tendencias y áreas de riesgo.

En resumen, las iniciativas de uso y apropiación de las TI en el ámbito del gobierno digital y la seguridad se enfocan en aprovechar la tecnología para fortalecer la gobernanza, aumentar la seguridad ciudadana y promover una mayor participación y colaboración entre el gobierno y la sociedad.

10. MODELO DE PLANEACIÓN

a) Lineamientos o principios que rigen el PETI

El Plan de Tecnología, Información y Comunicaciones se rige en las siguientes:

- Objetivos estratégicos de la institución
- Objetivos sectoriales del gobierno central
- Líneas de acción por parte de las autoridades de la Secretaría de Seguridad y Policía Nacional
- Necesidades de la población en el ámbito de la seguridad y servicios ofrecidos por la institución

b) Estructura de actividades estratégicas

- **Análisis de necesidades y diagnóstico**: Identificar las necesidades específicas de la Secretaría de Seguridad en cuanto a infraestructura tecnológica, sistemas de información, comunicaciones y seguridad cibernética. Realizar un diagnóstico de la situación actual para establecer áreas de mejora y oportunidades de desarrollo.

- **Definición de objetivos y metas**: Establecer objetivos claros y alcanzables en función de las necesidades identificadas y los requerimientos del entorno de seguridad. Establecer metas cuantificables y medibles para evaluar el progreso y el éxito de las iniciativas de TIC.

- **Planificación estratégica**: Desarrollar un plan estratégico de TIC que defina las acciones necesarias para alcanzar los objetivos establecidos. Esto incluiría la asignación de recursos, la definición de plazos y la identificación de responsables de cada actividad.

- **Implementación de infraestructura tecnológica**: Desplegar y mantener la infraestructura tecnológica necesaria para soportar las operaciones de seguridad, incluyendo redes de comunicaciones, sistemas de almacenamiento y procesamiento de datos, y sistemas de seguridad cibernética.

- **Desarrollo de sistemas de información**: Diseñar, desarrollar e implementar sistemas de información específicos para las necesidades de la Secretaría de Seguridad, como sistemas de gestión del delito, seguimiento de casos, análisis de datos y sistemas de información geoespacial.

- **Capacitación y formación**: Proporcionar capacitación y formación continua al personal de la Secretaría de Seguridad en el uso adecuado de las TIC, así como en temas de seguridad cibernética y protección de datos.

- **Gestión del cambio**: Gestionar el cambio organizacional asociado con la implementación de nuevas tecnologías y procesos, asegurando la aceptación y adopción por parte de los usuarios finales.

- **Monitoreo y evaluación**: Establecer mecanismos de monitoreo y evaluación para medir el progreso y el impacto de las iniciativas de TIC, así como para identificar áreas de mejora y ajuste continuo del plan estratégico.

c) Prioridades de implantación

Definir las prioridades de implementación de un plan de Tecnologías de la Información y Comunicación (TIC) en la Secretaría de Seguridad de Honduras requiere un enfoque que atienda tanto a las necesidades inmediatas de la institución en términos de seguridad y eficiencia operativa, como a sus objetivos a largo plazo de modernización y servicio a la comunidad.

1. **Fortalecimiento de la Infraestructura de TIC**: Priorizar la creación o actualización de una infraestructura tecnológica robusta y segura, que permita el funcionamiento eficiente de las operaciones diarias y garantice la integridad y disponibilidad de la información.

2. **Sistemas de Gestión de Información para la Seguridad**: Desarrollar e implementar sistemas integrados para la gestión de información relacionada con la seguridad pública, como reportes de delitos, investigaciones, y seguimiento de casos, que faciliten el análisis de datos y la toma de decisiones basada en evidencia.

3. **Comunicaciones Seguras**: Establecer sistemas de comunicación seguros para el personal de seguridad, incluyendo redes privadas virtuales (VPN), encriptación de datos y sistemas de comunicación encriptada, para proteger la información sensible y facilitar una respuesta rápida y coordinada ante incidentes.

4. **Capacitación y Desarrollo de Competencias en TIC**: Implementar programas de formación continua para el personal, centrados en el manejo de nuevas tecnologías, seguridad de la información, y análisis de datos, para asegurar que los recursos humanos pueden aprovechar plenamente las herramientas tecnológicas disponibles.

5. **Seguridad Cibernética y Protección de Datos**: Desarrollar una estrategia integral de seguridad cibernética para proteger la infraestructura de TIC contra ataques informáticos, incluyendo la implementación de herramientas de seguridad avanzadas, y la creación de políticas y procedimientos para la gestión de riesgos y la respuesta a incidentes.

6. **Plataformas de Servicio al Ciudadano**: Desplegar plataformas digitales que permitan a los ciudadanos acceder a servicios de seguridad, realizar denuncias o consultas de manera anónima, y recibir información relevante, promoviendo así una mayor participación comunitaria y transparencia.

7. **Gestión del Cambio y Adopción Tecnológica**: Asegurar un enfoque proactivo en la gestión del cambio para facilitar la adopción de nuevas tecnologías por parte del personal y los usuarios de los servicios, incluyendo estrategias de comunicación efectivas y apoyo continuo durante el proceso de transición.

d) Proyección de presupuesto del área de TI

Dada la naturaleza sensible de la información manejada por nuestra institución, su divulgación queda estrictamente restringida para asegurar la integridad y seguridad tanto de nuestras operaciones como del personal involucrado. Esta medida obedece a protocolos de confidencialidad y seguridad nacional, esenciales para preservar los intereses y bienestar colectivo, garantizando así el cumplimiento de nuestras responsabilidades y misiones institucionales de forma segura y efectiva.

e) Plan de implantación

i. Plan de intervención sistemas de información

Un plan de intervención para sistemas de información es un conjunto estructurado de acciones diseñadas para mejorar, actualizar o implementar sistemas de información dentro de una organización. Este plan debe ser específico, medible, alcanzable, relevante y temporalmente definido (criterios SMART).

1. **Diagnóstico inicial**
   - Evaluación de la situación actual: Analizar los sistemas de información existentes para identificar fortalezas, debilidades, oportunidades y amenazas (análisis FODA).
   - Identificación de necesidades: Determinar las necesidades de los usuarios y cómo los sistemas actuales no las cumplen eficazmente.

2. **Definición de objetivos**
   - Objetivos generales y específicos: Basados en el diagnóstico inicial, definir qué se busca lograr con la intervención en términos de mejora de procesos, eficiencia, seguridad de la información y satisfacción del usuario.

3. **Planificación estratégica**
    - Selección de tecnologías: Decidir qué tecnologías se implementarán o actualizarán.
    - Diseño del plan de acción: Detallar las acciones específicas, asignar responsables, recursos necesarios y plazos.
    - Estrategia de gestión del cambio: Desarrollar un enfoque para gestionar el cambio organizacional, incluyendo capacitación para los usuarios.
4. **Implementación**
    - Desarrollo o adquisición: Comenzar el desarrollo de sistemas personalizados o la adquisición de soluciones de software existentes.
    - Pruebas: Realizar pruebas exhaustivas para asegurar que los sistemas cumplen con los requisitos establecidos.
    - Capacitación: Proveer capacitación necesaria a los usuarios finales para asegurar una transición suave.
5. **Monitoreo y evaluación**
    - Monitoreo continuo: Seguir de cerca la implementación para identificar y resolver problemas rápidamente.
    - Evaluación post-implementación: Medir el éxito del proyecto en función de los objetivos definidos, analizar el retorno de la inversión (ROI) y determinar si se han cumplido las expectativas de los usuarios.
6. **Ajustes y mejoras**
    - Retroalimentación: Recoger comentarios de los usuarios para identificar áreas de mejora.

- Actualizaciones: Realizar ajustes y mejoras continuas basadas en la retroalimentación y en los avances tecnológicos.

ii. Plan de proyectos de servicios tecnológicos

Implementación de un dashboard mediante Power BI

1. Inicio del Proyecto

- **Objetivo del proyecto**:
  Implementar un dashboard de recursos humanos y flota vehicular que permita a la Policía Nacional monitorear de manera eficiente y centralizada la información relacionada con el personal y los vehículos, con el fin de optimizar la gestión de recursos, mejorar la toma de decisiones y fortalecer la seguridad ciudadana.

- **Alcance del proyecto:**
  Este sistema incluirá datos como asignación del personal, disponibilidad, distribución por escala y grado, estado y disponibilidad de vehículos, mantenimientos programados y realizados, así como el consumo de combustible. Las métricas clave a monitorear abarcarán tasas de ausentismo, rotación de personal, costos de mantenimiento vehicular, eficiencia en el uso de los vehículos, entre otros indicadores de rendimiento operativo y financiero.
  Diseñado para ser una herramienta de consulta y análisis para decisiones estratégicas, su uso estará destinado a los mandos medios y altos de la organización, incluyendo gestores de recursos humanos, administradores de la flota, hasta llegar a niveles directivos y de planificación estratégica.

  Este enfoque permitirá mejorar la asignación de recursos, optimizar las operaciones y elevar la eficiencia general de la Secretaría de Seguridad y la Policía Nacional de Honduras.

- **Equipo del proyecto**:
  Asignar roles y responsabilidades dentro del equipo, incluyendo al líder del proyecto, analistas de datos, expertos en Power BI y usuarios finales.

2. **Inicio del Proyecto**

- **Recolección de requisitos**:
  Entrevistar a los usuarios finales para entender sus necesidades y expectativas con respecto al dashboard.

- **Definición de KPIs**:
  Identificar los indicadores clave de rendimiento (KPIs) que serán monitoreados a través del dashboard.

- **Evaluación de fuentes de datos**:
  Determinar las fuentes de datos disponibles y evaluar su calidad y disponibilidad para su integración en Power BI.

3. **Diseño del Dashboard**

- **Diseño visual**:
  Crear un diseño visual atractivo y fácil de entender para el dashboard, utilizando las capacidades de visualización de datos de Power BI.

- **Desarrollo de modelos de datos**:
  Diseñar y desarrollar modelos de datos eficientes para almacenar y manipular los datos dentro de Power BI.

- **Configuración de conexiones:**
  Configurar conexiones a las fuentes de datos y establecer actualizaciones programadas para mantener los datos del dashboard al día.

4. **Desarrollo y Pruebas**

   - **Desarrollo del dashboard:**
     Construir el dashboard utilizando las herramientas y funcionalidades de Power BI, incluyendo la creación de gráficos, tablas y filtros interactivos.

   - **Pruebas de usuario**:
     Realizar pruebas exhaustivas del dashboard con los usuarios finales para asegurar que cumpla con sus necesidades y expectativas.

   - **Ajustes y optimizaciones:**
     Realizar ajustes y optimizaciones basados en los comentarios y retroalimentación de los usuarios durante las pruebas.

5. **Implementación y Entrega**

   - **Implementación del dashboard:**
     Desplegar el dashboard en el entorno de producción de Power BI y proporcionar acceso a los usuarios finales.

   - **Capacitación y soporte:**
     Proporcionar capacitación a los usuarios finales sobre cómo utilizar el dashboard y ofrecer soporte continuo para resolver cualquier problema que surja.

   - **Documentación:**
     Crear documentación detallada sobre el dashboard, incluyendo su propósito, cómo acceder a él, y cómo interpretar los datos mostrados.

6. Monitoreo y Mantenimiento

- **Monitoreo del rendimiento:**
  Monitorear el rendimiento del dashboard y su impacto en la toma de decisiones de la organización.

- **Actualizaciones y mejoras:**
  Realizar actualizaciones periódicas al dashboard para incorporar nuevas funcionalidades, corregir errores y mejorar su usabilidad.

- **Evaluación del proyecto:**
  Evaluar el éxito del proyecto en función de los objetivos establecidos e identificar lecciones aprendidas para futuras implementaciones.

f) Administración del riesgo

A continuación, se presenta la matriz de gestión del riesgo del proceso de Implementación de un Dashboard mediante Power BI:

Seguridad Gobierno de la República	SECRETARÍA DE ESTADO EN EL DESPACHO DE SEGURIDAD MATRIZ PARA LA EVALUACIÓN, ANÁLISIS Y RESPUESTA A LOS RIESGOS	NCI-TSC/222-00; NCI-TSC/223-00; NCI-TSC/224-00 Formulario 27 SESEGU

PROCESO:	Implementación de un dashboard mediante Power BI
NOMBRE DEL SUBPROCESO:	Implementación de un dashboard mediante Power BI
OBJETIVO:	Implementar un dashboard de recursos humanos y flota vehicular que permita a la Policía Nacional monitorear de manera eficiente y centralizada la información relacionada con el personal y los vehículos, con el fin de optimizar la gestión de recursos, mejorar la toma de decisiones y fortalecer la seguridad ciudadana.

No.	Etapa del proceso	Descripción del Riesgo	Riesgo Inherente		Zona de Riesgo Preliminar	Controles obligatorios para mitigar los riesgos	Controles que existen en la entidad	Controles pendientes por establecer para mitigar los riesgos	Riesgo Residual		Zona de Riesgo Final	Respuesta a los Riesgos
			P	I					P	I		
1	Definición de requerimientos y KPIs	Falta de claridad en los requisitos y KPIs	3	4	E	- Involucramiento de las partes interesadas claves - Realizar sesiones de recolección de requisitos	-	- Involucramiento de las partes interesadas claves - Realizar sesiones de recolección de requisitos	1	2	B	Aceptar el riesgo
2	Diseño del dashboard	Diseño ineficiente del dashboard	2	4	A	- Definición clara de requisitos de diseño - Creación de un diseño conceptual que represente la estructura y el contenido del mismo	-	- Definición clara de requisitos de diseño - Creación de un diseño conceptual que represente la estructura y el contenido del mismo	1	2	B	Aceptar el riesgo
3	Desarrollo y pruebas	Desviaciones significativas entre el diseño conceptual y la implementación	1	2	B	- Revisión y validación del diseño conceptual para verificar que refleje las expectativas de usuarios finales - Revisiones periódicas durante el desarrollo	-	- Revisión y validación del diseño conceptual para verificar que refleje las expectativas de usuarios finales - Revisiones periódicas durante el desarrollo	1	1	B	Aceptar el riesgo
4	Implementación y entrega	Retrasos en la implementación y entrega	2	4	A	- Planificación detallada y realista - Asignación adecuada de recursos humanos, técnicos y financieros	-	- Planificación detallada y realista - Asignación adecuada de recursos humanos, técnicos y financieros	1	2	B	Aceptar el riesgo
5	Monitoreo y mantenimiento	Ineficacia en el monitoreo y mantenimiento	2	2	B	- Establecimiento de métricas clave de rendimiento (KPIs) - Programar revisiones regulares	-	- Establecimiento de métricas clave de rendimiento (KPIs) - Programar revisiones regulares	1	1	B	Aceptar el riesgo

Elaborado por:	**Revisado por:**	**Aprobado por:**
Leonel Canales	Msc. Deiby Cerrato	Msc. Mariela García (Coordinadora COCOIN)
Firma:	**Firma:**	**Firma:**
Fecha: 05/03/2024	**Fecha:** 05/03/2024	**Fecha:** 05/03/2024

11. BIBLIOGRAFÍA

- Guide to Measuring the Information Society (2011). OECD; Clasificación Central de Productos -CPC Vers. 2 A.C. Dane; CRC (2010). Análisis del sector TIC en Colombia: evolución y desafíos, Raúl Katz (2015). El ecosistema y la economía digital en América Latina.

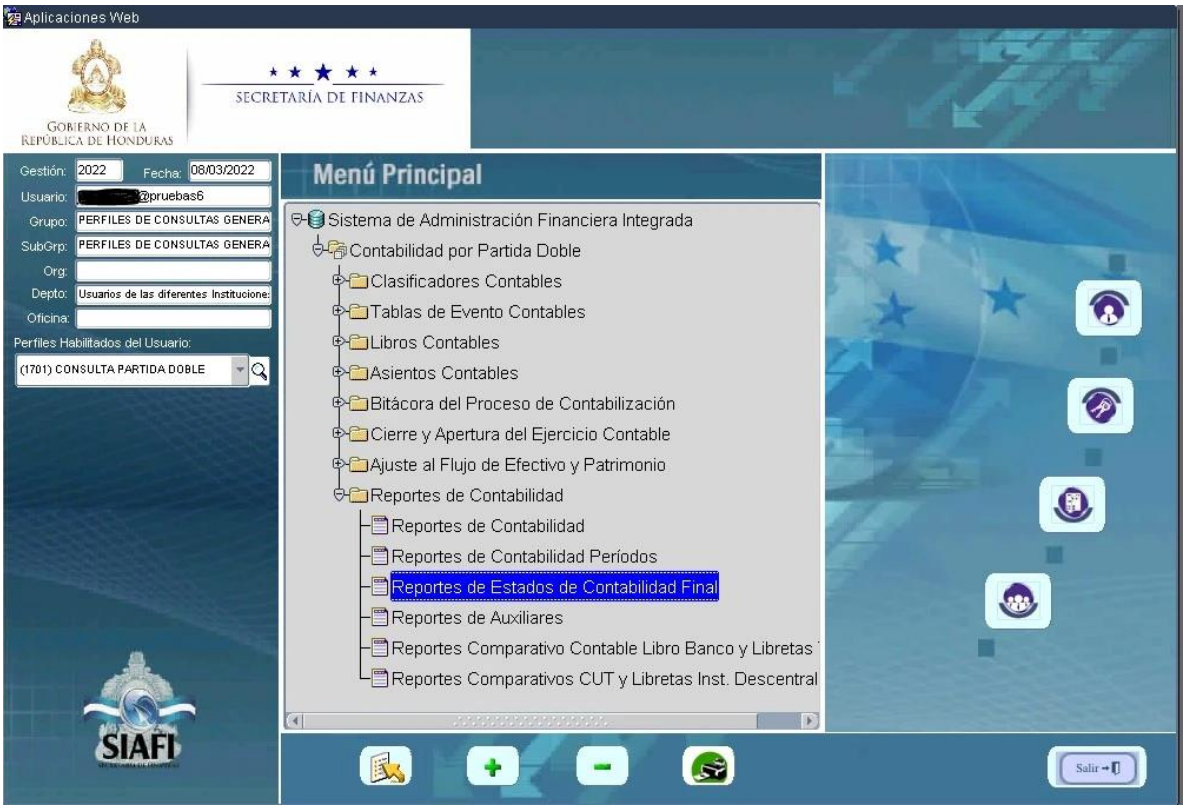
- ¿Cómo elaborar el plan estratégico de TI de una empresa? https://es.snhu.edu/noticias/como-elaborar-un-plan-estrategico-de-ti

- Planificación de Sistemas de Información https://manuel.cillero.es/doc/metodologia/metrica-3/procesos-principales/psi/

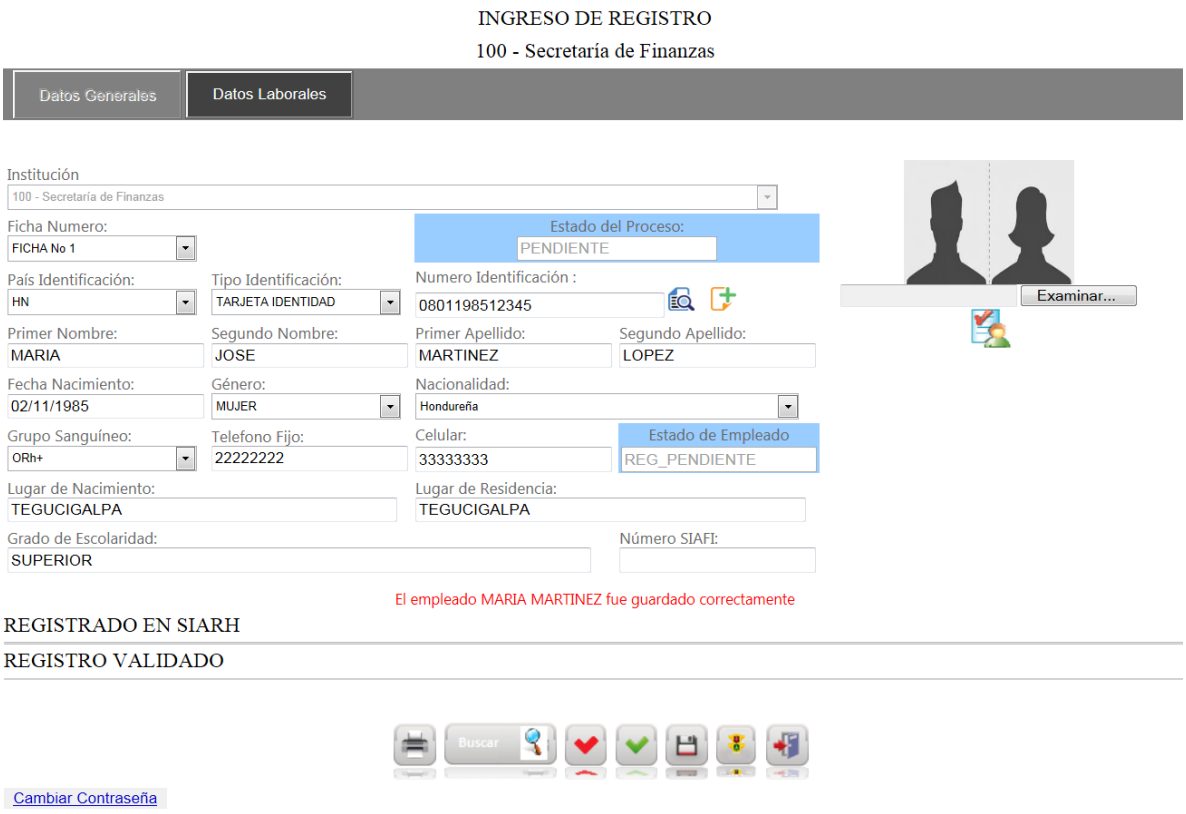
- ¿Qué es gestión de riesgos? https://www.ibm.com/mx-es/topics/risk-management

12. ANEXOS

Sistemas utilizados en la Secretaría de Estado en el Despacho de Seguridad

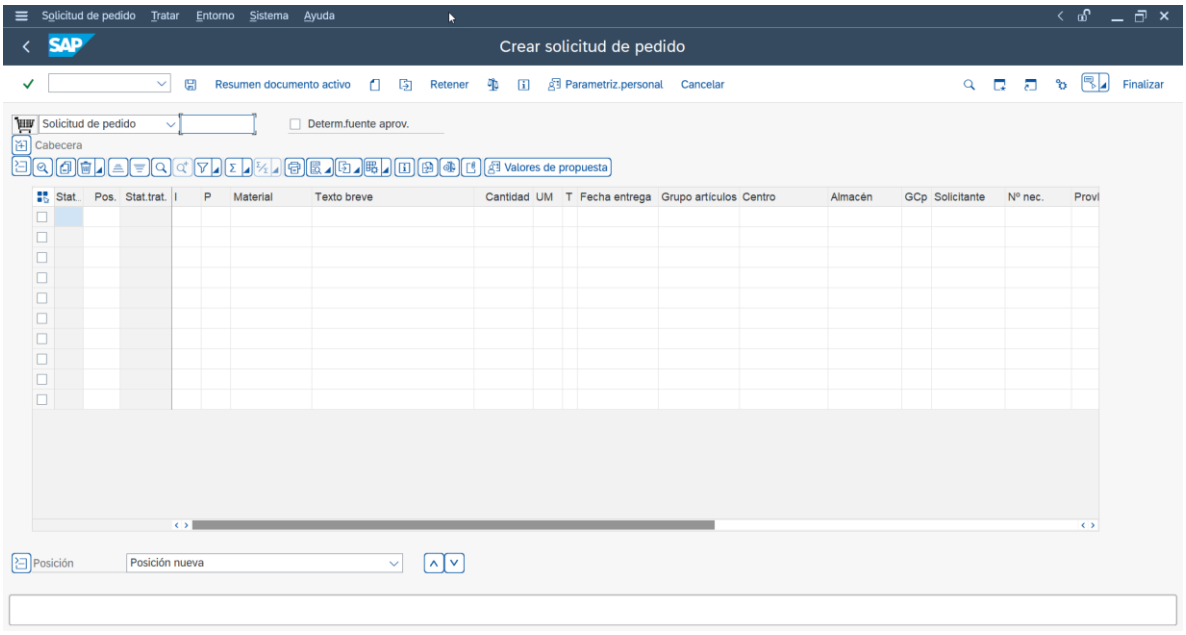


1 Sistema de Administración Financiera Integrada (SIAFI)



2 Sistema de Registro y Control de Servidores (SIREP)

3 DET-Live SAR



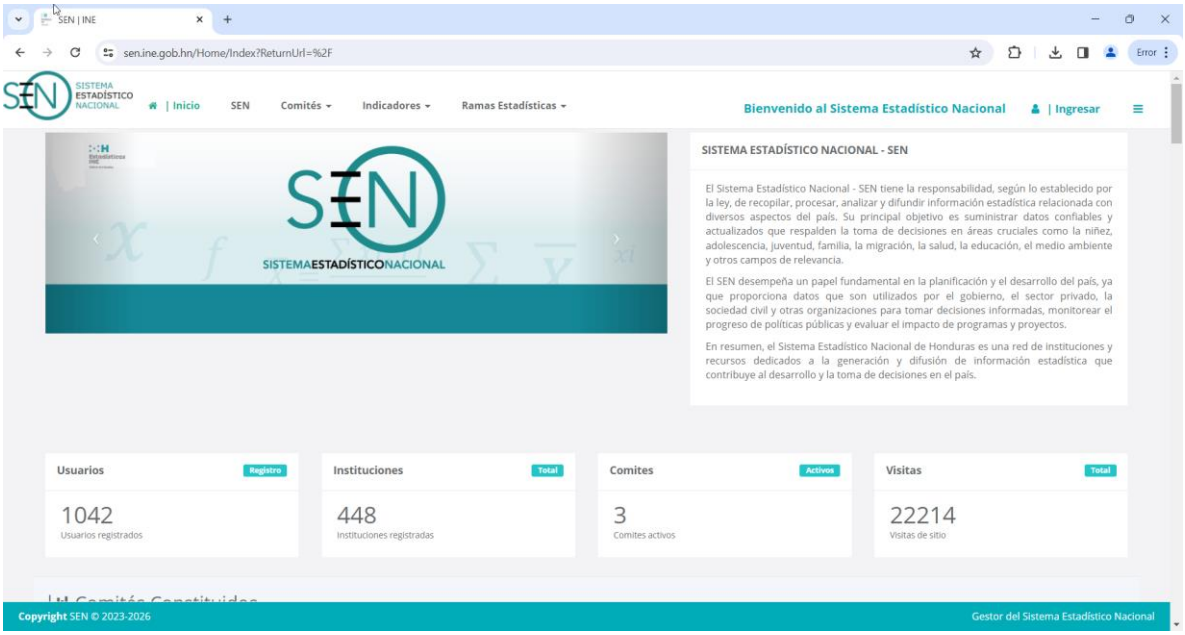
4 SAP ERP

5 Sitio web Secretaría de Seguridad

6 Sitio web Policía Nacional de Honduras

7 Sitio web Sistema Estadístico Policial en Línea (SEPOL)

8 Sistema de Información Electrónico de Honduras (SIELHO)



9 Sistema Estadístico Nacional (SEN)