PLAN ESTRATÉGICO DE TIC 2019-2022

PROYECTO: "DESARROLLO DE PLAN ESTRATÉGICO DE TIC CNE 2019-2022"

COMISIÓN NACIONAL DE PREVENCIÓN DE RIESGO Y ATENCIÓN A EMERGENCIAS

Grupo Empresarial DataSoft

Desarrollado por:

Servicios de Consultoría

Marzo, 2019

VERSIÓN 1.0

IDENTIFICACIÓN DE DOCUMENTO

DATOS DEL DOCUMENTO

Nombre de archivo:	DPETI_CNE_F3_Plan Estratégico de Tecnología de Información_v1.0.docx
Fecha de Creación:	22 de marzo de 2019
Última modificación:	09 de abril de 2019

HISTORIA DE REVISIÓN DEL DOCUMENTO

Fecha	Versión	Actualizado por	Información de los cambios
22 de marzo de 2019	1.0	Datasoft	Desarrollo de la primera Versión

ENTREGA Y ACEPTACIÓN DEL DOCUMENTO

Revisado por CNE	
Nombre:	Firma:
Por DataSoft.:	
Nombre: Randall Abarca Hernández.	Firma:

NOTA DE CONFIDENCIALIDAD

La información incluida en este documento ha sido preparada para ser utilizada en el contexto de este proyecto. No debe ser utilizada como modelo o precedente en ninguna situación fuera del presente proyecto.

Este documento no debe ser copiado o reproducido por ningún medio sin la autorización de las partes involucradas.

Se ha realizado un gran esfuerzo en la preparación de este documento para asegurar que la información presentada es correcta al momento de impresión. Las partes involucradas en este proyecto no asumen ninguna responsabilidad por cualquier error que pueda presentarse en la aplicación de esta información en un contexto diferente al proyecto para el que fue preparado.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Podemos definir la planificación estratégica de TIC como el proceso y la documentación en la que se identifica el portafolio o cartera de servicios (de TIC), aplicaciones y la infraestructura tecnológica que debe desarrollar la Institución para obtener ventajas sostenibles, de acuerdo con la estrategia a nivel general (Plan Estratégico Institucional). En otras palabras, el alineamiento estratégico, es la necesidad de encajar la estrategia de sistemas y tecnologías con la estrategia de la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias, de ahora en adelante CNE, en su conjunto.

El proceso de formular la estrategia para un aprovechamiento efectivo de las tecnologías es complejo, y se debe abordar globalmente, no es una responsabilidad únicamente de la Unidad de Tecnología. Debe atender diferentes dimensiones dentro de un marco general y, por tanto, requiere una combinación de aproximaciones y herramientas. Busca satisfacer a la vez la eficiencia y la efectividad (de las tecnologías) y la obtención de objetivos de valor añadido en términos de competitividad de la Institución. La implementación deberá abordar los temas del futuro inmediato y un horizonte temporal en línea con el horizonte de la estrategia de toda la Institución. Mientras que las aplicaciones críticas resultarán probablemente en sistemas estratégicos, la cartera o portafolio de proyectos tendrá que cubrir necesidades de todos los interesados (unidades o áreas de la Institución). Adicionalmente, es muy posible que se necesite una integración mayor de la información y de los sistemas actuales debido a que siempre existe una infraestructura tecnológica que se hereda en cada ciclo de planificación. Este ciclo de planificación por lo general suele ocurrir en la industria cada 5 años.

ALCANCE DEL PETI

El desarrollo del presente plan estratégico abarca el período comprendido entre el 2019 y el 2022, además, está alineado con el Plan Estratégico Institucional (PEI) de la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias 2018-2022; por lo tanto, los objetivos estratégicos y sus respectivas iniciativas deben estar alineados con los objetivos definidos en el PEI, apoyando y habilitando el cumplimiento de éstos a través de la adopción de las mejores prácticas de la industria para la gestión de la TIC.

BENEFICIOS DE LA PLANEACIÓN Y JUSTIFICACIÓN DEL PETI

A través de la ejecución del proceso de planificación estratégica la organización alcanzará los siguientes beneficios:

- Mejora la contribución de TIC en el funcionamiento de la Institución.

- Permite alinear la inversión de TIC con la estrategia y prioridades del negocio y también reconocer el retorno de la inversión en TIC.
- Se identifican aplicaciones estratégicas y nuevas aplicaciones con un retorno más grande de la inversión.
- Aumenta el involucramiento y compromiso de la alta dirección con TIC.
- Mejora la comunicación y el diálogo con los usuarios.
- Es posible prever las necesidades de recursos de TIC y asignarlos más adecuadamente.
- Se identifica y desarrolla un modelo/arquitectura de información estable y futuro.
- Mejora la visibilidad, el liderazgo y el reconocimiento de TIC en la organización.

METODOLOGÍA UTILIZADA

El proceso de generación del plan estratégico de tecnologías de información y comunicación se puede realizar con aproximaciones, más "tecnológicas" o más "de negocio", más comprensivas (incluyendo las aplicaciones, la infraestructura o todo), más "estratégicas" (globales y a largo plazo, incluyendo la identificación de grandes proyectos críticos) o más tácticas y de continuidad, con mayor o menor detalle. Se debe tener una metodología clara, explícita y discutida con las principales partes interesadas; las expectativas de los interesados serán consideraciones críticas para el éxito del plan, puesto que ayuda a manejar y a tener una visión clara y previa de los objetivos, el alcance y de cómo se ejecutará el plan (la visión conceptual y el plan de trabajo).

De esta manera, en este apartado describiremos la metodología utilizada para el desarrollo del presente plan estratégico de tecnología de información y comunicación. En primera instancia se debe indicar que este plan se realizó aplicando un enfoque basado en proyecto gestionado por las fases del ciclo de vida; la elaboración del plan estratégico de TIC en sí mismo fue un proyecto que contempló sus fases de iniciación, planeación, control y seguimiento, cierre.

Además, la metodología asegura que el plan cumpla con las siguientes características:

Tiene un enfoque de arriba-abajo, toma como punto de partida las prioridades estratégicas de la institución y sus implicaciones para las tecnologías de información y comunicación; sin embargo, se considera lo mejor del enfoque abajo-arriba ya que durante el análisis también se considera la infraestructura tecnológica existente.

Tiene una visión global y orientada a las necesidades de la institución en el contexto de su función de rectoría en el Sistema Nacional de Gestión del Riesgo, de ahora en adelante mencionado como SNGR. Durante sesiones de trabajo con los interesados del Comité Gerencia de TI (en adelante CGTI) no se analizaron cuestiones particulares o detalles sino más bien se propusieron soluciones integrales y concretas que devengue valor y faciliten la consecución de objetivos estratégicos institucionales.

El plan se desarrolló siguiendo un proceso coherente que dividió el trabajo en distintas fases y sesiones con los miembros del CGTI de donde se obtienen piezas o productos que servirán de insumo de las subsecuentes fases; asimismo se obtuvieron resultados coherentes con el plan estratégico instruccional el cual está alineado con los requerimientos del SNGR y su respetivo marco normativo.

El plan estratégico de TIC es el producto de un consenso de miembros del CGTI que contiene representación de todas las áreas de la institución y personal de TIC. Sin embargo, también participó la consultoría o asesoría externa aportando la metodología, neutralidad, documentación

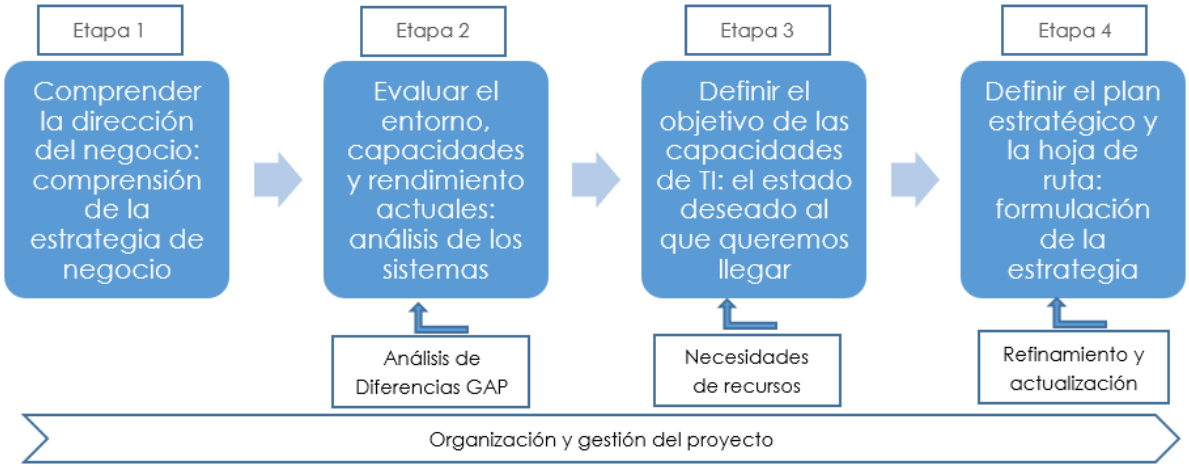
final del plan de forma ágil y finalmente aportar contraste y juicio experto sobre las conclusiones de los equipos.

El plan estratégico de TIC pone el énfasis en la comunicación y en la toma de decisiones. El plan se ha estructurado de tal forma que los productos esperados sean formulados para facilitar el diálogo con las partes interesadas del CGTI.

El plan estratégico de TIC debe facilitar la implantación y la actualización continua de las tecnologías de información en la CNE. El plan no será nunca fijo e inmutable. Las prioridades de gestión cambian o el énfasis varía. De modo que el plan debería desarrollar instrumentos metodológicos que faciliten la revisión y actualización cuando sea procedente. Este plan, en especial la descripción de las iniciativas estratégicas, serán la guía básica o insumo para la formulación y ejecución de los proyectos de TIC.

A continuación, se describen en términos generales, las etapas mediante las cuales se genera el plan PETI 2019-2022.

Figura 1. Etapas del proceso de planificación estratégica.



Fuente: Elaboración Datasoft

Etapa1: El objetivo de esta etapa es reconocer y comprender los objetivos y prioridades del negocio y las implicaciones sobre los sistemas de información y las tecnologías. Para alcanzar este objetivo se realizó un análisis de la documentación existente referente al estado actual de la CNE (Plan Estratégico Institucional, Ley N°8488 Ley Nacional de Emergencia y Prevención del Riesgo y Política Nacional de Gestión del Riesgo).

Etapa 2: El objetivo de esta etapa es la identificación de la situación actual de las TIC (sistemas de información actuales, arquitectura, eficiencia y nivel de servicio, las capacidades y recursos disponibles, el nivel de satisfacción de los usuarios y directivos de negocio). Además, se analizan

las tendencias del sector de la TIC de otras instituciones homólogas a la CNE fuera de nuestro país. Este análisis se realizó considerando las necesidades actuales de la institución y las necesidades futuras detectadas principalmente en la etapa 1. Adicionalmente se realizan sesiones de trabajo en sitio con los miembros de la Unidad de TI para el reconocimiento de la situación actual de la gestión de TIC a través de entrevistas y la aplicación de herramientas para la captura de información.

Etapa 3: El objetivo de esta etapa es la definición del nivel requerido y deseado, de las capacidades y los servicios de TIC; se describen los cambios a alto nivel que se deben realizar para alcanzar este nivel deseado. Para la realización de este objetivo se ejecutan en conjunto con el CGTI, sesiones para la identificación de Fortalezas, Oportunidades, Debilidades y Amenazas; los resultados de este ejercicio se utilizan como insumo para la formulación de aspiraciones estratégicas. Durante este proceso se realiza un recorrido por cada uno de los objetivos estratégicos institucionales contenidos en PEI 2018-2022, analizando el aporte que las TICS pudiesen hacer para cada uno de éstos, así como la identificación de las fortalezas, oportunidades, debilidades y amenazas en los distintos habilitadores tecnológicos (marco normativo, procesos, información, estructura organizativa, cultura-ética-comportamiento, infraestructura, habilidades y competencia).

Etapa 4: Se inicia con la creación de la estrategia futura de la TIC. En esta fase se solicita la participación de los miembros del CGTI para identificar y se definir iniciativas estratégicas que concreten en acciones o herramientas tecnológicas que generen impacto/valor para la Institución (valor en forma de servicios de tecnologías de información).

Finalmente, se les consulta sobre las aspiraciones en materia de tecnologías de información; las aspiraciones estratégicas servirán de insumo para construir una misión, visión de TI y orientar los objetivos estratégicos del plan PETI.

MARCO NORMATIVO APLICABLE

Para el desarrollo del presente plan estratégico de TIC es necesario realizar un reconocimiento de la normativa aplicable tanto para la CNE como para el SNGR, con el objetivo de obtener el mayor grado de alineamiento entre las iniciativas propuestas en plan y los objetivos estratégicos de la institución, los cuales a su vez velarán por el cumplimiento de la normativa aplicable. Por lo tanto; a continuación, se describen políticas, leyes y normativa que alcanza al PETI 2019-2022.

1. LEY N°8488 Ley Nacional de Emergencia y Prevención del Riesgo y Política Nacional de Gestión del Riesgo

Como se menciona en el plan estratégico institucional las competencias ordinarias de la CNE están conferidas en el artículo N°14 y extraordinarias (o de excepción) en el artículo N° 15. Además, la política nacional de gestión del riesgo establece los lineamientos generales para orientar, por un periodo de15 años (2016-2030), la elaboración sucesiva del Plan Nacional de Gestión de Riesgo, a la vez que establece la forma de cómo organizar la ejecución de éstos, para asegurar la fiscalización de las acciones y la medición de los resultados.

Tabla 1. LEY N°8488 Ley Nacional de Emergencia y Prevención del Riesgo y Política Nacional de Gestión del Riesgo

LEY N°8488 Ley Nacional de Emergencia y Prevención del Riesgo y Política Nacional de Gestión del Riesgo	
Declaración	Artículo N°5 - Política de gestión del riesgo. La política de gestión del riesgo constituye un eje transversal de la labor del Estado costarricense; articula los instrumentos, los programas y los recursos públicos en acciones ordinarias y extraordinarias, institucionales y sectoriales, orientadas a evitar la ocurrencia de los desastres y la atención de las emergencias en todas sus fases. Toda política de desarrollo del país debe incorporar tanto los elementos necesarios para un diagnóstico adecuado del riesgo y de la susceptibilidad al impacto de los desastres, así como los ejes de gestión que permitan su control. Artículo N°14. - Competencias ordinarias de prevención de la comisión. Artículo N°15. - Competencias extraordinarias de la Comisión.
Implicación	Estas atribuciones se pueden definir como las actividades sustantivas de la CNE, por lo tanto, el proceso de planificación estratégica de TIC y la gestión de las Tecnología de Información y Comunicación deben estar alineados con la realización y cumplimiento de estas atribuciones,

	tomando en consideración los lineamientos establecidos en la política nacional de gestión del riesgo.

2. Normas Técnicas para la Gestión y el Control de las Tecnologías de Información

Como se indica en el artículo 3 de Las Normas técnicas para la gestión y el control de las tecnologías de información, estas son de acatamiento obligatorio para la Contraloría General de la República y las instituciones y órganos sujetos a su fiscalización.

Tabla 2 Normas Técnicas para la Gestión y el Control de las Tecnologías de Información

Normas Técnicas para la Gestión y el Control de las Tecnologías de Información	
Declaración	**Apartado 1.1 Marco estratégico de TIC.** El jerarca debe traducir sus aspiraciones en materia de TIC en prácticas cotidianas de la organización, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido. **Apartado 1.6 Decisiones sobre asuntos estratégicos de TIC.** El jerarca debe apoyar sus decisiones sobre asuntos estratégicos de TIC en la asesoría de una representación razonable de la organización que coadyuve a mantener la concordancia con la estrategia institucional, a establecer las prioridades de los proyectos de TIC, a lograr un equilibrio en la asignación de recursos y a la adecuada atención de los requerimientos de todas las unidades de la organización. **Apartado 2.1 Planificación de las tecnologías de información.** La organización debe lograr que las TIC apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes.
Implicación	Según el apartado 2.1 de las Normas Técnicas la CNE debe contar con un proceso de planificación estratégica a través del cual logren que la TIC apoye su misión, visión y objetivos estratégicas. Además, los objetivos e iniciativas definidas en el Plan Estratégico de TIC deben incluir en su alcance cerrar cualquier brecha existente para el cumplimiento de esta norma.

3. Reglamento Autónomo de Organización y Servicio de la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias.

Este reglamento tiene como objetivo normar la estructura, las relaciones de jerarquía y la coordinación interna de la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias.

Tabla 3 Reglamento Autónomo de Organización Servicio de la CNE.

Reglamento Autónomo de Organización y Servicio de la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias.	
Declaración	**Artículo 3. – Acatamiento obligatorio.** El cumplimiento de lo dispuesto en este Reglamento es de acatamiento obligatorio para todos los servidores de la CNE, a efecto de llevar a cabo las labores dentro de la armonía requerida de forma eficiente y eficaz.
Implicación	Por tanto, para el desarrollo del presente documento se analizó y consideraron los lineamientos establecidos en el Reglamento Autónomo de Organización y Servicio de la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias.

ANÁLISIS DE SITUACIÓN ACTUAL

INFORMACIÓN GENERAL DE LA ORGANIZACIÓN

La Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (CNE) es la institución pública rectora en lo referente a la coordinación de las labores preventivas de situaciones de riesgo inminente, de mitigación y de respuesta a situaciones de emergencia.

Es un órgano de desconcentración máxima adscrito a la Presidencia de la República, con personería jurídica instrumental para el manejo y la administración de su presupuesto y para la inversión de sus recursos, con patrimonio y presupuesto propio. Su domicilio estará en la capital de la República, donde tendrá su sede principal.

Desde el 2006, el país cuenta con la Ley Nacional de Emergencias y Prevención del Riesgo N° 8488 que supera una serie de vacíos de legislaciones anteriores que limitaban el accionar de la institución.

Introduce, además, el concepto de prevención de riesgo y da un giro en el accionar institucional: regula la actividad extraordinaria que el Estado frente a un estado de emergencia, así como poner en práctica las acciones de prevención en todo el territorio nacional.

También, faculta a la CNE a coordinar el Sistema Nacional de Prevención y Atención de Emergencias, en donde cada institución debe participar en los temas específicos de su competencia y colaborar con los comités locales de prevención de riesgo y atención de emergencias.

OBJETIVO DE DESARROLLO

Fortalecer las capacidades del país en la gestión integral del riesgo, mediante la articulación del Sistema Nacional de Gestión de Riesgo y la aplicación concertada del Plan, orientado a la reducción de la vulnerabilidad para promover un desarrollo seguro y el bienestar de los habitantes.

MARCO FILOSÓFICO DE LA CNE

MISIÓN

La Comisión Nacional de Prevención de Riesgos y Atención de Emergencias es la institución rectora de la política del Estado en Gestión del Riesgo: promueve, organiza, dirige y coordina el funcionamiento del Sistema Nacional de Gestión del Riesgo que contribuye a reducir la vulnerabilidad, salvaguardar la vida y proteger los bienes públicos y privados.

VISIÓN

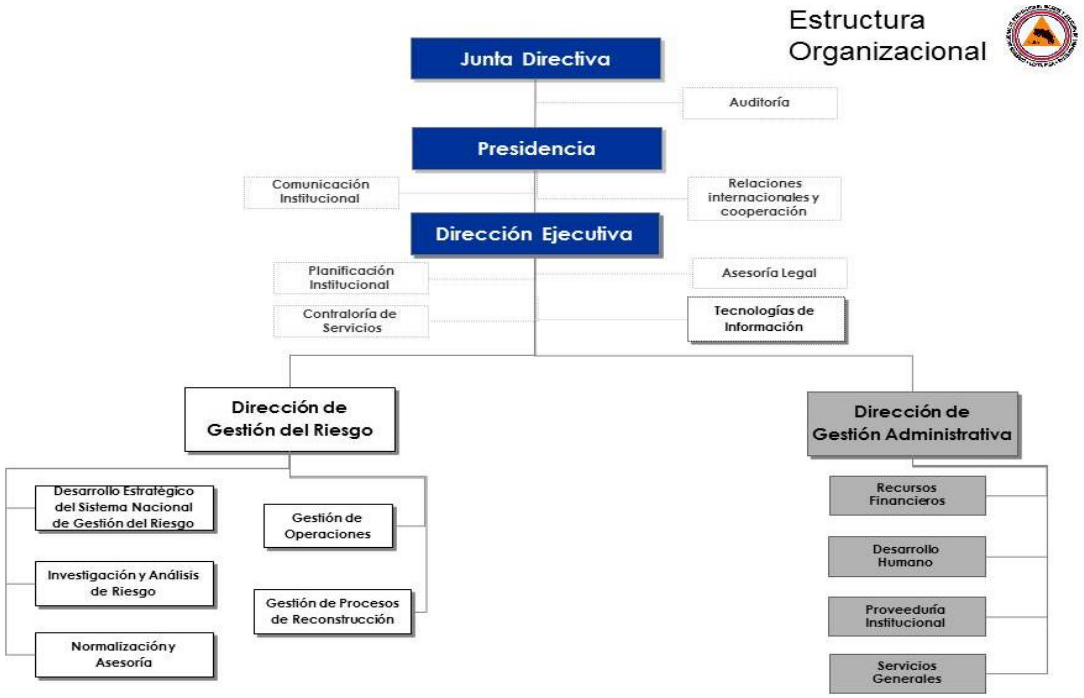
La Comisión Nacional de Prevención de Riesgos y Atención de Emergencias consolidada como ente rector del Sistema Nacional de Gestión del Riesgo, con capacidades materiales, técnicas y humanas para identificar los factores de riesgo, determinar su impacto y adoptar las medidas necesarias para reducirlo, controlarlo y atender sus consecuencias.

VALORES

- Liderazgo: El valor del liderazgo permite a los directores de la institución, así como a la misma entidad marcar el camino, aun en momentos difíciles.
- Solidaridad: El valor de la solidaridad refuerza la conciencia del funcionario para asistir y servir en busca del bienestar de los más necesitados.
- Transparencia: La transparencia es el valor que lleva al funcionario a crear mecanismos eficientes para el manejo de bienes y recursos de la institución. Es al final un medio para rendir cuentas ante los ciudadanos.
- Compromiso: Ser funcionario de la CNE significa asumir un compromiso con la misión de la institución y con el servicio que presta ante las necesidades de la ciudadanía.

ORGANIGRAMA

Figura 2. Organigrama de la CNE.



Fuente: Plan Estratégico Institucional - CNE 2018-2022

PROCESOS DE LA CNE

Como se menciona en el Plan Estratégico Institucional, específicamente en el apartado "Matriz de prioridades institucionales para la gestión estratégica", en la prioridad número dos "Rectoría de la CNE" se establece el producto "Manual de procesos y procedimientos institucionales", lo cual evidencia que la institución reconoce como una oportunidad de mejora la formalización de sus procesos y procedimientos.

Actualmente la CNE cuenta con una identificación inicial de procesos sustantivos y operativos, el Anexo A muestra un resumen de estos procesos y sus procedimientos.

MACROPROCESOS

La siguiente tabla muestra los macroprocesos de la CNE.

Tabla 4 Macroprocesos de la CNE.

Macroprocesos		
Prevención		Toda acción orientada a evitar que los eventos se conviertan en desastres. Procura el control de los elementos conformantes del riesgo, por lo que, por una parte, las acciones se orientan al manejo de los factores de amenaza y, por otra, a los factores que determinan la condición de vulnerabilidad (Art. 4, Definiciones, Ley N°8488).
Preparativos y Respuesta	**Preparativos**	Conjunto de actividades y medidas tomadas previamente, para asegurar una respuesta anticipada y efectiva ante el impacto negativo de un suceso. Incluye, entre otras medidas: la emisión de alertas y el traslado temporal de personas y bienes de una localidad amenazada (Art. 4, Definiciones, Ley N°8488).
	Respuesta	Acciones inmediatas a la ocurrencia de una emergencia; procuran el control de una situación, para salvaguardar obras y vidas, evitar daños mayores y estabilizar el área de la región impactada directamente por la emergencia (Art. 4, Definiciones, Ley N°8488).
Recuperación		Medidas finales que procuran la recuperación del área afectada, la infraestructura y los sistemas de producción de bienes y servicios, entre otros. En general, son acciones que contribuyen a estabilizar las condiciones sociales, económicas y ambientales de las áreas afectadas por una emergencia (Art. 4, Definiciones, Ley N°8488).

PRIORIDADES DE LA INSTITUCIÓN

De acuerdo con lo establecido en el Plan Estratégico Institucional de la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias para el periodo 2018-2022, las prioridades estratégicas de la organización giran alrededor de 4 ejes, los cuales se detallan a continuación:

- **Sistema Nacional de Gestión de Riesgo**

En la perspectiva del cliente, de conformidad con la Ley N° 8488, es importante reconocer que las acciones de servicio de la CNE están orientadas a los diversos actores que interactúan en el marco del Sistema Nacional de Gestión del Riesgo. La competitividad de la CNE de cara al Sistema será demostrada en la medida que logre articular en las instancias de coordinación a los actores, de cara a cumplir con los compromisos del Plan Nacional de Gestión del Riesgo, con estrategias y programas que se orientes a la asesoría, al fortalecimiento de capacidades y organización, a la entrega de la información sobre riesgo necesaria para la toma de decisiones y al monitoreo de sus actividades.

- **Rectoría de la CNE**

En la perspectiva de los procesos internos, la CNE debe ser una institución capaz de ejercer liderazgo a partir de sus competencias de rectoría de la gestión del riesgo y conducción de los procesos de emergencia. Para que ello sea posible los procesos estratégicos, operativos y de apoyo deben ser identificados, es necesaria la generación de nuevos procesos y la reingeniería de los existentes, así como la disposición de un modelo organizacional que responda a una gestión por resultado, es decir, capaz de cumplir con la misión institucional y brindar satisfacción a las demandas de servicio por parte del SNGR. La mejora continua, la innovación, el recurso a nueva tecnología, particularmente de información, el orden y la disposición de los suministros y equipos requeridos para una respuesta ágil y efectiva cercana a los territorios donde se requieren, así como la determinación de nuevas formas de relaciones con organismos que favorezcan el posicionamiento institucional son aspectos a considerar dentro de este eje de prioridades.

- **Ambiente Organizacional**

En la perspectiva de aprendizaje y crecimiento, es evidente que la CNE requiere generar condiciones de infraestructura, de clima organizacional y de capacidades de talento humano para el cumplimiento de sus competencias. La CNE nació al amparo de una Ley que solo demandaba la respuesta a emergencias, hoy en día, habiendo sido modificado ese marco normativo, la institución trabaja con la misma infraestructura y con un modelo de relaciones funcionales que no ha evolucionado a pesar de las nuevas competencias asignadas. Es imperativo generar cambios de cultura organizacional, dotar a los colaboradores de la infraestructura y ambiente apropiado, desarrollar las destrezas y habilidades y el marco normativo necesario par a que la CNE pueda cumplir con su responsabilidad.

- **Recursos Económicos de Gestión de Riesgo**

La perspectiva financiera de la CNE está relacionada con la fuente de recursos que son necesarios para satisfacer las demandas de servicio que tiene a cargo. La CNE recibe pocos recursos del Presupuesto Nacional y depende en gran medida de los recursos que entran al Fondo Nacional de Emergencias. Las complicaciones fiscales de que atraviesa el Gobierno, sumado a las disposiciones que el Ejecutivo adopta para enfrentar los problemas, atenta seriamente con la disponibilidad de los recursos, no solo para la operación ordinaria de la CNE, sino también para la atención de las emergencias que han sido declaradas emergencia nacional. La CNE tiene una fuente de recurso poco estable. En tal sentido, se disponen acciones destinadas a modificar los mecanismos de disposición y uso posible de los recursos, que contribuyan que la gestión del riesgo por medio del SNGR se pueda cumplir y a que la atención de las emergencias cuente con los recursos necesarios. Esto, unido a los avances que se logren en el marco de las prioridades del Ambiente Organizacional debe contribuir a la agilidad y la eficacia en los servicios institucionales.

SITUACIÓN ACTUAL DE LA TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN DE LA CNE

A continuación, se realiza una descripción de la situación actual de la Unidad de TI (UTI), permitiendo a su Jefatura y el CGTI conocer y contrastar las capacidades actuales e identificar la brecha que existe para alcanzar el estado deseado de las tecnologías de información y comunicación en la CNE.

Para el desarrollo del análisis de situación actual se toma como referencia mejores prácticas de la industria para la gobernanza y gestión de la tecnología de información como COBIT 5 e ITIL, marcos regulatorios, como las Normas Técnicas de la Contraloría General de la República. La información obtenida en sesiones de trabajo en conjunto con los miembros de la UTI se organiza de acuerdo a los siete habilitadores de COBIT 5 para el gobierno y la gestión TIC, estos son: principios, políticas y marcos; procesos; estructura organizativa; cultura ética y comportamiento; información; servicios, aplicaciones e infraestructura; personas, habilidades y competencias.

PRINCIPIOS, POLÍTICAS Y MARCOS

Este apartado trata sobre la(s) política(s) aplicadas en CNE para la gestión de las tecnologías de la información; las políticas específicas, la normativa existente, así como las distintas responsabilidades que genera el marco de gestión en materia de TIC.

Basado en los resultados obtenidos luego del reconocimiento de situación actual de la gobernanza y gestión de la TIC en la CNE es posible afirmar que:

- No existe un marco de gestión de TIC formalizado, el cual debería contar con políticas, directrices, procesos y procedimientos para la gestión de la Tecnología de Información y Comunicación.
- Pese a que la organización comprende el valor y la importancia de los servicios de Tecnología de Información y Comunicación, actualmente no se cuenta con un proceso ni procedimiento documentado para la evaluación y monitoreo de la creación y entrega de valor de la TIC para la organización.
- No existe un proceso o procedimiento documentado para la evaluación y monitoreo de la gestión de recursos en TIC.

PLANIFICACIÓN ESTRATÉGICA

Del análisis realizado es posible afirmar que, la UTI de la CNE no cuenta con un proceso, ni procedimientos formalizados para la generación, seguimiento y actualización del plan estratégico de TIC. Además, las responsabilidades de los actores involucrados en el proceso no están claramente identificadas ni comunicadas.

Esta situación implica que los esfuerzos que realiza la UTI para contribuir con el logro misión y los objetivos estratégicos de la institución no puedan ser medidos y comunicados. Lo cual podría impedir la consecución de beneficios como:

- Alineamiento de la inversión de TIC con la estrategia y prioridades del negocio y reconocimiento del retorno de la inversión en TIC.
- Identificación proactiva de aplicaciones estratégicas y nuevas aplicaciones con un retorno más grande de la inversión.
- Involucramiento y compromiso de la alta dirección del negocio con TIC.
- Mejora la comunicación con los usuarios de los servicios que provee la UTI.
- Prevención y asignación oportuna de los recursos de TIC.
- Identificación y desarrollo de un modelo/arquitectura de información estable y futuro.
- Visibilidad, el liderazgo y el reconocimiento de TIC en la organización.

PROCESOS

Este apartado trata sobre la revisión de la existencia de procesos (conjunto de actividades y responsabilidades asociadas para la gestión o consecución de objetivos) para la gobernanza y gestión de las tecnologías información, así como procedimientos documentados más específicos que dicten el cómo se ejecutaran dichas actividades.

Actualmente no existen procesos formalizados para la gobernanza, gestión ni operación de la UTI. Sin embargo, la UTI realizó un esfuerzo inicial para el levantamiento de sus procesos, el cual se utilizó como insumo para la elaboración de la estructura organizativa de TIC.

PROCESO GESTIÓN DE RIESGOS DE TIC

En las Normas técnicas para la gestión y el control de las Tecnologías de Información se indica que "La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TIC, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional (SEVRI) y considere el marco normativo que le resulte aplicable. Respecto a este apartado identifica una oportunidad de mejora pues no es posible identificar un proceso, procedimiento o metodología de gestión de riesgos específico para **la Unidad de Tecnología de Información.**

PROCESO GESTIÓN DE LA CONTINUIDAD DE LOS SERVICIOS DE TIC

No es posible identificar un proceso, procedimiento o práctica relacionado con la continuidad de los servicios de TIC, los cuales son el soporte de los procesos institucionales y a su vez son habilitadores para el cumplimiento de los objetivos de la CNE. Del análisis realizado se puede afirmar que:

- No existe un procedimiento documentado para la gestión de riesgos asociados a la continuidad de los servicios de TIC.
- No existe un procedimiento documentado para la ejecución de un análisis de impacto de negocio, el cual es un insumo para la construcción de un plan de continuidad de servicios de TIC.
- No existe un procedimiento para la identificación y documentación de estrategias de continuidad de los servicios de TIC.
- No se cuenta con un plan de continuidad de los servicios de tecnologías de información y comunicación.

CULTURA, ÉTICA Y COMPORTAMIENTO

Este apartado trata sobre la revisión del factor talento humano de TIC y de la institución. La cultura, ética y comportamiento de los colaboradores de la CNE, debe ser un factor de éxito en las actividades de gobierno y gestión de las tecnologías de la información.

En este particular, los colaboradores de la CNE deben acatar los lineamientos establecidos en el RAOS (Reglamento Autónomo de Servicios y Organización); por esta razón se listan aquellos apartados asociados con el habilitador de Cultura, Ética y Comportamiento:

- El capítulo II "Deberes y Obligaciones de los Servidores, incluye artículos los cuales especificación los deberes y obligaciones de los servidores y titulares subordinas, estos artículos son:
    - Artículo 39 – Deberes y Responsabilidades de los funcionarios.
    - Artículo 40 – Obligaciones de los Titulares Subordinados.
- El capítulo III "De Las Prohibiciones", incluye todas las prohibiciones que deben respetar servidores de la CNE y por tanto aplican a los miembros de la UTI, en este apartado se encuentran los siguientes artículos:
    - Artículo 41 – Prohibiciones a servidores.

No obstante, no existen lineamientos específicos que regulen y dicten un comportamiento ético para el uso responsable de los recursos tecnológicos de la institución.

ARQUITECTURA DE INFORMACIÓN

Este apartado evalúa la existencia de un modelo de arquitectura de información aprobado y comunicado a los miembros de CNE. Es de suma importancia reconocer la información que se gestiona en los procesos o servicios de la institución, los dueños de la información, sus requerimientos de calidad y seguridad e inclusive los criterios de clasificación de ésta. El modelo de gestión y de arquitectura de TIC debe soportar los requisitos generales de arquitectura de la institución.

Los modelos de arquitectura de información incluyen:

- Procesos de la organización-arquitectura de negocio.
- Arquitectura de datos (información).
- Arquitectura de aplicaciones.
- Arquitectura de infraestructura tecnológica.

En el análisis realizado no se identifica un proceso o procedimiento para la definición de la arquitectura de la información. Además, como se mencionó en el apartado de procesos actualmente no existen procesos formalizados a nivel institucional ni a nivel de la UTI. Por lo tanto, tampoco es posible identificar la información que fluye y se transforma a través de estos. Por último, no existe trazabilidad de cómo el modelo de gestión y de arquitectura de TIC soportan los requisitos generales de arquitectura de la institución.

Como se indica en las Normas Técnicas en el apartado 1.4 "Gestión de la seguridad de la información", la organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.

De la evaluación realizada se concluye que en la UTI no se realiza una adecuada identificación, clasificación y etiquetado de los activos de información.

Además, en el apartado 2.2 "Modelo de arquitectura de información" indica que la organización debe optimizar la integración, uso y estandarización de sus sistemas de información de manera que se identifique, capture y comunique, en forma completa, exacta y oportuna, sólo la información que sus procesos requieren. Sobre este apartado es posible afirmar que la institución no cuenta con una arquitectura de información completa, pues aún no hay procesos formalizados.

ESTRUCTURA ORGANIZATIVA

En este apartado reconocemos y analizamos la estructura organizativa existente incluyendo comités, roles y responsabilidades asignadas a cada miembro que corresponda en la CNE; responsabilidades asociadas con la gestión de las tecnologías de la información.

Actualmente la UTI no cuenta con una estructura organizativa definida formalmente, sin embargo, como parte de los productos entregables del proyecto asociado a la contratación 2018CD-000047-0006500001 la empresa adjudica generará una propuesta de estructura organizativa la cual ayude a la UTI a cumplir sus metas y objetivos.

Además, no es posible identificar procedimientos que aseguren la revisión y actualización periódica de la estructura organizativa; tal y como se menciona en el apartado de procesos (página 21), éstos aún no están formalizados.

PERSONAS, HABILIDADES Y COMPETENCIAS

Este apartado versa sobre el reconocimiento y evaluación del estado actual de los controles que aseguren las habilidades y competencias del personal de CNE que gestionan y opera las tecnologías de información

La Unidad de Tecnología de Información de la Comisión Nacional de Prevención de Riesgo y Atención de Emergencias actualmente cuenta con los siguientes perfiles de talento humano:

Tabla 5Talento humano de la UTI

Talento Humano	Perfil de Puesto
Licenciado Gustavo Sánchez Coto	Profesional en Informática - Jefe 1
Licenciado Luis Guillermo Sancho Zeledón	Profesional en Informática 2
Licenciado Daniel Ibarra Miranda	Profesional en Informática 1C
Licenciado Wilgen Saborío Córdoba	Profesional en Informática 1C
Bachiller David Piedra Rojas	Profesional en Informática 1B
Luis Carlos Morales Méndez	Oficinista de Servicio Civil 2

*El departamento cuenta con un manual de cargos el cual es utilizado como referencia (Manual de Clases Anchas de la Dirección General de Servicio Civil), sin embargo, este no refleja las funciones de los roles necesarios para una adecuada gestión y operación de la TIC.

Desarrollo de habilidades y competencias.

En la evaluación del desempeño que se aplica a todos los funcionarios a principio de año, existe un apartado denominado CAPACITACIÓN REQUERIDA POR EL SERVIDOR, donde la jefatura consigna las actividades de capacitación que debería recibir el funcionario evaluado. Esta información la consolida la Unidad de Desarrollo Humano, y de ahí surgen las propuestas de capacitación que serán ejecutadas cada año. Otras capacitaciones que no estén registradas en este instrumento no se tramitan por dicha unidad, salvo excepciones calificadas.

Sin embargo, no fue posible identificar evidencia de la existencia de un procedimiento en la UTI ni herramientas (únicamente el RAOS) para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos de la Unidad de TI. De tal forma que los roles, funciones y las expectativas de desempeño mantengan al personal competente y motivado.

La UTI debería contar con una matriz de responsabilidades y competencias para los distintos roles de TI, ésta debe constituir uno de los principales insumos para la formulación de los planes de desarrollo personal de cada miembro de la UTI y además estar alineado o proporcionar entradas al proceso de gestión de Desarrollo Humano de CNE. La jefatura de la UTI en su rol de administrador tiene la responsabilidad de gestionar su recurso humano, esto incluye el desarrollo de habilidades y competencias.

SERVICIOS, APLICACIONES E INFRAESTRUCTURA DE TIC

Actualmente la UTI no cuenta con un sistema formal para la gestión de Servicios de TIC, tampoco existe un catálogo de servicio formalizado el cual permitiría, entre otras cosas, categorizar los servicios de TIC según la orientación y generación de valor al cliente o usuarios., Además, la inexistencia de un catálogo dificulta que los colaboradores de la CNE perciban el valor que aporta la tecnología de información y comunicación. Del análisis realizado es posible afirmar que la UTI no cuenta con:

- Un proceso y procedimientos documentados para la gestión de acuerdos de nivel de servicio.
- Un proceso y procedimientos documentados para la gestión del portafolio de TIC.
- Un proceso y procedimientos documentados para la gestión del presupuesto y costos de TIC.

- Un proceso y procedimientos documentados para la gestión de proveedores de TIC.
- Un proceso y procedimientos documentados para la gestión de la innovación de TIC.
- Un proceso y procedimientos documentados para la gestión de la disponibilidad y capacidad de los servicios de TIC.
- Un proceso y procedimientos documentados para la gestión de cambios de TIC.
- Un proceso y procedimientos documentados para la gestión del conocimiento.
- Un proceso y procedimientos documentados para la gestión de solicitudes e incidentes de TIC.
- Un proceso y procedimientos documentados para la gestión de problemas de TIC

Sin embargo, existe una identificación informal de los servicios que brinda la UTI, estos servicios se listan a continuación:

- Soporte Técnico.
- Correo electrónico.
- Servicio de gestión de la plataforma tecnológica.
- Servicio de conectividad a la red.
- Servicio de administración de la plataforma Moodle.
- Servicio de administración de página web.
- Servicio de administración del ERP.
- Servicio de control de marcas y asistencia TAS.
- Servicio de gestión de la infraestructura.
- Comunicaciones unificadas.
- Servicio de Impresión.
- Gestión de la Intranet o plataforma de gestión documental.
- Gestión de almacenamiento en la nube.
- Gestión de servicios de red.
- Gestión de antivirus.
- Gestión de actualizaciones de software.

Otro posible inconveniente de la carencia de un catálogo de servicios es la pérdida de trazabilidad de como los servicios que provee la UTI atienden las necesidades y habilitan el logro de la razón de ser de la CNE.

SERVICIOS E INFRAESTRUCTURA

Este apartado incluye la evaluación del estado actual de los componentes de infraestructura, la tecnología y las aplicaciones que proveen el soporte a la información que se gestiona en CNE.

La siguiente tabla muestra la situación actual de los servidores con los que cuenta la UTI de la Comunión Nacional de Prevención de riesgos y Atención de Emergencias.

Tabla 6 Servidores de la UTI

Servidores de la UTI									
Hostname Server	Físico/ Virtual	Versión del hypervisor	Disk GB	Memoria RAM	# Procesadores	Vel. Procesador	IP	Sistema Operativo	Ubicación
CNE-DC-01	Físico	-	500	4	2	2.66	192.168.5.5	Windows Server 2012 R2	Cuarto de Servidores de TIC
CNE-HPV-04	Físico	hyper vi versión 6.3	300	256	4	2.66	192.168.5.67	Windows Server 2012 R2 Datacenter	COE
CNE-HPV-04	Físico	hyper vi versión 6.3	400 (Arreglo)	256	2	2.66		Windows Server 2012 R2 Datacenter	COE
CNE-HPV-09	Físico	hyper vi version 10	600	128	1	3.2	192.168.5.69	Windows Server 2016 Datacenter	COE
CNE-HPV-10	Físico	hyper vi version 10	600	128	1	3.2	192.168.5.69	Windows Server 2016 Datacenter	COE
CNE-UVC-VIDEOENGINE	Virtual	hyper vi versión 6.3	100	6	1	2.7	172.20.1.6	Ubuntu Server 10.04	COE
CNE-UVC-MULTIPOINT	Virtual	hyper vi versión 6.3	100	6	1	2.7	172.20.1.7	Ubuntu Server 10.04	COE
CNE-DRUPAL8-01	Virtual	hyper vi versión 6.3	100	4	1	2.7	172.20.1.3	Ubuntu 16.04	COE
CNE-Edge	Virtual	hyper vi versión 6.3	80	2.5	1	2.7	172.20.1.13	Windows Server 2012 r2 Standard	COE

CNE-LYNC-Web	Virtual	hyper vi versión 6.3	80	2	1	2.7	172.20.1.12	Windows Server 2012 r2 Standard	COE
CNE-OWNCLOUD-01	Virtual	hyper vi versión 6.3	100	2	1	2.7	172.20.1.14	Ubuntu 14.04	COE
CNE-SEGSNGR-01	Virtual	hyper vi versión 6.3	200	2	1	2.7	172.20.1.18	Ubuntu 14.04	COE
CNE-SNGR-WEB	Virtual	hyper vi versión 6.3	100	2	1	2.7	172.20.1.9	Ubuntu 14.04	COE
CNE-ZENTYAL-01	Virtual	hyper vi versión 6.3	100	4	1	2.7	172.20.1.11	ZENTYAL	COE
McaFee Anti SPAM	Virtual	hyper vi versión 6.3	100	4	1	2.7	172.20.1.51	McAfee	COE
REMOTE	Virtual	hyper vi versión 6.3	126	16	1	2.7	172.20.1.21	Windows Server 2012 R2 Standard	COE
CNE-DNS-PUBLICO	Virtual	hyper vi versión 6.3	50	2	1	2.7	172.20.1.5	Windows Server 2008 r2	COE

En la siguiente tabla se muestra la lista de servidores que serán migrados en el año 2019:

Tabla 7 Servidores que serán migrados

Servidores que serán migrados									
Hostname Server	**Físico/Virtual**	**Versión del hypervisor**	**Disk GB**	**Memoria RAM**	**# Procesadores**	**Vel. Procesador**	**IP**	**Sistema Operativo**	**Ubicación**
CNE-FE	Virtual	hyper vi version 6.3	120	8	1	2.2	192.168.5.28	Windows Server 2012 r2 Standard	Cuarto Servidores de TIC
CNE-PrintServer-01	Virtual	hyper vi version 6.3	70	4	1	2.2	192.168.5.27	Windows Server 2008 r2 Enterprise	Cuarto de Servidores TIC
CNE-UNIFI-01	Virtual	hyper vi version 6.3	80	6	1	2.2	192.168.5.160	Windows Server 2012 r2 Standard	Cuarto de Servidores TIC
CNE-1I	Virtual	hyper vi version 6.3	200	8	1	2.2	192.168.5.30	Windows Server 2008 r2 Enterprise	Cuarto de Servidores TIC
CNE-OWAPP-01	Virtual	hyper vi version 6.3	100	8	1	2.2	192.168.5.135	Windows Server 2008 r2 Enterprise	Cuarto de Servidores TIC
CNE-SPWEB-01	Virtual	hyper vi version 6.3	100	8	1	2.2	192.168.5.131	Windows Server 2012 r2 Standard	Cuarto de Servidores TIC
CNE-SPWEB-02	Virtual	hyper vi version 6.3	100	8	1	2.2	192.168.5.132	Windows Server 2012 r2 Standard	Cuarto de Servidores TIC
CNE-SPAPP-01	Virtual	hyper vi version 6.3	100	8	1	2.2	192.168.5.133	Windows Server 2012 r2 Standard	Cuarto de Servidores TIC
CNE-SPAPP-02	Virtual	hyper vi versión 6.3	100	8	1	2.2	192.168.5.134	Windows Server 2012 r2 Standard	Cuarto de Servidores TIC
CNE-SPAPP-03	Virtual	hyper vi versión 6.3	100	8	1	2.2	192.168.5.137	Windows Server 2012 r2 Standard	Cuarto de Servidores TIC
CNE-SPWF-01	Virtual	hyper vi versión 6.3	100	8	1	2.2	192.168.5.136	Windows Server 2012 r2 Standard	Cuarto de Servidores TIC

Servidores que serán migrados

CNE-WSUS	Virtual	hyper vi versión 6.3	600	16	1	2.2	192.168.5.16	Windows Server 2012 r2 Standard	Cuarto de Servidores TIC
CNE-PDQ-01	Virtual	hyper vi versión 6.3	160	16	1	2.2	192.168.5.150	Windows Server 2012 r2 Standard	Cuarto de Servidores TIC
CNE-VPRO	Virtual	hyper vi versión 6.3	120	8	1	2.2	192.168.5.60	Windows Server 2012 r2 Standard	Cuarto de Servidores TIC
CNE-AV-01	Virtual	hyper vi versión 6.3	200	16	1	2.2	192.168.5.12	Windows Server 2016 Standard	Cuarto de Servidores TIC
CNE-Print	Virtual	hyper vi versión 6.3	200	8	1	2.2	192.168.5.26	Windows Server 2016 Standard	Cuarto de Servidores TIC
CNE-WIZDOM-01	Virtual	hyper vi versión 6.3	80	8	1	2.2	192.168.5.140	Windows Server 2012 r2 Standard	Cuarto de Servidores TIC
OPTEC1	Virtual	hyper vi versión 6.3	80	2	1	2.2	192.168.5.104	Windows 7 Professional	Cuarto de Servidores TIC
PC-002375-V	Virtual	hyper vi versión 6.3	150	4	1	2.2	192.168.5.157	Windows 10 Pro	Cuarto de Servidores TIC
CNE-GLOBALX	Virtual	hyper vi versión 6.3	100	2	1	2.2	192.168.5.122	Windows 7 Professional	Cuarto de Servidores TIC
CNE-GLPI-01	Virtual	hyper vi versión 6.3	500	4	1	2.2	192.168.5.14	Ubuntu 14.04	Cuarto de Servidores TIC
CNE-MBX-02	Virtual	hyper vi versión 6.3	140	32	1	2.2	192.168.5.47	Windows Server 2008 r2 Enterprise	Cuarto de Servidores TIC
CNE-Sistemas	Virtual	hyper vi versión 6.3	70	8	1	2.2	192.168.5.3	Windows Server 2008 r2	Cuarto de Servidores TIC
CNE-TASKONTROL-01	Virtual	hyper vi versión 6.3	100	2	1	2.2	192.168.5.155	Windows Server 2008 r2	Cuarto de Servidores TIC
CNE-W7-01	Virtual	hyper vi versión 6.3	100	3	1	2.2	192.168.5.120	Windows 7 Professional	Cuarto de Servidores TIC

Servidores que serán migrados									
AV-TEST	Virtual	hyper vi versión 6.3	70	12	1	2.2	192.168.5.202	Windows Server 2008 r2	Cuarto de Servidores TIC
PRTG	Virtual	hyper vi versión 6.3	126	8	1	2.2	192.168.5.141	Windows Server 2008 r2	Cuarto de Servidores TIC

En la siguiente tabla se muestran los servidores que ingresaran a inicios del año 2019:

Tabla 8 Servidores nuevos

Servidores Ingreso Inicio del 2019										
Hostname Server	**Físico/Virtual**	**Versión del hypervisor**	**Disk GB**	**Memoria RAM**	**# Procesadores**	**Vel. Procesador**	**IP**	**Sistema Operativo**	**Ubicación**	
Pendiente	Físico	Hyper vi pendiente	800	512	2	2.2	Pendiente	Windows Server 2016	Cuarto Servidores de TIC	
Pendiente	Físico	Hyper vi pendiente	800	512	1	2.2	Pendiente	Windows Server 2016	Cuarto de Servidores de TIC	
Pendiente	Físico	Hyper vi pendiente	800	128	1	2.2	Pendiente	Windows Server 2016	Cuarto Servidores de TIC	
Pendiente	Físico	Hyper vi pendiente	800	128	1	2.2	Pendiente	Windows Server 2016	Cuarto de Servidores TIC	

APLICACIONES

Actualmente la UTI cuenta con las siguientes aplicaciones (sistemas informáticos):

Tabla 9 Software de la UTI

Nombre	Servicio TIC	Encargado	Ente Desarrollador	Area usuaria	Servidor	¿En qué está desarrollada?	Donde está en la Institución
CNE Web	Sitio web institucional	Gustavo Sánchez	UTI	Interno y externo	CNE-Web	PHP, MySQL	Centro de datos COE
WIZDOM	ERP	Gustavo Sánchez	OPTEC SISTEMAS	Administrativa, Financiero, Proveeduría y RH	CNE-WIZDOM-01	Power Builder y SQL Server	Centro de Datos TIC

SIGE	Bitácora de Incidentes	Gustavo Sánchez	Proyecto Universitario	Unidad de Gestión de Operaciones	CNE-SQL-01	VB 6.0 y SQL Server	Centro de Datos TIC
Intranet (Plataforma de gestión documental)	SharePoint	Gustavo Sánchez	Microsoft	Todas las Unidades de la CNE	Granja SharePoint	.NET y SQL Server	Centro de Datos TIC
GLPI	Sistema para la Gestión de TIC	Gustavo Sánchez	Insepet Association	UTI	CNE-GLPI-01	PHP y MySQL Server	Centro de Datos TIC
monitor	Sistema de Seguimiento y Monitoreo	Gustavo Sánchez	PREVENTEC	Unidad de Desarrollo Estratégico del SNGR	CNE-SEGSNGR-01	PHP y PostgreSQL Server	Centro de Datos COE
Taskontrol	Control de Asistencia Funcionarios	Gustavo Sánchez	Grupo TAS Corp	Desarrollo Humano	CNE-TASKONTROL	.NET y SQL Server	Centro de Datos TIC

A continuación, se muestra una tabla la cual contiene la información de las bases de datos que son administradas por la UTI de la CNE.

Tabla 10 Bases de datos de la CNE

Nombre Data Base	Aplicaciones	Gestor Versión	Responsable de la BD	Almacenamiento físico	Instancia	Esquema	servidor	Sistema Operativo Servidor
CNEWizdom8	Wizdom 8	SQL Server 2008 R2	Gustavo Sánchez	SAN	CNE-SISTEMAS-01		CNE-SQLC-01	WINDOWS SERVER 2008 R2
SIGE	SIGE	SQL Server 2008 R2	Gustavo Sánchez	SAN	CNE-SISTEMAS-01		CNE-SQLC-01	WINDOWS SERVER 2008 R2
MASTERTAS	TASKONTROL	SQL Server 2008 R2	Gustavo Sánchez	SAN	CNE-SISTEMAS-01		CNE-SQLC-01	WINDOWS SERVER 2008 R2
EmpresasDataDB1	TASKONTROL	SQL Server 2008 R2	Gustavo Sánchez	SAN	CNE-SISTEMAS-01		CNE-SQLC-01	WINDOWS SERVER 2008 R2
CNE_Contenido_Intranet_DB	SharePoint (Plataforma de Gestión Documental)	SQL Server 2014	Gustavo Sánchez	SAN	CNE-SP2013-01\CONTENIDOINT		CNE-SQLC-02	WINDOWS SERVER 2012 R2
CNE_SharePoint_Config	SharePoint (Plataforma de Gestión Documental)	SQL Server 2014	Gustavo Sánchez	SAN	CNE-SP2013-01\CONTENIDOINT		CNE-SQLC-02	WINDOWS SERVER 2012 R2
CNE_Profile_DB	SharePoint (Plataforma de Gestión Documental)	SQL Server 2014	Gustavo Sánchez	SAN	CNE-SP2013-01\CONTENIDOINT		CNE-SQLC-02	WINDOWS SERVER 2012 R2
ReportingService	SharePoint (Plataforma de Gestión Documental)	SQL Server 2014	Gustavo Sánchez	SAN	CNE-SP2013-01\CONTENIDOINT		CNE-SQLC-02	WINDOWS SERVER 2012 R2
SharePoint_AdminContent	SharePoint (Plataforma de Gestión Documental)	SQL Server 2014	Gustavo Sánchez	SAN	CNE-SP2013-01\CONTENIDOINT		CNE-SQLC-02	WINDOWS SERVER 2012 R2
CNE_WSS_Content	SharePoint (Plataforma de Gestión Documental)	SQL Server 2014	Gustavo Sánchez	SAN	CNE-SP2013-01\CONTENIDOINT		CNE-SQLC-02	WINDOWS SERVER 2012 R2
StateService	SharePoint (Plataforma de Gestión Documental)	SQL Server 2014	Gustavo Sánchez	SAN	CNE-SP2013-01\CONTENIDOINT		CNE-SQLC-02	WINDOWS SERVER 2012 R2
MonitorSNGR	Monitor	PostgreSQL 9	Gustavo Sánchez	Disco Virtial del equipo	MonitorSNGR	Public	CNE-SEGSNGR-01	Ubuntu 14.04
GLPI	GLPI	MYSQL SERVER 5	Gustavo Sánchez	Disco Virtial del equipo	GLPI		CNE-GLPI-01	Ubuntu 14.04

La siguiente tabla contiene una descripción del estado actual de los activos de red con los que cuenta la UTI de la CNE.

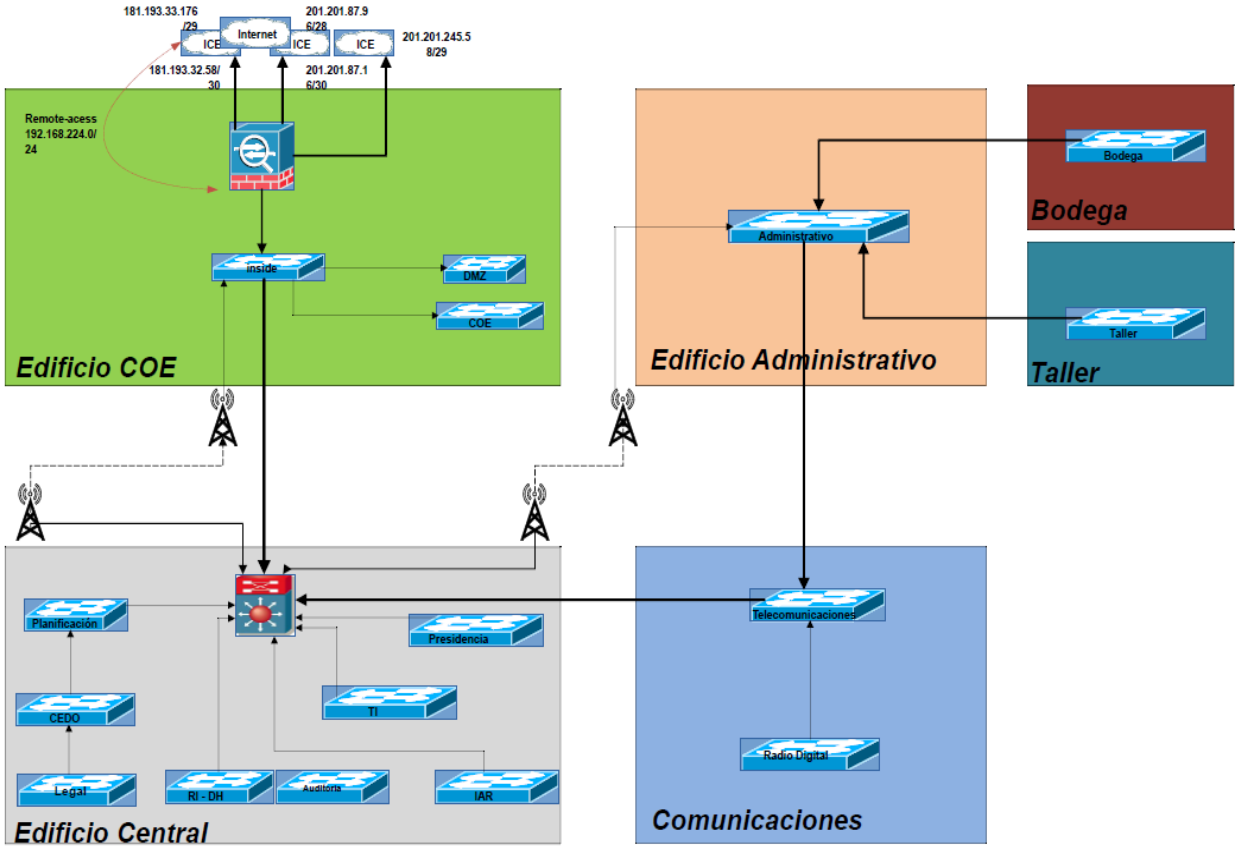
Tabla 11 Activos de red custodiados por la UTI

Marca	Fecha de recepción	Responsable del activo	Ubicación	Segmento de Red
Dell	23/11/2018	Gustavo Sánchez Coto	Centro de Datos TIC	VLAN 4, 8, 12, 13, 25, 30
Dell	23/11/2018	Gustavo Sánchez Coto	Auditoria	VLAN 4, 8, 12, 13, 25, 30
Dell	23/11/2018	Gustavo Sánchez Coto	Investigación y Análisis del Riesgo	VLAN 4, 8, 12, 13, 25, 30
Dell	23/11/2018	Gustavo Sánchez Coto	Presidencia	VLAN 4, 8, 12, 13, 25, 30
Dell	23/11/2018	Gustavo Sánchez Coto	Desarrollo Estratégico	VLAN 4, 8, 12, 13, 25, 30
Dell	23/11/2018	Gustavo Sánchez Coto	Centro de Documentación	VLAN 4, 8, 12, 13, 25, 30
Dell	23/11/2018	Gustavo Sánchez Coto	Asesoría Legal	VLAN 4, 8, 12, 13, 25, 30
Dell	23/11/2018	Gustavo Sánchez Coto	Proceso de Telecomunicaciones	VLAN 4, 8, 12, 13, 25, 30
Dell	23/11/2018	Gustavo Sánchez Coto	Bodega	VLAN 4, 8, 12, 13, 25, 30
Dell	23/11/2018	Gustavo Sánchez Coto	Centro de Datos Edificio COE	VLAN 4, 8, 12, 13, 25, 30
Dell	23/11/2018	Gustavo Sánchez Coto	Edificioicio. Administrativo	VLAN 4, 8, 12, 13, 25, 30
Dell	23/11/2018	Gustavo Sánchez Coto	Centro de Datos TIC	VLAN 4, 8, 12, 13, 25, 30
Dell	23/11/2018	Gustavo Sánchez Coto	Centro de Datos Edificioicio COE	VLAN 4, 8, 12, 13, 25, 30
Dell	23/11/2018	Gustavo Sánchez Coto	Centro de Datos Edificioificio COE	VLAN 4, 8, 12, 13, 25, 30
Dell	23/11/2018	Gustavo Sánchez Coto	Centro de Datos TIC	TODAS LAS VLAN
Dell	23/11/2018	Gustavo Sánchez Coto	Centro de Datos TIC	TODAS LAS VLAN
Dell	23/11/2018	Gustavo Sánchez Coto	Centro de Datos TIC	TODAS LAS VLAN
Dell	23/11/2018	Gustavo Sánchez Coto	Centro de Datos TIC	TODAS LAS VLAN
FORTIGATE	22/12/2017	Gustavo Sánchez Coto	Centro de Datos Edificio COE	TODAS LAS VLAN
FORTIGATE	22/12/2017	Gustavo Sánchez Coto	Edificio.COE	vlan 4 y vlan 30
FORTIGATE	22/12/2017	Gustavo Sánchez Coto	Presidencia	vlan 4 y vlan 30
FORTIGATE	22/12/2017	Gustavo Sánchez Coto	Investigación y Análisis del Riesgo	vlan 4 y vlan 30
FORTIGATE	22/12/2017	Gustavo Sánchez Coto	Asesoría Legal	vlan 4 y vlan 30
FORTIGATE	22/12/2017	Gustavo Sánchez Coto	Pasillo TIC	vlan 4 y vlan 30
FORTIGATE	22/12/2017	Gustavo Sánchez Coto	Bodega	vlan 4 y vlan 30
FORTIGATE	22/12/2017	Gustavo Sánchez Coto	Edificio. Administrativo	vlan 4 y vlan 30
FORTIGATE	22/12/2017	Gustavo Sánchez Coto	Gestion de Procesos de Reconstrucción	vlan 4 y vlan 30
FORTIGATE	22/12/2017	Gustavo Sánchez Coto	Telecomunicaciones	vlan 4 y vlan 30
FORTIGATE	22/12/2017	Gustavo Sánchez Coto	Oficina de TIC	vlan 4 y vlan 30

Tabla 12 VLAN de la UTI

VLAN ID	Descripción	VLAN ID	Descripción
4	Computadoras	17	Respaldos
5	Servidores	18	Video_Vigilancia
8	Teléfonos	25	VC
12	Impresoras	30	Red_Invitados_CNE
13	Administración	31	Invitados_Emergencia
14	Inside_ASA	32	Wan-Invitados
15	ISA_Inside	100	Inside-Internet
16	RADIO_DIGITAL	200	Inside-VPN

Figura 3. Diagrama de Red UTI



Fuente: UTI de la CNE

En este apartado se describe como la UTI responde y da apoyo a las actividades sustantivas de la organización.

Reconociendo cual es la razón de ser la organización y, en concordancia con las atribuciones establecidas en la Ley N°8488, las prioridades definidas en el PEI, y los resultados del análisis de situación actual, se considera que las soluciones de tecnologías de información y comunicación de la CNE soportan principalmente los procesos de apoyo de la institución. En otras palabras, de las aplicaciones identificadas únicamente las siguientes apoyan directamente la misión y razón de ser de la CNE:

- El gestor documental.
- La herramienta de gestión de aprendizaje, Moodle.
- Correo electrónico.
- Sistema Monitor.
- Software de ofimática.
- Acuersoft.
- SIGE.

De forma específica, los objetivos estratégicos y/o actividades sustanciales soportadas por TI son la siguientes:

- Realizar la promoción temática, por medio de programas permanentes de educación y divulgación.
- Promover y apoyar estudios e investigaciones en materias relacionadas con sus fines, así como la elaboración de proyectos que impulsen sistemas físicos, técnicos y educativos orientados a la prevención y mitigación de desastres, y a los preparativos para enfrentarlos.

MARCO ESTRATÉGICO DE LA TIC

MISIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Para contribuir al logro de la misión de la Institución, se definió en conjunto con el CGTI, la siguiente contribución de las Tecnologías de Información a la CNE:

Las tecnologías de información y comunicación gestionadas por la Unidad de TI proveen de servicios de calidad orientados a suplir de forma efectiva las necesidades de la Institución, por medio de habilitadores tecnológicos, la participación en innovación de todos los procesos, la aplicación de las mejores prácticas de TIC, el uso adecuado de la TIC y la integración de la información relevante para para soportar la razón de ser de la CNE.

VISIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Para contribuir al logro de la visión de la Institución, se definió en conjunto con el CGTI, la siguiente visión de las Tecnologías de Información de la CNE:

En el 2022 el proceso de gestión de la TIC será reconocido como un referente de línea estratégica que genera valor en forma de servicios y desarrollo de iniciativas para el cumplimiento de la misión de la CNE.

VALORES DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Para este plan aplican los principios y valores definidos en el Plan Estratégico Institucional 2018-2022. Estos valores guiarán la forma de conducirse de todo el personal de la Institución que utiliza diariamente los servicios de tecnologías de información y comunicación para la ejecución de sus procesos y desempeño de sus funciones, incluyendo por supuesto al personal de la Unidad de TI.

- ***"Liderazgo**: El valor del liderazgo permite a los directores de la institución, así como a la misma entidad marcar el camino, aun en momentos difíciles.*
- ***Solidaridad**: El valor de la solidaridad refuerza la conciencia del funcionario para asistir y servir en busca del bienestar de los más necesitados.*
- ***Transparencia**: La transparencia es el valor que lleva al funcionario a crear mecanismos eficientes para el manejo de bienes y recursos de la institución. Es al final un medio para rendir cuentas ante los ciudadanos.*
- ***Compromiso**: Ser funcionario de la CNE significa asumir un compromiso con la misión de la institución y con el servicio que presta ante las necesidades de la ciudadanía".*

Mediante ejercicio en conjunto con los miembros del CGTI, se realizó un recorrido por cada uno de los objetivos y productos del Plan Estratégico Institucional 2018-2022 con la intención de identificar grado explotación de las tecnologías de la información para cada uno de éstos, así como analizar el entorno externo e interno de la Institución identificado fortalezas, oportunidades, debilidades y amenazas de las tecnologías de información y comunicación en la Institución.

De este ejercicio se obtuvo el siguiente resultado:

Tabla 13 Consolidado de fortalezas – Análisis FODA

Fortalezas
1. Se asignan recursos en el presupuesto institucional para las TIC.
2. Existe capacidad instalada de infraestructura, aplicativos y recurso humano de TIC.
3. Renovación de la infraestructura de TIC, para atender las necesidades actuales de la CNE.
4. Existe un levantamiento inicial de procesos para la Unidad de Tecnologías de Información.
5. Existe apoyo de la administración superior para la adopción de nuevas soluciones tecnológicas.
6. Existe equipo humano capacitado con conocimiento de la institución y el SNGR.
7. Existe una identificación inicial de procesos de negocio (procesos institucionales).
8. La CNE dispone de un marco jurídico para la ejecución de sus competencias.
9. La CNE tiene una alianza con el Sistema Nacional de Información Territorial (SNIT) que faculta la ubicación y publicación de información en el geo portal oficial del estado costarricense.
10. Los usuarios estratégicos y tácticos de la CNE cuentan con dispositivos móviles para la ejecución de sus tareas diarias.
11. El sitio web de la CNE monitorea en tiempo real ciertas amenazas.
12. El área de comunicación institucional hace uso de diferentes medios (escritos, televisión, radial y redes sociales) para comunicar a la población.
13. Existen alianzas con instituciones científico-técnicas que generan información, para el monitoreo de amenazas, alertamiento y toma de decisiones.
14. Se cuenta con la política nacional de riesgo 2016-2030 la cual dicta las pautas de la implementación del SNGR.
15. Existen sistemas de alerta temprana para eventos de origen hidrometereológico.
16. La CNE cuenta con el módulo desarrollado para el Monitoreo del Sistema de Información SNGR (sistema Monitor).
17. Difusión de las alertas según eventos a los actores del SNGR.
18. CNE cuenta con un sistema informático para el seguimiento y monitoreo del cumplimiento de los compromisos del plan y la política de gestión del riesgo (módulo Monitor).

Fortalezas
19. Recientemente la UTI ha instalado y configurado la herramienta denominada GLPI, herramienta de software libre y que permite gestionar inventarios de equipos, incidentes y solicitudes de usuario final. Asimismo, se cuenta con procedimientos documentados para la atención de usuario interno; sin embargo, tanto la herramienta como el procedimiento no han sido oficializados ni comunicados al personal.

Tabla 14 Consolidado de oportunidades – Análisis FODA

Oportunidades
1. Identificar e integrar nuevos actores externos de la CNE que puedan aportar información o recursos al SNGR. 2. Se puede utilizar recursos Tecnológicos de actores relacionados con el SNGR y la cooperación internacional, para la implementación de diferentes programas o proyectos. 3. Potenciar herramientas o plataformas para la información, sensibilización y capacitación de los actores del SNGR, mediante mecanismos de control y seguimiento. 4. Disposición de una norma específica "Ley 8642, artículo 5" la cual indica que la CNE "En caso de declaración de emergencia decretada, conforme al ordenamiento jurídico, el Poder Ejecutivo podrá dictar medidas temporales que deberán ser cumplidas por los operadores, proveedores y usuarios de los servicios de telecomunicaciones. Dichas medidas se adoptarán conforme al marco constitucional vigente. 5. Utilización de plataformas masivas de mensajería. 6. Oportunidad de acondicionar una sala de monitoreo y alerta para observación del territorio nacional y sus amenazas. 7. Revisión de los requerimientos de usuarios del sistema de seguimiento y monitoreo del plan nacional de Gestión de Riesgo. 8. Aprovechamiento de las nuevas tecnologías en videoconferencias para servicio de las necesidades institucionales. 9. Uso de tecnología para el control y seguimiento de activos. 10. Las TIC podrían estar al servicio de la iniciativa de teletrabajo. 11. Herramientas de trabajo colaborativo para aprovechar los dispositivos móviles brindados por la CNE. 12. Posibilidad de actualizar la plataforma administrativa y financiera de la CNE explorando opciones disponibles en el mercado o analizando el recurso existente para realizar desarrollo interno. 13. Existe una iniciativa para aprovechar convenios con el MICITT, SINART y el gobierno de Japón, para el envío de información en situaciones de emergencia a través de la señal de televisión digital abierta.

Oportunidades
14. Definición de la arquitectura de información para todos los módulos de la plataforma del Sistema Nacional de Gestión del Riesgo. 15. En el marco del programa de asesoría se está preparando la malla curricular de la oferta de iniciativas de capacitación para los actores del Sistema Nacional de Gestión del Riesgo. 16. La Unidad de TI trabaja en un proyecto para un sitio alterno de TIC, para garantizar la continuidad del negocio. 17. CNE tiene planificado realizar estudios de percepción sobre necesidades de capacitación y sensibilización. 18. Existe normativa sobre el marco de gestión de las TIC, emitida por la Contraloría General de la República, que debe ser utilizado como insumo para el desarrollo de los procesos de gestión de la Unidad de TI.

Tabla 15 Consolidado de debilidades – Análisis FODA

Debilidades
1. Falta de visión sobre TIC de última generación, las diferentes unidades o áreas de la institución no han tenido participación activa en la identificación de tecnologías invocadores que apoyen a sus procesos. 2. Falta de procedimientos para la operación diaria de la organización. Falta de segregación de tareas y responsabilidades basadas en procesos de negocio. 3. Ausencia de un Plan Estratégico de TIC. 4. CNE no cuenta con un plan de "continuidad de negocio" soportado por un plan de continuidad de los servicios de tecnologías de información. 5. Presupuesto limitado para inversión en tecnologías de información. 6. Sitio Web de CNE con debilidades de usabilidad y acceso a la información requerida por el SNGR. 7. Falta de documentación para la creación y distribución de información a los medios de comunicación del SNGR. 8. Falta de un desarrollo y adopción de herramientas tecnológicas apropiadas para la transferencia de información técnica con instituciones externas. 9. No existe una plataforma de información integrada (solo módulo Monitoreo y Seguimiento) para atender las necesidades del SNGR. 10. No existe una infraestructura de TIC capaz de brindar continuidad a los procesos y servicios de la CNE en caso de eventos disruptivos. 11. No se cuenta con programa de sensibilización y capacitación en tecnologías de información y comunicación que involucre a todo el personal de la institución.

Debilidades

12. No hay marco de gestión de TIC (conjunto de políticas, procesos, procedimientos para administración de las TI) implementado y alineado con los requerimientos normativos aplicables (Normas Técnicas de Gestión y Control de las Tecnologías de Información).
13. No se cuenta con una estructura interna de TIC acorde a las necesidades de la CNE
14. No se cuenta con un contrato de soporte vigente para el soporte, desarrollo y/o mejoras de módulo de Monitoreo y Seguimiento para el SNGR.
15. Falta de política de desarrollo humano para la generación de competencias den el uso y apropiación de las TIC.
16. No se cuenta con instalaciones físicas adecuadas y equipamiento tecnológico dedicado para videoconferencias según requisitos de comunicación de la CNE.
17. Desconocimiento de las capacidades de solución tecnológica existente (implementada actualmente), las áreas usuarias desconocen si la solución permite la trazabilidad, control y seguimiento de los activos de la CNE.
18. Infraestructura inadecuada para las necesidades de la CNE y las instancias del SNGR.
19. Sistema de gestión institucional (ERP) que no se adapta a las necesidades actuales de la institución.
20. Ausencia de documentación de los procesos y procedimientos institucionales, lo cual impide la descentralización (regionalización) de la gestión del riesgo.
21. La organización no ha hecho esfuerzos en la identificación de activos de información y clasificación de la información (nota al pie) para cada uno de los procesos institucionales identificados.
22. Sub utilización del software Acuersoft para el seguimiento de actas y acuerdos.
23. No se cuenta con una herramienta para la gestión de proyectos.
24. Ausencia de controles de seguridad física para la protección de los activos de información en los comités regionales y locales, lo que puede significar la materialización de eventos cuyas consecuencias sean pérdidas financieras, afectación legal o daños a la imagen de CNE.
25. Los requerimientos aún no identificados de capacidad de recursos tecnológicos para el SNGR podrían superar lo proyectado por la Unidad de TI de la CNE.
26. Ausencia de procedimientos para la administración de las bodegas de la CNE y los recursos asignados a cada una de éstas.
27. Los usuarios finales de las tecnologías de información de CNE no cuentan con una interfaz o mesa de ayuda que les facilite el proceso de gestión de sus solicitudes e incidentes.

Tabla 16 Consolidado de amenazas – Análisis FODA

Amenazas
1. Vulnerabilidad multi-amenazas. 2. Pérdida de servicios esenciales de tecnología de información por fallas en suministro eléctrico. 3. Compromiso de la integridad y confidencialidad de información (incluye pérdida, robo, alteración, modificación indebida, fraude). 4. Fallas técnicas provocadas por saturación de sistemas o mal funcionamiento de equipos (procesamiento y telecomunicaciones). 5. Daños a la imagen y el efecto multiplicador de la materialización de una situación de desastre y su impacto para la CNE. 6. El entorno externo a CNE y los requerimientos del SNGR demandan capacidades de TIC. 7. Que el personal capacitado y formado abandone (renuncia) la institución. 8. Probabilidad de poca aceptación de soluciones implementadas por la Unidad de TI debido a la eventual falta de involucramiento o participación de las áreas usuarias durante las fases de diseño (incluye levantamiento de requerimientos) y puesta en marcha.

MATRIZ DE ANÁLISIS FODA PARA LA DETERMINACIÓN DE ACCIONES ESTRATÉGICAS

En este apartado se detalla el resultado obtenido en al análisis (cruce matricial) FODA realizado en conjunto con los miembros del CGTI para la identificación de acciones estratégicas para **aprovechar** oportunidades explotando las fortalezas identificadas; **fortalecer** debilidades a través de oportunidades; **contrarrestar** amenazas con fortalezas y **mejorar** amenazas y debilidades mediante las estrategias identificadas.

Tabla 17 Cruce matricial Oportunidades – Fortalezas: Aprovechar.

Oportunidades – Fortalezas: Aprovechar
1. Potenciar herramientas tecnológicas para la información, sensibilización y capacitación de los actores del SNGR, que permita, además, la generación de métricas e indicadores para el control y seguimiento de su efectividad. 2. Promover un sitio web actualizado, el cual contenga un espacio para la atención de consultas públicas sobre los servicios que brinda la CNE.

Oportunidades – Fortalezas: Aprovechar
3. Establecer y consolidar una sala de monitoreo que permita dar seguimiento a información de carácter científico técnica y que facilite el proceso de toma de decisiones para la prevención del riesgo y atención de emergencias. 4. Buscar recursos de cooperación internacional en pro de la implantación de tecnologías de comunicación que faciliten la colaboración entre los actores del SNGR y las instituciones que proveen información técnica. 5. Aplicar las nuevas tecnologías y herramientas tecnológicas en la reingeniería y automatización de aquellos procesos estratégicos, operativos y de apoyo que lo requieran. 6. Homologar una plataforma de amenazas múltiples aprovechando el potencial de la TIC existentes de forma tal que los actores externos a la CNE y que proveen de información científico-técnica cuenten con un canal estándar de comunicación. 7. Aprovechar el uso de nuevas tecnologías como por ejemplo mapas interactivos, para implementar las estrategias de comunicación y sensibilización requeridas para la gestión del riesgo. **8.** Implementar una herramienta tecnológica (sistema de observación y seguimiento) que les facilite a los gobiernos locales, la captura de información en las fases de prevención, preparativos y respuesta ante emergencias.

Tabla 18 Cruce matricial Amenazas – Fortalezas: Contrarrestar

Amenazas – Fortalezas: Contrarrestar
1. Plan de continuidad (emergencias), el cual contemple estrategias que garanticen la continuidad de los procesos críticos de la CNE. 2. Plan de continuidad de los servicios de TIC integrado con el plan de continuidad institucional. 3. Implementar un proyecto de digitalización del sistema de radio comunicación, de tal forma que se puedan utilizar los canales digitales para la trasferencia de información. 4. Generar un sistema de gestión de conocimiento de TIC integrado con los planes de capacitación y concientización y de conformidad con una de las prioridades para la institución: *"En la perspectiva de aprendizaje y crecimiento, es evidente que la CNE requiere generar condiciones de infraestructura, de clima organizacional y de capacidades de talento humano para el cumplimiento de sus competencias".* 5. Invertir en una infraestructura que permita asegurar la continuidad de negocio durante eventos disruptivos. 6. Plan de mantenimiento para los sistemas de soporte (infraestructura) que proveen servicios esenciales (electricidad, instalaciones, fuentes de agua), tomando en cuenta los criterios técnicos correspondientes.

7. Desarrollar un análisis de capacidades de TIC para determinar si los recursos soportados por la UTI atienden los requisitos actuales y futuros de la CNE y el SNGR.

Tabla 19 Cruce matricial Oportunidades – Debilidades: Fortalecer

Oportunidades – Debilidades: Fortalecer
1. Administrar una planificación financiera de proyectos escalonada según las fechas del PETI. 2. Seleccionar e implementar una solución de Gestión Administrativo Institucional que responda a las necesidades de conformidad con los procesos obtenidos como resultado de la reingeniería mencionada como prioridad para la institución. 3. Definir e implementar procedimientos seguros para la gestión de la información de tal forma que se logre una administración integral de las bodegas de las CNE. 4. Desarrollar una plataforma para el manejo de información en situaciones de emergencia para el Centro de Información y Análisis (CIA). 5. Actualizar el software Acuersoft y capacitar al personal para el uso y adopción de esta herramienta. 6. Desarrollar una metodología para la gestión de proyectos, apoyándose en herramientas tecnológicas para la administración de proyectos. 7. Poner en marcha una herramienta tecnológica (Sistema de Información Territorial de Riesgo a Desastres) para la gestión de la información del modelo de la base datos geográfica sobre pérdidas históricas, la cual implemente tecnologías de geoposicionamiento, utilice lógica de indicadores y método de estimación probabilística de pérdidas del modelo y se integre con el Sistema Nacional de Gestión del Riesgo (módulo de seguimiento y monitoreo y al subsistema de reconstrucción). De conformidad con iniciativa estratégica *"1.2.6. Diseño e instrumentalización de un Sistema de Información Territorial de Riesgo a Desastres con tecnología actualizada"* del PEI. 8. Implementar una mesa de ayuda que provea al usuario final de las tecnologías de información de herramienta técnica, procedimientos y personal de TIC (agentes de soporte) para atender solicitudes y reportes de incidentes.

Tabla 20 Cruce matricial Amenazas – Debilidades: Mejorar

Amenazas – Debilidades: Mejorar
1. Implementar un sistema de gestión de seguridad. (Incluye esfuerzos de clasificación y etiquetado de los activos de información).

2. Implementar y/o fortalecer el marco de gestión de TIC alineado con los requisitos exigidos por las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información" emitidas por la Contraloría General de la República.
3. Utilizar las herramientas tecnológicas existentes para que las distintas áreas o dependencias de la institución cuenten con una interfaz de automatización de procesos y procedimientos, y articulen su catálogo de servicios; de tal forma que se logre una generación de valor a lo largo del flujo de información en los procesos internos.

ASPIRACIONES, INSUMO PARA LA ESTRATEGÍA

En este apartado se abordan las aspiraciones estratégicas del plan; mediante un ejercicio guiado con el CGTI se realiza un recorrido en cascada que utiliza como insumo los productos obtenidos en las etapas anteriores el análisis de situación actual, el análisis FODA, la misión, visión y valores, así como el Anexo 2 Necesidades de las Partes Interesadas del marco de referencia COBIT 5[1]. Las aspiraciones son los bloques que proporcionan contenido a la misión, son más cualitativos y genéricos. Los objetivos han de ser operativos y, por tanto, se tienen que poder convertir en programas o proyectos y su resultado debe ser medido.

De la ejecución del ejercicio en cuestión, se obtienen las siguientes aspiraciones (a fecha 2022 según plan PEI) para las tecnologías de información:

- Las tecnologías de información y comunicación deben ser percibidas en la Institución como un medio imprescindible para la generación de valor y consecución de los objetivos estratégicos.
- Una cultura institucional que se adapte a los cambios constantes y rápidos de TIC, donde los funcionarios sean generadores de cambio, capacitados y motivados para el uso y adopción de las tecnologías de información actuales y las propuestas en el plan estratégico de TIC para el alcance de los objetivos institucionales.
- Mejora de la gestión institucional para contar con procesos estratégicos, operativos y de apoyo, definidos en tecnología o sistemas de información.
- La Unidad de TI debe ser vista como un rol de custodio de la información institucional, debido a que cada miembro de la Institución tiene responsabilidades para la adecuada

[1] COBIT 5 es el marco de gestión y de negocio global para el gobierno y la gestión de las TI de la empresa. Este documento contiene los 5 principios de COBIT 5 y define los 7 catalizadores que componen el marco.

gestión de las tecnologías y de la información que fluye a través de los procesos institucionales.

- Se aspira a poseer sistemas de información y comunicación integrados tanto para la gestión administrativa como para la gestión de los procesos sustantivos de la Institución.
- Se aspira a tecnologías de información y comunicación que soporten y sean generadoras de valor de todos los procesos institucionales.
- La Institución debe tener la capacidad de recuperarse ante un evento adverso mayor generado por multi-amenazas.
- Una cultura ambiental que se apoye en la política institucional e incluya la gestión responsable de las tecnológica de información minimizando el impacto sobre el medio ambiente.

OBJETIVOS ESTRATÉGICOS DE LAS TECNOLOGÍAS DE INFORMACIÓN

Este apartado describe los objetivos estratégicos de las tecnologías de información y comunicación de la CNE para el período 2019-2022. Se utiliza como principal insumo el Plan Estratégico Institucional 2018-2022, teniendo como precedente la política y el plan del Sistema Nacional de Riesgo.

Asimismo, se consideran los resultados de los apartados anteriores obtenidos con la participación de los miembros del CGTI:

- Misión, Visión, Valores de TIC.
- FODA de TIC.
- Matriz de análisis matricial del FODA de TIC.
- Aspiraciones.

Durante este análisis aseguramos que cada objetivo estratégico institucional ha sido revisado, analizado y que se demostrará un claro alineamiento de objetivos de TIC con las necesidades de la Institución y tomando en consideración los aportes de valor del CGTI.

Nota: Debe leerse la siguiente tabla tal cual fue estructurada en el Plan Estratégico Institucional 2018-2022; la redacción de Prioridad, Declaración de rumbo estratégico, Objetivo estratégico institucional ha sido tomada precisamente de este plan.

Tabla 21 Objetivos Estratégicos Prioridad: Sistema Nacional de Gestión del Riesgo.

1. PRIORIDAD: SISTEMA NACIONAL DE GESTIÓN DEL RIESGO
DECLARACIÓN DE RUMBO ESTRATEGICO: Fortaleceremos el SNGR para el cumplimiento de la Política y el Plan Nacional de Gestión del Riesgo
1.1. OBJETIVO ESTRATEGICO INSTITUCIONAL: Fortalecer los mecanismos coordinación del SNGR para el cumplimiento de la Política y el Plan Nacional de Gestión del Riesgo.
1.1.1. Objetivo de TIC: Facilitar mediante herramientas tecnológicas los mecanismos de coordinación del SNGR para el cumplimiento de la Política y el Plan Nacional de Gestión del Riesgo.
1.2. OBJETIVO ESTRATEGICO INSTITUCIONAL: Desarrollar las capacidades del SNGR para el fomento de una cultura proactiva entorno al riesgo de desastres.
1.2.1. Objetivo de TIC: Proveer herramientas tecnológicas que le permitan a la CNE desarrollar las capacidades de la población y de los actores del SNGR para el fomento de una cultura proactiva en torno al riesgo de desastres. **1.2.2. Objetivo de TIC:** Proveer herramientas tecnológicas que faciliten la vigilancia y alertamiento para la activación ante situaciones de riesgo y desastres.
1.3. OBJETIVO ESTRATEGICO INSTITUCIONAL: Verificar el cumplimiento del Plan Nacional de Gestión del Riesgo por ámbitos de gestión.
1.3.1. Objetivo de TIC: Facilitar mediante herramientas tecnológicas el proceso de verificación del cumplimiento del Plan Nacional de Gestión del Riesgo por ámbitos de gestión.

Tabla 22 Objetivos Estratégicos Prioridad: Rectoría de la CNE

2. PRIORIDAD: RECTORÍA DE LA CNE
DECLARACIÓN DE RUMBO ESTRATEGICO: Perfeccionaremos nuestras políticas, procesos y procedimientos, para mejorar la gestión institucional de forma integral y enfoque inclusivo
2.1. OBJETIVO ESTRATEGICO INSTITUCIONAL: Mejorar la gestión institucional para el ejercicio de la rectoría en gestión del riesgo, apoyada por políticas, planificación y asignación de recursos presupuestarios, procesos y procedimientos internos claros que fomenten eficiencia, transparencia, coordinación, uso de tecnología, comunicación efectiva y la inclusividad.
2.1.1. Objetivo de TIC: Facilitar mediante herramientas tecnológicas la gestión institucional para el ejercicio de la rectoría en gestión del riesgo, apoyada por políticas, planificación y asignación de recursos presupuestarios, procesos y procedimientos internos claros que fomenten eficiencia, transparencia, coordinación, uso de tecnología, comunicación efectiva y la inclusividad.

2.1.2. Objetivo de TIC: Aplicar las mejores prácticas y marco normativo de TIC a la gestión institucional para el ejercicio de la rectoría en gestión del riesgo, apoyada por políticas, planificación y asignación de recursos presupuestarios, procesos y procedimientos internos claros que fomenten eficiencia, transparencia, coordinación, uso de tecnología, comunicación efectiva y la inclusividad.
2.2. OBJETIVO ESTRATEGICO INSTITUCIONAL: Orientar las relaciones internacionales y la cooperación en materia de gestión de riesgo.
2.2.1. Objetivo de TIC: Facilitar herramientas tecnológicas para orientar las relaciones internacionales y la cooperación en materia de gestión de riesgo.

Tabla 23 Objetivos Estratégicos Prioridad: Ambiente Organizacional

3. PRIORIDAD: AMBIENTE ORGANIZACIONAL
DECLARACIÓN DE RUMBO ESTRATEGICO: Fortaleceremos el ambiente organizacional y el desarrollo del talento humano, para crear una atmósfera de trabajo saludable.
3.1. OBJETIVO ESTRATEGICO INSTITUCIONAL: Establecer un ambiente de trabajo que favorezca un clima organizacional armónico y saludable en la institución.
3.1.1. Objetivo de TIC: Facilitar herramientas tecnológicas para establecer un ambiente de trabajo que favorezca un clima organizacional armónico y saludable en la institución.
3.2. OBJETIVO ESTRATEGICO: Estimular el talento humano ante los retos de la institución en su ejercicio de rectoría y capacidad de conducción.
3.2.1. Objetivo de TIC: Desarrollar las competencias de TIC para estimular el talento humano ante los retos de la institución en su ejercicio de rectoría y capacidad de conducción.

Tabla 24 Objetivos Estratégicos Prioridad: Recursos Económicos en Gestión del Riesgo

4. PRIORIDAD: RECURSOS ECONÓMICOS EN GESTIÓN DEL RIESGO
DECLARACIÓN DE RUMBO ESTRATEGICO: Encauzaremos esfuerzos tendientes a la obtención de los recursos económicos necesarios, para una gestión integral de riesgo.
4.2. OBJETIVO ESTRATEGICO: Gestionar ante los Organismos de Cooperación los recursos técnicos y financieros, que coadyuven en la consolidación del SNGR.
4.2.1. Objetivo de TIC: Facilitar herramientas tecnológicas para gestionar ante los Organismos de Cooperación los recursos técnicos y financieros, que coadyuven en la consolidación del SNGR.

Tabla 25 Matriz de Planeación Estratégica de TIC, Objetivo estratégicos de TIC alineados con objetivos PEI

1. PRIORIDAD: SISTEMA NACIONAL DE GESTIÓN DEL RIESGO								
DECLARACIÓN DE RUMBO ESTRATEGICO: Fortaleceremos el SNGR para el cumplimiento de la Política y el Plan Nacional de Gestión del Riesgo.								
1.1. OBJETIVO ESTRATEGICO: Fortalecer los mecanismos coordinación del SNGR para el cumplimiento de la Política y el Plan Nacional de Gestión del Riesgo.								
1.1.1 Objetivo TI: Facilitar mediante herramientas tecnológicas los mecanismos coordinación del SNGR para el cumplimiento de la Política y el Plan Nacional de Gestión del Riesgo.					**Cumplimiento Objetivo TI**		**REQUERIDO**	
							100%	
PRODUCTO	**INDICADOR**	**META**	**ACCIÓN (INICIATIVA) ESTRATÉGICA**	**RESPONSABLE**	**META PARA PERÍODO**			**MODO DE VERIFICACIÓN**
					PERÍODO	**AÑO**	**REQUERIDO**	
					Cumplimiento Producto 1		100%	
P1. Herramienta tecnológica para brindar y medir el alcance de la asesoría en materia de Gestión del Riesgo, así como también fortalecer el Sistema Nacional de Gestión del Riesgo mediante capacitación y sensibilización	Porcentaje de implementación de la (s) herramienta (s) según cronograma.	100% del cumplimiento del cronograma	Potenciar herramientas tecnológicas para la información, sensibilización y capacitación de los actores del SNGR, que permita, además, la generación de métricas e indicadores para el control y seguimiento de su efectividad	Jefatura de Tecnologías de Información	La herramienta tecnológica debe estar desarrollada en su totalidad	2019	100%	Avance de actividades ejecutadas/Avance de actividades programadas Registro en la herramienta tecnológica, de las personas e instancias que han recibido capacitación Registro en la herramienta tecnológica, de las comunicades a las que se les ha impartido talleres
	Porcentaje de aulas y cursos creados según programa	100% de cursos/aulas para atender los requerimientos de la institución	Desarrollo de aulas y cursos virtuales para integrarlos con la herramienta tecnológica de tal forma que se pueda brindar asesoría y fortalecer el Sistema Nacional de Gestión del Riesgo mediante capacitación y sensibilización.	Jefatura de Normalización y Asesoría	El 100% de las personas, instancias y comunidades deben ser capacitadas para orientar la gestión de riesgo	2019	100%	Cantidad de cursos o aulas creados/Cantidad de cursos o aulas requeridos
						2020	100%	Cursos o aulas registradas en la herramienta tecnológica
						2021	100%	
						2022	100%	

1. PRIORIDAD: SISTEMA NACIONAL DE GESTIÓN DEL RIESGO								
DECLARACIÓN DE RUMBO ESTRATEGICO: Fortaleceremos el SNGR para el cumplimiento de la Política y el Plan Nacional de Gestión del Riesgo								
1.2. OBJETIVO ESTRATEGICO INSTITUCIONAL: Desarrollar las capacidades del SNGR para el fomento de una cultura proactiva entorno al riesgo de desastres.								
1.2.1. Objetivo de TI: Proveer herramientas tecnológicas que le permitan a CNE desarrollar las capacidades de la población y de los actores del SNGR para el fomento de una cultura proactiva entorno al riesgo de desastres.					**Cumplimiento Objetivo TI**		**REQUERIDO**	
							100%	
PRODUCTO	**INDICADOR**	**META**	**ACCIÓN (INICIATIVA) ESTRATÉGICA**	**RESPONSABLE**	**META PARA PERÍODO**			**MODO DE VERIFICACIÓN**
					PERÍODO	**AÑO**	**REQUERIDO**	
					Cumplimiento Producto 1		100%	
P1. Herramienta tecnológica que sirva como plataforma para recursos de Sensibilización al Riesgo de Desastre.	Porcentaje de implementación de la (s) herramienta (s) según cronograma	100% del cumplimiento del cronograma	Aprovechar el uso de nuevas tecnologías para implementar las estrategias de comunicación y sensibilización requeridas para la gestión del riesgo	Jefatura de Tecnologías de Información	La herramienta tecnológica debe estar desarrollada en su totalidad	2019	100%	Avance de actividades ejecutadas/Avance de actividades programadas
	Cantidad de accesos a los recursos de sensibilización dispuestos en la herramienta	100% de los recursos requeridos institución	Uso de recursos tecnológicos interactivos para desplegarse a través de la plataforma o herramienta tecnológica que debe tener capacidad de registrar y evaluar a las personas.	Jefatura de Comunicación Institucional	El 100% de la población meta de la institución deberá ser sensibilizada por medio de los recursos creados	2019	100%	Registro de acceso a los recursos de sensibilización
						2020	100%	
						2021	100%	
						2022	100%	
					Cumplimiento Producto 2		100%	
P2. Herramienta tecnológica *(Sistema de Información Territorial de Riesgo a Desastres)* para gestión de la información territorial de Riesgo a Desastres.	Porcentaje de implementación de la (s) herramienta (s) según cronograma	100% del cumplimiento del cronograma	Poner en marcha una herramienta tecnológica (Sistema de Información Territorial de Riesgo a Desastres) para la gestión de la información del modelo de la base datos geográfica sobre pérdidas históricas, la cual implemente tecnologías de geoposicionamiento, lógica de indicadores y método de estimación probabilística de pérdidas del modelo y se integre con el Sistema Nacional de Gestión del Riesgo (módulo de seguimiento y monitoreo y al subsistema de reconstrucción).	Jefatura de Tecnologías de Información	La herramienta tecnológica debe estar desarrollada en su totalidad	2019	100%	Avance de actividades ejecutadas/Avance de actividades programadas
	Cantidad de actores o instituciones reportando en la Sistema de Información Territorial de Riesgo a Desastres	100% de los actores requeridos por la Institución deben registrar en el Sistema de Información Territorial de Riesgo a Desastres	Las instituciones deben realizar registros regulares sobre pérdidas y daños en el Sistema de Información Territorial de Riesgo a Desastres.	Dirección de Gestión del Riesgo	El 100% de las instituciones requeridas por la institución reportando en la herramienta tecnológica	2019	100%	Cantidad de actores registrados en el sistema/Cantidad de actores requeridos en el sistema
						2020	100%	Registro de actores en la herramienta
						2021	100%	
						2022	100%	

1.2.2. Objetivo de TI: Proveer herramientas tecnológicas que faciliten la vigilancia y alertamiento para la activación ante desastres.					Cumplimiento Objetivo TI		REQUERIDO 100%	ALCANZADO 0%	
PRODUCTO	INDICADOR	META	ACCIÓN (INICIATIVA) ESTRATÉGICA	RESPONSABLE	META PARA PERÍODO				MODO DE VERIFICACIÓN
					PERÍODO	AÑO	REQUERIDO	ALCANZADO	
					Cumplimiento Producto 1		100%	0%	
P1. Herramientas tecnológicas para Sistema de Vigilancia y Alertamiento	Porcentaje de cumplimiento de cronograma de implementación	100% del cumplimiento del cronograma	Implantación de tecnologías de comunicación que faciliten la colaboración entre los actores del SNGR y las instituciones que proveen información técnica; por medio de homologación de una plataforma de amenazas múltiples y un canal estándar de comunicación con la CNE.	Jefatura de Tecnologías de Información	La herramienta tecnológica debe estar desarrollada en su totalidad	2019	100%	0%	Avance de actividades ejecutadas/Avance de actividades programadas
	Cantidad de actores registrados usando la herramienta tecnológica	100% de los actores requeridos institución	Los actores del SNGR articulados en sistemas de alerta y activación que deben recibir información en tiempo real para el alertamiento y activación ante desastres.	Jefatura de Gestión de Operaciones	El 100% de los actores requeridos por la institución deben estar registrados en la herramienta	2019	100%	0%	Cantidad de actores registrados en el sistema/Cantidad de actores requeridos en el sistema
						2020	100%	0%	Registro de actores en la herramienta
						2021	100%	0%	
						2022	100%	0%	
					Cumplimiento Producto 2		100%	0%	
P2. Plataforma para el manejo de información en situaciones de emergencia para el CIA	Porcentaje de cumplimiento de cronograma de implementación	100% del cumplimiento del cronograma	Desarrollar una plataforma para el manejo de información en situaciones de emergencia para el Centro de Información y Análisis (CIA).	Jefatura de Tecnologías de Información	La herramienta tecnológica debe estar desarrollada en su totalidad	2020	100%	0%	Avance de actividades ejecutadas/Avance de actividades programadas
					Cumplimiento Producto 3		100%	0%	
P3. Sala o centro de monitoreo	Porcentaje de cumplimiento de cronograma de implementación	100% del cumplimiento del cronograma	Establecer y consolidar una sala de monitoreo que permita dar seguimiento a información de carácter científico técnica y que facilite el proceso de toma de decisiones para la prevención del riesgo y atención de emergencias.	Jefatura de Tecnologías de Información Jefatura de Gestión de Operaciones	La debe estar equipada con hardware y software al 100% según cronograma	2020	20%	0%	Avance de actividades ejecutadas/Avance de actividades programadas
						2021	40%	0%	
						2022	40%	0%	

1. PRIORIDAD: SISTEMA NACIONAL DE GESTIÓN DEL RIESGO								
DECLARACIÓN DE RUMBO ESTRATEGICO: Fortaleceremos el SNGR para el cumplimiento de la Política y el Plan Nacional de Gestión del Riesgo								
1.3. OBJETIVO ESTRATEGICO INSTITUCIONAL: Verificar el cumplimiento del Plan Nacional de Gestión del Riesgo por ámbitos de gestión.								
1.3.1. Objetivo de TI: Facilitar mediante herramientas tecnológicas el proceso de verificación del cumplimiento del Plan Nacional de Gestión del Riesgo por ámbitos de gestión.					**Cumplimiento Objetivo TI**		**REQUERIDO**	
							100%	
PRODUCTO	**INDICADOR**	**META**	**ACCIÓN (INICIATIVA) ESTRATÉGICA**	**RESPONSABLE**	**META PARA PERÍODO**			**MODO DE VERIFICACIÓN**
					PERÍODO	**AÑO**	**REQUERIDO**	
					Cumplimiento Producto 1		100%	
P1. Herramienta tecnológica para el seguimiento del cumplimiento del Plan Nacional de Gestión del Riesgo	Porcentaje de implementación de la (s) herramienta (s) según cronograma	100% del cumplimiento del cronograma	Asegurar la intregración y/o actualización del Sistema de Seguimiento y Monitoreo mediante la creación de un modelo de información y arquitectura para el SNGR que considere el sistema Monitor existente y todos los módulos o subsistemas así como los requisitos actuales y futuros del SNGR.	Jefatura de Tecnologías de Información	La herramienta tecnológica debe ser integrada a los módulos o subsistemas del SNGR. Por tanto el modelo de arquitectura e integración debe desarrollarse en su totalidad.	2019	100%	Avance de actividades ejecutadas/Avance de actividades programadas

2. PRIORIDAD: RECTORÍA DE LA CNE									
DECLARACIÓN DE RUMBO ESTRATEGICO: Perfeccionaremos nuestras políticas, procesos y procedimientos, para mejorar la gestión institucional de forma integral y enfoque inclusivo.									
2.1. OBJETIVO ESTRATEGICO INSTITUCIONAL: Mejorar la gestión institucional para el ejercicio de la rectoría en gestión del riesgo, apoyada por políticas, planificación y asignación de recursos presupuesatrios, procesos y procedimientos internos claros que fomenten eficiencia, transparencia, coordinación, uso de tecnología, comunicación efectiva y la inclusividad.									
2.1.1. Objetivo de TI: Facilitar mediante herramientas tecnológicas la gestión institucional para el ejercicio de la rectoría en gestión del riesgo, apoyada por políticas, planificación y asignación de recursos presupuestarios, procesos y procedimientos internos claros que fomenten eficiencia, transparencia, coordinación, uso de tecnología, comunicación efectiva y la inclusividad.					**Cumplimiento Objetivo TI**		**REQUERIDO**	**ALCANZADO**	
							100%	**0%**	
PRODUCTO	**INDICADOR**	**META**	**ACCIÓN (INICIATIVA) ESTRATÉGICA**	**RESPONSABLE**	**META PARA PERÍODO**				**MODO DE VERIFICACIÓN**
					PERÍODO	**AÑO**	**REQUERIDO**	**ALCANZADO**	
					Cumplimiento Producto 1		100%	0%	
P1. Herramienta tecnológica para el seguimiento y evaluación de la planificación y presupuestación.	Porcentaje de implementación de la (s) herramienta (s) según cronograma	100% del cumplimiento del cronograma	Herramienta tecnológica para el establecimiento de un modelo de gestión por resultados	Jefatura de Tecnologías de Información Jefatura de Planificación Institucional	La herramienta tecnológica debe estar desarrollada en su totalidad	2019	100%	0%	Avance de actividades ejecutadas/Avance de actividades programadas
					Cumplimiento Producto 2		100%	0%	
P2. Herramienta tecnológica para la gestión de procesos y procedimientos institucionales.	Porcentaje de implementación de la (s) herramienta (s) según cronograma	100% del cumplimiento del cronograma	Utilizar las herramientas tecnológicas de tipo BMP y las plataforma existentes (intranet) para que las distintas áreas o dependencias de la institución cuenten con una interfaz de automatización de procesos y procedimientos, y articulen su catálogo de servicios; de tal forma que se logre una generación de valor a lo largo del flujo de información en los procesos internos.	Jefatura de Tecnologías de Información	La herramienta tecnológica debe estar desarrollada en su totalidad	2019	100%	0%	Avance de actividades ejecutadas/Avance de actividades programadas
	Porcentaje de avance en la aplicación de la herramienta para la automatización de procesos y servicios	100% de los proceoss requeridos por la Institución deben ser automatizados mediante la herramienta(s)	Aplicar las nuevas tecnologías y herramientas tecnológicas en la reingeniería y automatización de aquellos procesos estratégicos, operativos y de apoyo que lo requieran.	Jefatura de todas las Unidades	El 100% de aquellos procesos y servicios que se puedan automatizar en la herramienta (s)	2019	25%	0%	Cantidad de procesos y servicios implementados/Cantidad de actores requeridos en el sistemaCantidad de procesos y servicios requeridos
						2020	25%	0%	
						2021	25%	0%	
						2022	25%	0%	
					Cumplimiento Producto 3		100%	0%	
P3. Herramienta tecnológica para la Gestión Administrativo Institucional	Porcentaje de implementación de la (s) herramienta (s) según cronograma	100% del cumplimiento del cronograma	Seleccionar e implementar una solución de Gestión Administrativo Institucional que responda a las necesidades de conformidad con los procesos.	Jefatura de Tecnologías de Información Dirección Ejecutiva Dirección Gestion de Riesgo Dirección Gestión Administrativa	La herramienta tecnológica debe estar desarrollada en su totalidad	2020	50%	0%	Avance de actividades ejecutadas/Avance de actividades programadas
						2021	50%	0%	

					Cumplimiento Producto 4		100%	0%	
P4. Herramientas tecnológicas actualizadas que sirvan de canal de comunicación con la población	Porcentaje avancen de actualizacipon de la (s) herramienta (s) según cronograma	100% del cumplimiento del cronograma	Promover un sitio web actualizado, el cual contenga un espacio para la atención de consultas públicas sobre los servicios que brinda la CNE.	Jefatura de Tecnologías de Información Jefatura Todas las Unidades	La herramienta(s) tecnológica (s) debe(n) actualizarse en su totalidad	2020	100%	0%	Avance de actividades ejecutadas/Avance de actividades programadas
					Cumplimiento Producto 5		100%	0%	
P5. Equipos y herramientas de tecnología actualizados.	Porcentaje de actualización de equipos	100% de necesidades de tecnología de información de la institución atendida	Actualizar los equipos y herramientas tecnológicas de la CNE.	Jefatura de Planificación Institucional	Actualizar en un 100% de los equipos y herramientas tecnológicas de la CNE.	2019	25%	0%	Cantidad de equipos actualizados/Cantidad de equipos requeridos
						2020	25%	0%	
						2021	25%	0%	
						2022	25%	0%	
2.1.2. Objetivo de TI: Aplicar las mejores prácticas y marco normativo de TI a la gestión institucional para el ejercicio de la rectoría en gestión del riesgo, apoyada por políticas, planificación y asignación de recursos presupuestarios, procesos y procedimientos internos claros que fomenten eficiencia, transparencia, coordinación, uso de tecnología, comunicación efectiva y la inclusividad.					**Cumplimiento Objetivo TI**		**REQUERIDO**	**ALCANZADO**	
							100%	**0%**	
PRODUCTO	**INDICADOR**	**META**	**ACCIÓN (INICIATIVA) ESTRATÉGICA**	**RESPONSABLE**	**META PARA PERÍODO**				**MODO DE VERIFICACIÓN**
					PERÍODO	**AÑO**	**REQUERIDO**	**ALCANZADO**	
					Cumplimiento Producto 1		100%	0%	
P1. Implementación de Normas Técnicas para Gestión de TI	Porcentaje de implementación de procesos	100% de los procesos según Normas Técnicas de TI deben implementarse	Implementar y/o fortalecer el marco de gestión de TIC alineado con los requisitos exigidos por las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información" emitidas por la Contraloría General de la República.	Jefatura de Tecnologías de Información	Marco estratégico y gobierno de TI. Catálogo de servicios de servicios, calidad de servicios	2019	25%	0%	Cantidad de procesos implementados/Cantidad de procesos requeridos
					Procesos de gestión de riesgos de TI y seguridad informática	2020	25%	0%	
					Procesos de gestión de continuidad de servicios de TI	2021	25%	0%	
					Procesos de gestión de proyectos	2022	25%	0%	
					Cumplimiento Producto 2		100%	0%	
P2. Implementación de Sistema de Gestión de Continuidad de Negocio	Porcentaje de implementación del sistema de continuidad según cronograma	100% del cumplimiento del cronograma	Plan de continuidad institucional, el cual contemple estrategias que garanticen la continuidad de los procesos críticos de la CNE	Dirección Ejecutiva	Análisis de riesgos de continuidad	2019	25%	0%	Avance de actividades ejecutadas/Avance de actividades programadas
					Definición de BIA, procesos críticos	2020	25%	0%	
					Definición de estrategias y procedimientos alternativos	2021	25%	0%	
					Implementación de la estrategia de continuidad	2022	25%	0%	
					Cumplimiento Producto 3		100%	0%	
P3. Implementación de Sistema de Seguridad de la Información	Porcentaje de implementación del sistema de seguridad de la información, según cronograma	100% del cumplimiento del cronograma	Implementar un sistema de gestión de seguridad. (Incluye esfuerzos de clasificación y etiquetado de los activos de información).	Dirección Ejecutiva	Un sistema de gestión de seguridad con controles físicos y lógicos deben estar operando en la Institución	2020	50%	0%	Avance de actividades ejecutadas/Avance de actividades programadas
						2021	50%	0%	

2. PRIORIDAD: RECTORÍA DE LA CNE									
DECLARACIÓN DE RUMBO ESTRATEGICO: Perfeccionaremos nuestras políticas, procesos y procedimientos, para mejorar la gestión institucional de forma integral y enfoque inclusivo.									
2.2. OBJETIVO ESTRATEGICO: Orientar las relaciones internacionales y la cooperación en materia de gestión de riesgo.									
2.2.1 Objetivo TI: Facilitar las herramientas tecnológicas que soporten la estrategia de relaciones internacionales y la cooperación en materia de gestión de riesgo.					**Cumplimiento Objetivo TI**		**REQUERIDO**	**ALCANZADO**	
							100%	**0%**	
PRODUCTO	**INDICADOR**	**META**	**ACCIÓN (INICIATIVA) ESTRATÉGICA**	**RESPONSABLE**	**META PARA PERÍODO**				**MODO DE VERIFICACIÓN**
					PERÍODO	**AÑO**	**REQUERIDO**	**ALCANZADO**	
					Cumplimiento Producto 1		100%	0%	
P1. Relaciones internacionales y cooperación para recursos tecnológicos	Número de actores internacionales y de cooperación que se relacionan con la CNE aportando recursos para la implantación de tecnologías para el fortalecimiento del SNGR.	Al menos un actor internacional y de cooperación que se relacionan con la CNE aportando recursos para la implantación de tecnologías para el fortalecimiento del SNGR.	Buscar recursos de cooperación internacional en pro de la implantación de tecnologías de información y comunicación que faciliten la colaboración entre los actores del SNGR y las instituciones que proveen información técnica	Jefatura de Relaciones Internacionales y Cooperación	Un actor internacional y de cooperación que se relacionan con la CNE aportando recursos para la implantación de tecnologías para el fortalecimiento del SNGR.	2019	1	0	Cantidad de actores que relacioandos con CNE y SNGR/Cantidad de actores requeridos

3. PRIORIDAD: AMBIENTE ORGANIZACIONAL								
DECLARACIÓN DE RUMBO ESTRATEGICO: Fortaleceremos el ambiente organizacional y el desarrollo del talento humano, para crear una atmósfera de trabajo saludable.								
3.1. OBJETIVO ESTRATEGICO INSTITUCIONAL: Establecer un ambiente de trabajo que favorezca un clima organizacional armónico y saludable en la institución.								
3.1.1 Objetivo TI: Facilitar herramientas tecnológicas para establecer un ambiente de trabajo que favorezca un clima organizacional armónico y saludable en la institución.				**Cumplimiento Objetivo TI**			**REQUERIDO**	
							100%	
PRODUCTO	**INDICADOR**	**META**	**ACCIÓN (INICIATIVA) ESTRATÉGICA**	**RESPONSABLE**	**META PARA PERÍODO**			**MODO DE VERIFICACIÓN**
					PERÍODO	**AÑO**	**REQUERIDO**	
					Cumplimiento Producto 1		100%	
P1. Herramientas tecnológicas para fortalecer clima organizacional	Porcentaje de implementación de la (s) herramienta (s) según cronograma	100% del cumplimiento del cronograma	Promover la adopción de Herramientas tecnológicas de trabajo colaborativo que favorezcan un clima organizacional armónico y saludable en la institución. Considerar herramientas para teletrabajo.	Jefatura de Tecnologías de Información	Las herramientas tecnológicas deben implementarse en su totalidad	2020	100%	Avance de actividades ejecutadas/Avance de actividades programadas
					El 100% de los colaboradores que requiera la Institución deben usar las herramientas	2021	100%	Cantidad de colaboradores que usan las herramientas/Cantidad de colaboradores requeridos
					El 100% de los colaboradores que requiera la Institución deben usar las herramientas	2022	100%	

3. PRIORIDAD: AMBIENTE ORGANIZACIONAL									
DECLARACIÓN DE RUMBO ESTRATEGICO: Fortaleceremos el ambiente organizacional y el desarrollo del talento humano, para crear una atmósfera de trabajo saludable.									
3.2. OBJETIVO ESTRATEGICO INSTITUCIONAL: OBJETIVO ESTRATEGICO: Estimular el talento humano ante los retos de la institución en su ejercicio de rectoría y capacidad de conducción.									
3.2.1 Objetivo TI: Desarrollar las competencias de TIC para estimular el talento humano ante los retos de la institución en su ejercicio de rectoría y capacidad de conducción.					**Cumplimiento Objetivo TI**		**REQUERIDO**	**ALCANZADO**	
							100%	**0%**	
PRODUCTO	**INDICADOR**	**META**	**ACCIÓN (INICIATIVA) ESTRATÉGICA**	**RESPONSABLE**	**META PARA PERÍODO**				**MODO DE VERIFICACIÓN**
					PERÍODO	**AÑO**	**REQUERIDO**	**ALCANZADO**	
					Cumplimiento Producto 1		100%	0%	
P1. Desarrollo Humano con competencias en tecnologías de información y comunicación	Porcentaje de colaboradores del la CNE con las competencias TIC requeridas	100% de los colaboradores requeridos por la Institución	Generar un sistema de gestión de conocimiento de TI integrado con los planes de capacitación y concientización y de conformidad con una de las prioridades (Ambiente organizacional) para la institución: *"En la perspectiva de aprendizaje y crecimiento, es evidente que la CNE requiere generar condiciones de infraestructura, de clima organizacional y de capacidades de talento humano para el cumplimiento de sus competencias"*	Jefatura de Desarrollo Humano Jefatura de Tecnologías de Información	Diagnóstico de necesidades de capacitación y formación en TICs incluido en programa de inducción, capacitación y formación de CNE.	2019	100%	0%	Diagnóstico y plan de capacitación
					El 100% de los colaboradores que requiera la Institución deben capacitarse en TIC.	2020	100%	0%	Cantidad de colaboradores que se capacitan/Cantidad de colaboradores requeridos
					El 100% de los colaboradores que requiera la Institución deben capacitarse en TIC.	2021	100%	0%	
					El 100% de los colaboradores que requiera la Institución deben capacitarse en TIC.	2022	100%	0%	

4. PRIORIDAD: RECURSOS ECONÓMICOS EN GESTIÓN DEL RIESGO									
DECLARACIÓN DE RUMBO ESTRATEGICO: Encauzaremos esfuerzos tendientes a la obtención de los recursos económicos necesarios, para una gestión integral de riesgo.									
4.2. OBJETIVO ESTRATEGICO: Gestionar ante los Organismos de Cooperación los recursos técnicos y financieros, que coadyuven en la consolidación del SNGR.									
4.2.1 Objetivo TI: Facilitar herramientas tecnológicas para gestionar ante los Organismos de Cooperación los recursos técnicos y financieros, que coadyuven en la consolidación del SNGR.					**Cumplimiento Objetivo TI**		**REQUERIDO**	**ALCANZADO**	
							100%	**0%**	
PRODUCTO	**INDICADOR**	**META**	**ACCIÓN (INICIATIVA) ESTRATÉGICA**	**RESPONSABLE**	**META PARA PERÍODO**				**MODO DE VERIFICACIÓN**
					PERÍODO	**AÑO**	**REQUERIDO**	**ALCANZADO**	
					Cumplimiento Producto 1		100%	0%	
P1. Herramientas tecnológicas para la gestión de proyectos	Porcentaje de implementación de la (s) herramienta (s) según cronograma	100% del cumplimiento del cronograma	Desarrollar una metodología para el proceso de gestión de proyectos, apoyándose en herramientas tecnológicas para su automatización.	Jefatura de Tecnologías de Información	Las herramientas tecnológicas deben estar implementadas en su totalidad	2019	100%	0%	Avance de actividades ejecutadas/Avance de actividades programadas
	Porcentaje de proyectos gestionados mediante las herramientas tecnológicas	100% de cursos/aulas para atender los requerimientos de la institución	Cartera de proyectos de cooperación internacional gestionada mediante herramientas tecnológicas.	Jefatura de Relaciones Internacionales y Cooperación.	El 100% de los proyectos requeridos por la Institución deben utilizar las herramientas tecnológicas	2019	100%	0%	Cantidad de proyectos gestionados mediante la herramienta tecnológica/Cantidad de proyectos requeridos
						2020	100%	0%	
						2021	100%	0%	
						2022	100%	0%	

CUMPLIMIENTO DE ACCIONES ESTRATÉGICAS

Oportunidades – Fortalezas: Aprovechar	Cumplimiento
1. Potenciar herramientas tecnológicas para la información, sensibilización y capacitación de los actores del SNGR, que permita, además, la generación de métricas e indicadores para el control y seguimiento de su efectividad.	Objetivo TIC: 1.1.1 Producto: 1
2. Promover un sitio web actualizado, el cual contenga un espacio para la atención de consultas públicas sobre los servicios que brinda la CNE.	Objetivo TIC: 2.1.1 Producto: 4
3. Establecer y consolidar una sala de monitoreo que permita dar seguimiento a información de carácter científico técnica y que facilite el proceso de toma de decisiones para la prevención del riesgo y atención de emergencias.	Objetivo TIC: 1.2.2 Producto: 3
4. Buscar recursos de cooperación internacional en pro de la implantación de tecnologías de comunicación que faciliten la colaboración entre los actores del SNGR y las instituciones que proveen información técnica.	Objetivo TIC: 2.2.1 Producto: 1
5. Aplicar las nuevas tecnologías y herramientas tecnológicas en la reingeniería y automatización de aquellos procesos estratégicos, operativos y de apoyo que lo requieran.	Objetivo TIC: 2.2.1 Producto: 1 y Producto: 2
6. Homologar una plataforma de amenazas múltiples aprovechando el potencial de la TIC existentes de forma tal que los actores externos a la CNE y que proveen de información científico-técnica cuenten con un canal estándar de comunicación.	Objetivo TIC: 1.2.2 Producto: 1
7. Aprovechar el uso de nuevas tecnologías como por ejemplo mapas interactivos, para implementar las estrategias de comunicación y sensibilización requeridas para la gestión del riesgo.	Objetivo TIC: 1.2.1 Producto: 1
8. Implementar una herramienta tecnológica (sistema de observación y seguimiento) que les facilite a los gobiernos locales, la captura de información en las fases de prevención, preparativos y respuesta ante emergencias.	Objetivo TIC: 1.3.1 Producto: 1

Amenazas – Fortalezas: Contrarrestar	Cumplimiento
1. Plan de continuidad institucional (emergencias), el cual contemple estrategias que garanticen la continuidad de los procesos críticos de la CNE.	Objetivo TIC: 2.1.2 Producto: 2
2. Plan de continuidad de los servicios de TIC integrado con el plan de continuidad institucional.	Objetivo TIC: 2.1.2 Producto: 2, incluir en plan operativo
3. Implementar un proyecto de digitalización del sistema de radio comunicación, de tal forma que se puedan utilizar los canales digitales para la trasferencia de información.	Objetivo TIC: 1.2.2 Producto: 1, incluir en plan operativo
4. Generar un sistema de gestión de conocimiento de TIC integrado con los planes de capacitación y concientización y de conformidad con una de las prioridades para la institución: *"En la perspectiva de aprendizaje y crecimiento, es evidente que la CNE requiere generar condiciones de infraestructura, de clima organizacional y de capacidades de talento humano para el cumplimiento de sus competencias"*, prioridad Ambiente organizacional, plan estratégico institucional.	Objetivo TIC: 3.2.1 Producto: 1
5. Invertir en una infraestructura que permita asegurar la continuidad de negocio durante eventos disruptivos.	Objetivo TIC: 2.1.2 Producto: 1, incluir en plan operativo
6. Plan de mantenimiento para los sistemas de soporte (infraestructura) que proveen servicios esenciales (electricidad, instalaciones, fuentes de agua), tomando en cuenta los criterios técnicos correspondientes.	Objetivo TIC: 2.1.2 Producto: 3
7. Desarrollar un análisis de capacidades de TIC para determinar si los recursos soportados por la UTI atienden los requisitos actuales y futuros de la CNE y el SNGR.	Objetivo TIC: 2.1.2 Producto: 2

Oportunidades – Debilidades: Fortalecer	Cumplimiento
1. Administrar una planificación financiera de proyectos escalonada según las fechas del PETI.	Objetivo TIC: 2.1.1 Producto: 3
2. Seleccionar e implementar una solución de Gestión Administrativo Institucional que responda a las necesidades de conformidad con los procesos obtenidos como resultado de la reingeniería mencionada como prioridad para la institución.	Objetivo TIC: 2.1.1 Producto: 3
3. Definir e implementar procedimientos seguros para la gestión de la información de tal forma que se logre una administración integral de las bodegas de las CNE.	Objetivo TIC: 2.1.1 y 2 Producto: 3
4. Desarrollar una plataforma para el manejo de información en situaciones de emergencia para el Centro de Información y Análisis (CIA).	Objetivo TIC: 1.2.2 Producto: 1
5. Actualizar el software Acuersoft y capacitar al personal para el uso y adopción de esta herramienta.	Objetivo TIC: 3.2.1 Producto: 1
6. Desarrollar una metodología para el proceso de gestión de proyectos, apoyándose en herramientas tecnológicas para su automatización.	Objetivo TIC: 4.2.1 Producto: 1
7. Poner en marcha una herramienta tecnológica (Sistema de Información Territorial de Riesgo a Desastres) para la gestión de la información del modelo de la base datos geográfica sobre pérdidas históricas, la cual implemente tecnologías de geoposicionamiento, utilice lógica de indicadores y método de estimación probabilística de pérdidas del modelo y se integre con el Sistema Nacional de Gestión del Riesgo (módulo de seguimiento y monitoreo y al subsistema de reconstrucción). De conformidad con iniciativa estratégica *"1.2.6. Diseño e instrumentalización de un Sistema de Información Territorial de Riesgo a Desastres con tecnología actualizada"* del PEI.	Objetivo TIC: 1.2.1 Producto: 2
8. Implementar una mesa de ayuda que provea de una herramienta técnica, procedimientos y personal de TIC (agentes de soporte) para atender solicitudes y reportes de incidentes de usuario final de las tecnologías de información y comunicación.	Objetivo TIC: 2.1.2 Producto: 1

Amenazas – Debilidades: Mejorar	Cumplimiento
1. Implementar un sistema de gestión de seguridad. (Incluye esfuerzos de clasificación y etiquetado de los activos de información).	Objetivo TIC: 2.1.2 Producto: 3
2. Implementar y/o fortalecer el marco de gestión de TIC alineado con los requisitos exigidos por las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información" emitidas por la Contraloría General de la República.	Objetivo TIC: 2.12 Producto: 1
3. Utilizar las herramientas tecnológicas existentes para que las distintas áreas o dependencias de la institución cuenten con una interfaz de automatización de procesos y procedimientos, y articulen su catálogo de servicios; de tal forma que se logre una generación de valor a lo largo del flujo de información en los procesos internos.	Objetivo TIC: 2.1.1 Producto: 2

ARQUITECTURA

La arquitectura empresarial (como se le conoce formalmente en la industria) es una metodología que, basada en una visión integral permite alinear procesos, datos, aplicaciones e infraestructura tecnológica con los objetivos estratégicos de la Institución o con la razón de ser de ésta. Su principal objetivo es garantizar la correcta alineación de la tecnología y los procesos institucionales, con el propósito de alcanzar el cumplimiento de sus objetivos estratégicos. Esta arquitectura debe definir situación actual y el objetivo de la arquitectura de las tecnologías para los dominios negocio, información, datos, aplicaciones y tecnología.

Con el presente plan estratégico de TIC es evidente que se requiere aplicar cambios a la arquitectura existente en CNE de forma tal que las tecnologías de información permitan alcanzar el cumplimiento de los objetivos estratégicos globales; así como sentar las bases o principios que guiarán la arquitectura durante el período de vigencia de dicho plan. Este apartado del documento describe la arquitectura empresarial sugerida (con conocimiento previo del contexto institucional) a CNE para soportar el Plan Estratégico de TIC 2019-2022.

El desarrollo o actualización de la arquitectura empresarial y de información permitirá a la CNE dar cumplimiento a las Normas técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), Capítulo II Planificación y organización, específicamente: "*2.2 Modelo de arquitectura de información y 2.3 Infraestructura tecnológica.*" Asimismo, las recomendaciones expresadas en este apartado se han considerado las mejores prácticas del marco de referencia internacional en arquitectura empresarial TOGAF®[2].

Con base en dicho marco, se plantea este procedimiento que contiene los siguientes elementos:

1. Principios.
2. Dominios.
3. Base de conocimiento de cada Dominio:
    a. Lineamientos.
    b. Estándares.
    c. Mejores prácticas.
    d. Normativa aplicable.

[2] El Marco de Arquitectura de Grupo Abierto (TOGAF) es un marco para la arquitectura empresarial que proporciona un enfoque para el diseño, planificación, implementación y gobierno de una arquitectura de tecnología de la información empresarial.

Los principios de Arquitectura Empresarial son reglas de alto nivel que guiarán a la Institución en la toma de decisiones relacionadas con TIC. La Arquitectura Empresarial contempla principios generales y principios específicos:

- Principios generales de la arquitectura
- Principios del dominio de estrategia TIC
- Principios del dominio de gobierno TIC.
- Principios del dominio datos e información
- Principios del dominio de aplicaciones (sistemas)
- Principios del dominio de tecnología (infraestructura)

Principios generales de la arquitectura de TIC de CNE

Excelencia al servicio del SNGR: Servicios de tecnologías de información al servicio de los distintos actores y ciudadanos que interactúan con el SNGR.

Inversión con buena relación costo/beneficio: Propender porque las inversiones de TIC representen un retorno medido, por el impacto de los proyectos.

Racionalización: Buscar la optimización en el uso de los recursos teniendo en cuenta criterios de pertinencia y reutilización.

Estandarización: Desarrollar soluciones o herramientas tecnológicas que permitan la base para la definición de los lineamientos, políticas y procedimientos que faciliten la homologación de una plataforma de amenazas múltiples.

Interoperabilidad: Fortalecer los esquemas de interoperabilidad que estandaricen y faciliten el intercambio de información entre actores del SNGR, manejo de fuentes únicas de información y la habilitación de servicios.

Co-creación: Permitir componer nuevas soluciones tecnológicas y servicios sobre lo ya construido y definido con la participación de todos aquellos actores involucrados en el SNGR.

Escalabilidad: Permitir la evolución continua y la adición de todos los componentes y dominios que lo componen, sin perder calidad ni articulación.

Seguridad de la Información: Permitir la definición, implementación y verificación de controles de seguridad de la información.

Sostenibilidad: Aportar al equilibrio ecológico por medio de las TIC.

Los dominios son dimensiones desde las cuales la Institución podrá organizar su gestión estratégica de TIC. Agrupan y organizan los objetivos, áreas y temáticas relativas a las TIC. Cada dominio contiene su propio portafolio de instrumentos y herramientas de gestión TIC que le permitirán a la Institución implementar los requisitos.

Dominio arquitectura de negocio:

Esta categoría de arquitectura está compuesta por los siguientes elementos:

- Estrategia de TIC: Define estándares y lineamientos, para diseñar la estrategia de TIC y lograr su alineación con las estrategias a nivel Institucional.
- Gobierno de TIC: Define estándares y lineamientos para diseñar e implementar esquemas de gobernabilidad de TIC; alinear los procesos de la Institución con los requerimientos del SNGR y los procesos para la gestión de TIC; definición de estructura organizacional de TIC; y definición de procesos entre ellos la gestión de proveedores y la gestión de proyectos.

Dominio arquitectura de información:

Esta categoría de arquitectura está compuesta por los siguientes elementos:

- Dominio de Información: Define estándares y lineamientos para la gestión de información como principal generador de valor estratégico para la Institución. Comprende la definición de los siguientes aspectos: diseño de los servicios de información, la gestión de la calidad de ésta, la gestión del ciclo de vida de los datos y de información, el análisis de información y el desarrollo de capacidades para el uso estratégico de ésta.
- Servicios Tecnológicos: Define estándares y lineamientos para la gestión de la infraestructura tecnológica que soporta los sistemas y los servicios de información, así como los servicios requeridos para su operación. Comprende la definición de la infraestructura tecnológica, la gestión de la capacidad de los servicios de TIC, la gestión de la operación y la gestión de los servicios de soporte.

Dominio arquitectura de aplicaciones (sistemas):

Define estándares y lineamientos para la gestión de los sistemas de información, incluyendo su arquitectura, ciclo de vida, las aplicaciones que los conforman y los procesos de implementación y soporte.

Dominio arquitectura de servicios tecnológicos:

Define estándares y lineamientos para la gestión de la infraestructura tecnológica que soporta los sistemas y los servicios de información, así como los servicios requeridos para su operación. Comprende la definición de la infraestructura tecnológica, la gestión de la capacidad de los servicios de TIC, la gestión de la operación y la gestión de los servicios de soporte.

FUNDAMENTOS PARA LOS DOMINIOS DE ARQUITECTURA

La base de conocimiento de los dominios de una arquitectura empresarial son un conjunto de instrumentos y herramientas que guían y ayudan a la Institución en la implementación y cumplimiento de la estrategia de tecnologías de información.

Cada dominio de arquitectura empresarial demuestra los siguientes fundamentos:

1. Principios: Son una orientación de carácter general, corresponden a una disposición o directriz que orientan la implementación de la estrategia del plan.

2. Estándares: Especificaciones técnicas que tienen una función instrumental y que responden a cómo se implementa un principio o elemento.

3. Mejores prácticas: Identifica y relaciona la mejor práctica aplicable para apoyar o implementar en el dominio. Las mejores prácticas generalmente se encuentran en los marcos como COBIT, ITIL[3], normas ISO[4]. Se recomienda a la CNE utilizar estas mejores prácticas como referencia, adoptar lo mejor de éstas a la gestión de las tecnologías de información en la Institución; se agrega TOGAF® como marco de Arquitectura Empresarial que nos permitirá dividir la arquitectura en dominios o capas.

4. Normativa: Relaciona la normatividad del entorno regulatorio de Costa Rica que aplica a la CNE al dominio de arquitectura.

[3] ITIL consiste de un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

[4] La Organización Internacional de Normalización conocida por la abreviación ISO, es una organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de estandarización

El desarrollo o actualización de este dominio de la arquitectura, le permitirá a la CNE demostrar alineación de las estrategias y procesos institucionales (estratégicos, operativos y de apoyo) con las tecnologías de información y comunicación. También le permitirán diseñar e implementar esquemas de gobernabilidad de TIC e incorporar políticas de TIC en los procesos de gestión de TIC.

DOMINIO ESTRATEGIA DE TIC

La estrategia de TIC del domino arquitectura de negocio de la CNE se verá impactada ya que deberá considerar los elementos desarrollados en este plan, propiamente el apartado Marco Estratégico de la TIC:

- Misión y visión de la TIC 2019-2022.
- Matriz FODA de TIC.
- Objetivos estratégicos de TIC.

Adicionalmente, será necesario para una exitosa implementación de las iniciativas y objetivos estratégicos del plan, que la CNE defina y ponga en práctica una serie de políticas de gestión y gobernanza de las tecnologías de información. Entre ellas recomendamos:

- Política de gestión de servicios de tecnologías de información y comunicación.
- Política de gestión de seguridad de la información.
- Política de gestión de la continuidad de los servicios.
- Política de uso aceptable de los activos de tecnologías de información y comunicación.
- Política de gestión del riesgo de tecnologías de información y comunicación.

Asimismo, el dominio estrategia TIC considera los objetivos estratégicos institucionales vigentes en el Plan Estratégico Institucional 2018-2022:

1. PRIORIDAD: SISTEMA NACIONAL DE GESTIÓN DEL RIESGO

DECLARACIÓN DE RUMBO ESTRATEGICO: Fortaleceremos el SNGR para el cumplimiento de la Política y el Plan Nacional de Gestión del Riesgo

1.1. OBJETIVO ESTRATEGICO INSTITUCIONAL: Fortalecer los mecanismos coordinación del SNGR para el cumplimiento de la Política y el Plan Nacional de Gestión del Riesgo.

1.2. OBJETIVO ESTRATEGICO INSTITUCIONAL: Desarrollar las capacidades del SNGR para el fomento de una cultura proactiva entorno al riesgo de desastres.

1.3. OBJETIVO ESTRATEGICO INSTITUCIONAL: Verificar el cumplimiento del Plan Nacional de Gestión del Riesgo por ámbitos de gestión.

2. PRIORIDAD: RECTORÍA DE LA CNE

DECLARACIÓN DE RUMBO ESTRATEGICO: Perfeccionaremos nuestras políticas, procesos y procedimientos, para mejorar la gestión institucional de forma integral y enfoque inclusivo

2.1. OBJETIVO ESTRATEGICO INSTITUCIONAL: Mejorar la gestión institucional para el ejercicio de la rectoría en gestión del riesgo, apoyada por políticas, planificación y asignación de recursos presupuestarios, procesos y procedimientos internos claros que fomenten eficiencia, transparencia, coordinación, uso de tecnología, comunicación efectiva y la inclusividad.

2.1. OBJETIVO ESTRATEGICO INSTITUCIONAL: Orientar las relaciones internacionales y la cooperación en materia de gestión de riesgo.

3. PRIORIDAD: AMBIENTE ORGANIZACIONAL

DECLARACIÓN DE RUMBO ESTRATEGICO: Fortaleceremos el ambiente organizacional y el desarrollo del talento humano, para crear una atmósfera de trabajo saludable.

3.1. OBJETIVO ESTRATEGICO INSTITUCIONAL: Establecer un ambiente de trabajo que favorezca un clima organizacional armónico y saludable en la institución.

3.2. OBJETIVO ESTRATEGICO: Estimular el talento humano ante los retos de la institución en su ejercicio de rectoría y capacidad de conducción.

4. PRIORIDAD: RECURSOS ECONÓMICOS EN GESTIÓN DEL RIESGO

DECLARACIÓN DE RUMBO ESTRATEGICO: Encauzaremos esfuerzos tendientes a la obtención de los recursos económicos necesarios, para una gestión integral de riesgo.

4.2. OBJETIVO ESTRATEGICO: Gestionar ante los Organismos de Cooperación los recursos técnicos y financieros, que coadyuven en la consolidación del SNGR.

En el apartado gobernanza de las tecnologías de información y comunicación deberá considerarse que la Institución ya cuenta con una identificación inicial de procesos (ver anexo A Procesos de la CNE). De manera que el alcance del dominio de arquitectura de negocio se limita a estos procesos. Sin embargo, se hace la salvedad que también se ha identificado como necesidad en el Plan Estratégico Institucional 2018-2022, la actualización o reingeniería de dichos procesos: *Objetivo 2.1 "Mejorar la gestión institucional para el ejercicio de la rectoría en gestión del riesgo, apoyada por políticas, planificación y asignación de recursos presupuestarios, procesos y procedimientos internos claros que fomenten eficiencia, transparencia, coordinación, uso de tecnología, comunicación efectiva y la inclusividad*". Por tanto, una vez que se actualicen y se definan claramente los procesos y procedimientos, recomendamos que se actualice la capa de arquitectura negocios; de manera que el alcance de ésta aborde procesos actualizados y que serán soportados efectivamente mediante servicios de tecnologías de información y comunicación por medio de soluciones tecnológicas o sistemas de información.

El soporte a la gestión de los procesos se refiere a que, en lugar de tener herramientas para el registro de los resultados de las actividades realizadas previamente de manera manual, la CNE cuente con procesos automatizados que permitan la optimización de los recursos tecnológicos y humanos con el fin de trasmitir información de calidad, y que contemplen las características de oportunidad, disponibilidad y seguridad que la Institución requiere.

Considerando la documentación existente de los procesos (ver anexo A Procesos de la CNE), se propone la tabla 26 *"Aplicaciones actuales y futuras que soportarán la gestión de los procesos de CNE"*. Algunas de estas futuras aplicaciones formarán parte del Sistema Nacional de Gestión de Riesgo, el cual debería ser un Sistema Integrado de Información compuesto de varias aplicaciones y componentes lógicos de software que automatizan los procesos de la CNE priorizados en el alcance del presente PETI.

Tabla 26 Aplicaciones actuales y futuras que soportarán la gestión de los procesos de CNE.

Procesos CNE (ver anexo A)
Macroprocesos sustantivos • Prevención • Preparativos y Respuesta • Recuperación Macroprocesos de apoyo
Aplicaciones actuales
• El gestor documental basado en MS SharePoint • La herramienta de gestión de aprendizaje, Moodle.

- MS Office 365, Software de ofimática.
- Aplicativos de videoconferencia.
- Correo electrónico.
- Sistema Monitor (Seguimiento y monitoreo de PNGR).
- Acuersoft.
- SIGE.
- Sitio Web
- Sistema de gestión administrativa, Wizdom.

Aplicaciones futuras

- Herramienta tecnológica: para brindar y medir el alcance de la asesoría en materia de gestión del riesgo.
- Herramienta tecnológica: Plataforma para recursos de sensibilización al riesgo de desastre.
- Herramienta tecnológica: Sistema de Información Territorial de Riesgo a Desastre
- Herramienta tecnológica para manejar de información en situación de emergencia (CIA)
- Herramienta tecnológica para seguimiento del cumplimiento del PNGR
- Herramienta tecnológica para la gestión de procesos y procedimientos institucionales
- Herramienta tecnológica para la Gestión Administrativa Institucional.
- Herramienta tecnológica para la gestión de proyectos

IMPACTO DE LA ESTRATEGIA DE TIC SOBRE EL DOMINIO ARQUITECTURA DE DATOS-INFORMACIÓN

PRINCIPIOS DE ARQUITECTURA DE DATOS

Los siguientes principios de arquitectura de datos, del dominio de Información, son reglas de alto nivel que se consideran relevantes dentro del contexto de la Institución, que la guiarán en la toma de decisiones de alto nivel relacionadas con los datos e información manejadas por las distintas áreas de la Institución. Se recomienda que los siguientes principios de arquitectura de datos sean adoptados por la CNE durante la implementación de los productos establecidos en este plan estratégico de TIC.

Con la información recopilada y con el alcance del Plan Estratégico de TIC, se identificaron estos 5 principios:

Tabla 27 Principios de arquitectura de datos

Principio	01. Estructura de Datos Común
Declaración	La Arquitectura de Datos describe las estructuras de los datos mediante un modelo común para apoyar los flujos de información
Justificación	La definición de un modelo de entidades de negocio facilita el proceso de normalizar o diseñar las bases de datos de las soluciones.
Implicaciones	• Asegurar que la información de la Institución y los requerimientos de datos son entendidos claramente para su estructuración en un modelo común. • Documentar los flujos de información y puntos de contacto en la Institución para tener un entendimiento preciso de los roles y responsabilidades de los funcionarios respecto a la gestión de los datos. • Establecer un modelo formal que apoye la administración de los datos de la Institución.
Principio	**02. Registro y Fuentes únicas de datos**
Declaración	La Arquitectura de datos exige que todo sistema de información ingrese datos por un solo punto, garantizando que el repositorio de almacenamiento represente la fuente única de datos para el ámbito que le corresponde.
Justificación	Mecanismos de registro desde puntos únicos garantiza contar con la versión verdadera de los datos, para poder convertirla en información de valor.
Implicaciones	• Establecer el modelo de gestión de data maestra. • Alinear el gobierno de las aplicaciones con la gestión de la data maestra.
Principio	**03. Disponibilidad de la información**
Declaración	La información de la Institución que soporta los procesos misionales y de apoyo debe estar disponible en el momento adecuado y en los tiempos esperados, garantizando así el uso eficiente y eficaz en los procesos de la función misional de la Institución. En la norma ISO 27001 la Disponibilidad, asegura que los usuarios autorizados tengan acceso a la información y activos relacionados cuando sea requerido.
Justificación	La disponibilidad de la información conduce a la eficiencia y eficacia en la toma de decisiones y brinda respuesta oportuna a la prestación de servicios. Los datos son propiedad de las áreas usuarias y por lo tanto cuentan con los adecuados esquemas de gestión de la información que facilitan desarrollar la función principal de la Institución.

Implicaciones	• Los esquemas de acceso y publicación de la información deben ser lo suficientemente adaptables para satisfacer una amplia gama de canales para los usuarios. • Las áreas usuarias deben someterse a los mecanismos y herramientas que provean las áreas encargadas de desarrollar las funciones TIC, en cuanto al manejo de datos.
Principio	**04. Integridad de la información**
Declaración	La gestión de información debe contemplar la seguridad en su acceso y divulgación. En la norma ISO 27001 la Confidencialidad, asegura la accesibilidad de la información solamente a los que estén autorizados.
Justificación	La seguridad de la información permite el control de la divulgación de información sensible para el cumplimiento de la función principal de la Institución.
Implicaciones	• Establecer políticas de seguridad de la información. • Establecer los procedimientos de controles de acceso. • Definir roles y perfiles de acceso a la información.

MODELO DE CATEGORIZACIÓN DE LOS DATOS Y CAPACIDADES CLAVE

El modelo de categorización le permitirá a la Institución clasificar sus activos de información en grupos, para aplicar distintas políticas a cada grupo; este será un requisito fundamental además para implementar el sistema de gestión de seguridad de la información identificado claramente en este plan estratégico. Por ejemplo, políticas de ciclo de vida de los datos, de controles de seguridad, o de sitio de almacenamiento.

Las capacidades clave de datos que se recomiendan apuntan a que la Institución pueda atender los requerimientos de TIC relacionados con el dominio de información.

A continuación, una lista ejemplo estándar de la industria que sirva de insumo a la CNE para categorizar sus datos:

1. Metadatos: Consiste en las estructuras que describen las entidades de datos a través de atributos como su nombre, definición o dimensión.

2. Datos transaccionales: Son aquellos datos que resultan de las transacciones diarias de la Institución, los cuales son capturados durante la operación y procesos.

3. Datos maestros: Se refiere a las entidades de datos de alto nivel que son de valor estratégico para la Institución. Estas entidades no son de naturaleza volátil ni transaccional, dado que, una vez creadas, el conjunto de sus atributos típicamente sufre muy pocas modificaciones, o en muchas ocasiones ninguno.

4. Datos de referencia: Son estructuras conformadas por información de origen interno o externo a la Institución usada para soportar las decisiones y operaciones realizadas dentro de los procesos que ejecuta.

5. Datos no estructurados: Son aquellos activos de información que soportan las actividades de los funcionarios de la Institución, como lo pueden ser los Archivos en Excel, presentaciones en PowerPoint, documentos en formato Word e imágenes (activos de información).

6. Gestión de los Datos Maestros: se refiere a la capacidad de gestionar los datos a través de la definición de los activos de información fundamentales dentro de la Institución. Además, realiza la definición de las funciones que aseguran la integridad de los datos por medio de reglas y estructuras específicas.

7. Gestión del Contenido a nivel general: La gestión de contenidos no estructurados es necesaria para el manejo de los registros documentales, multimedia o la captura de imágenes. Además, se requieren mecanismos de búsqueda y flujo de trabajo adecuados para permitir una rápida recuperación de la información pertinente para la toma de decisiones dentro de la Institución.

8. Gestión del ciclo de vida de los datos: Se refiere a la capacidad desarrollada mediante procedimientos y herramientas que aseguran que en el ciclo de vida de los datos solo se retiene la información necesaria para la operación del negocio y el cumplimiento a regulaciones tanto internas como externas, determinando la vida útil de la información y su pertinencia legal.

9. Seguridad de los Datos: deben existir controles de seguridad sobre los datos, que permitan proteger la integridad, confidencialidad y disponibilidad de la información. Los datos deben estar protegidos en todos los estados de su ciclo de vida: activos, en almacenamiento histórico

y en disposición final. Se deben establecer los mecanismos para que la información sea segura y fiable a través de las diferentes fuentes y destinos de datos.

10. Calidad y Depuración de Datos: se refiere a la capacidad de gestionar, mediante políticas y procedimientos, la calidad, disponibilidad, integridad y depuración de los datos.

En esta etapa es crucial indicar que los datos (activos de información) se pueden clasificar en distintas categorías en función a su nivel de confidencialidad o privacidad.

A continuación, una lista ejemplo estándar de la industria que servirá de insumo para la CNE clasifique sus datos:

1. Información de carácter restringido o confidencial: Cuando la información presenta un nivel mayor de privacidad para la institución, esto quiere decir que el perímetro de acceso es muy limitado, los controles y procedimientos que intervienen en el manejo de la información representan un riesgo potencial para la Institución en cuanto a aspectos financieros, legales y de imagen, independientemente de los medios que se utilicen para almacenar, procesar y distribuir la información ya sea que esta se encuentre físico (papel impreso, sobres, folders, ampos, archiveros, etc.) o digital (llaves mayas, discos duros, servidores, laptops, almacenamiento en nube, sistemas, aplicaciones, bases de datos, etc.).

2. Información de uso interno: Es cuando la información presenta un nivel más bajo de confidencialidad, esto no quiere decir que es de dominio público, sino más bien que mientras la información cumple ciertas etapas de tramitación a través de los diferentes procesos solo será utilizada por el personal con fines operacionales dentro de la Institución. Una vez que la información cumpla su respectiva tramitación dentro del proceso, el resultado bien podría considerarse como información de acceso público, pero eso solo hasta que así se defina por el dueño del proceso o el dueño de la información.

3. Información pública: Es cuando la información es accesible a todo el público.

4. Esta información puede ser el resultado final de un proceso, que sea de interés público y que revele información como datos estadísticos sobre, por ejemplo, informes de gestión, datos relativos a transparencia institucional o información estadística de amenazas y eventos de riesgo.

A continuación, se referencian las principales Normativas y Estándares que se recomienda a la CNE tener en cuenta dentro del dominio de información, con el objetivo de establecer y dar sostenibilidad al Gobierno de la Información y la Arquitectura de datos misma, así como también cumplir con los objetivos y productos del PETI.

Normativa y Políticas:

- Ley N° 8488, Ley Nacional de Emergencias y Prevención del Riesgo.
- Política Nacional de Gestión del Riesgo.
- Ley n.º 8422, Ley contra la corrupción y el enriquecimiento ilícito en la función pública.
- Constitución Política de Costa Rica.
- Normas Técnicas de Gestión y Control de TIC.
- Directrices del Servicio Civil.
- Ley n.º 8968, Ley de Protección de la Persona Frente al tratamiento de sus datos personales.
- Decreto Ejecutivo n.º 40199-MP de la apertura de datos públicos.
- Ley n.º 7202, Ley de Sistema Nacional de Archivos.
- Normativa emitida por Comisión Nacional de Selección y Eliminación de Documentos (CNSED) de la Dirección General del Archivo Nacional.

Estándares:

Tabla 28 Estándares aplicables a la Arquitectura de Datos

Normativa	Descripción
ISO-IEC 27001: 2013	Requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información.
IEC 27002: 2013	Controles de los dominios del sistema de gestión de la seguridad de la información.
ISO/IEC 25012:2008.	Modelo de calidad de datos.
ISO/IEC 11179	Uso y descripción información semántica, centrado en la integración, uso compartido, de intercambio, y de migración de datos entre sistemas de información.

El desarrollo o actualización (producto del PETI) de este dominio de Arquitectura Empresarial le permitirá a la CNE mejorar su gestión de los sistemas de información, incluyendo su arquitectura, ciclo de vida, las aplicaciones que los conforman y los procesos de implementación y soporte.

PRINCIPIOS DE ARQUITECTURA DE APLICACIONES

Los principios de arquitectura de aplicaciones, del dominio de Sistemas de Información, son reglas de alto nivel que se consideran relevantes dentro del contexto de la Institución, que la guiarán en la toma de decisiones relacionadas con la arquitectura de las aplicaciones informáticas empleadas por las distintas áreas de la Institución. Se recomienda a la CNE que aplique estos principios en sus proyectos de implementación de nuevas aplicaciones o de mejora de las actuales.

Tabla 29 Principios de Arquitectura de Aplicaciones

Principio	**01. Flexibilidad de aplicaciones**
Declaración	La arquitectura de aplicaciones debe ser modular, escalable y de fácil acoplamiento.
Justificación	Las aplicaciones con estas características permiten: • Optimizar la agilidad y minimizar la complejidad de integración. • Simplificar la implementación y mantenimiento. • Gestionar los cambios en las soluciones con un impacto bajo en los procesos y facilita una arquitectura orientada a servicios.
Implicaciones	• Establecer un método de integración común. • Implementar arquitecturas basadas en servicios. • Establecer estrategias de integración de aplicaciones.
Principio	**02. Racionalización de Aplicaciones**
Declaración	La arquitectura de aplicaciones debe promover la racionalización en el portafolio de soluciones de la Institución, maximizando su aprovechamiento y evitando la implementación de funcionalidades ya existentes.
Justificación	La correcta identificación del portafolio de aplicaciones de la CNE evita que se propongan e implementen soluciones que cubran funcionalidades ya existentes en aplicaciones actuales.
Implicaciones	• Gestionar el portafolio de aplicaciones de la CNE

	• Gestionar los requerimientos comparándolos con las funcionalidades existentes en las aplicaciones actuales. • Establecer trazabilidad en la identificación de necesidades de modernización y relevamiento de aplicaciones
Principio	**03. Reutilización de Funcionalidades**
Declaración	La arquitectura de aplicaciones debe establecer soluciones conformadas por componentes y servicios que habiliten la reutilización de funcionalidades.
Justificación	El proceso de reusar aplicaciones reduce costos y promueve la integración por componentes asegurando consistencia en el desarrollo de soluciones.
Implicaciones	• Reusar componentes actuales de aplicación mientras sea posible. • Establecer el catálogo de servicios (funcionalidades expuestas por otros aplicativos).
Principio	**04. Aplicaciones orientadas al usuario o actores de SNGR**
Declaración	La arquitectura de aplicaciones debe procurar la implementación de soluciones de negocio orientadas al ciudadano y la prestación de servicios.
Justificación	La liberación de soluciones de negocio debe evitar la generación rechazo o resistencia al cambio por su dificultad de uso o complejidad.
Implicaciones	• Fácil usabilidad de aplicaciones • Soportar eficiencia de los procesos • Trámites o procesos interinstitucionales (o actores de SNGR)

POLÍTICAS Y/O ESTÁNDARES A IMPLEMENTAR

A continuación, se referencian las principales Políticas y Estándares que se recomienda a la CNE tener en cuenta dentro del dominio de Sistemas de Información.

Normativa y Políticas:

- Normas Técnicas de Gestión y control de TIC
- Normas internacionales de contabilidad, sistemas financieros. NIC
- Ley n.º 8968, Ley de Protección de la Persona Frente al tratamiento de sus datos personales.
- Decreto Ejecutivo n.º 40199-MP de la apertura de datos públicos.
- Ley n.º 7202, Ley de Sistema Nacional de Archivos.

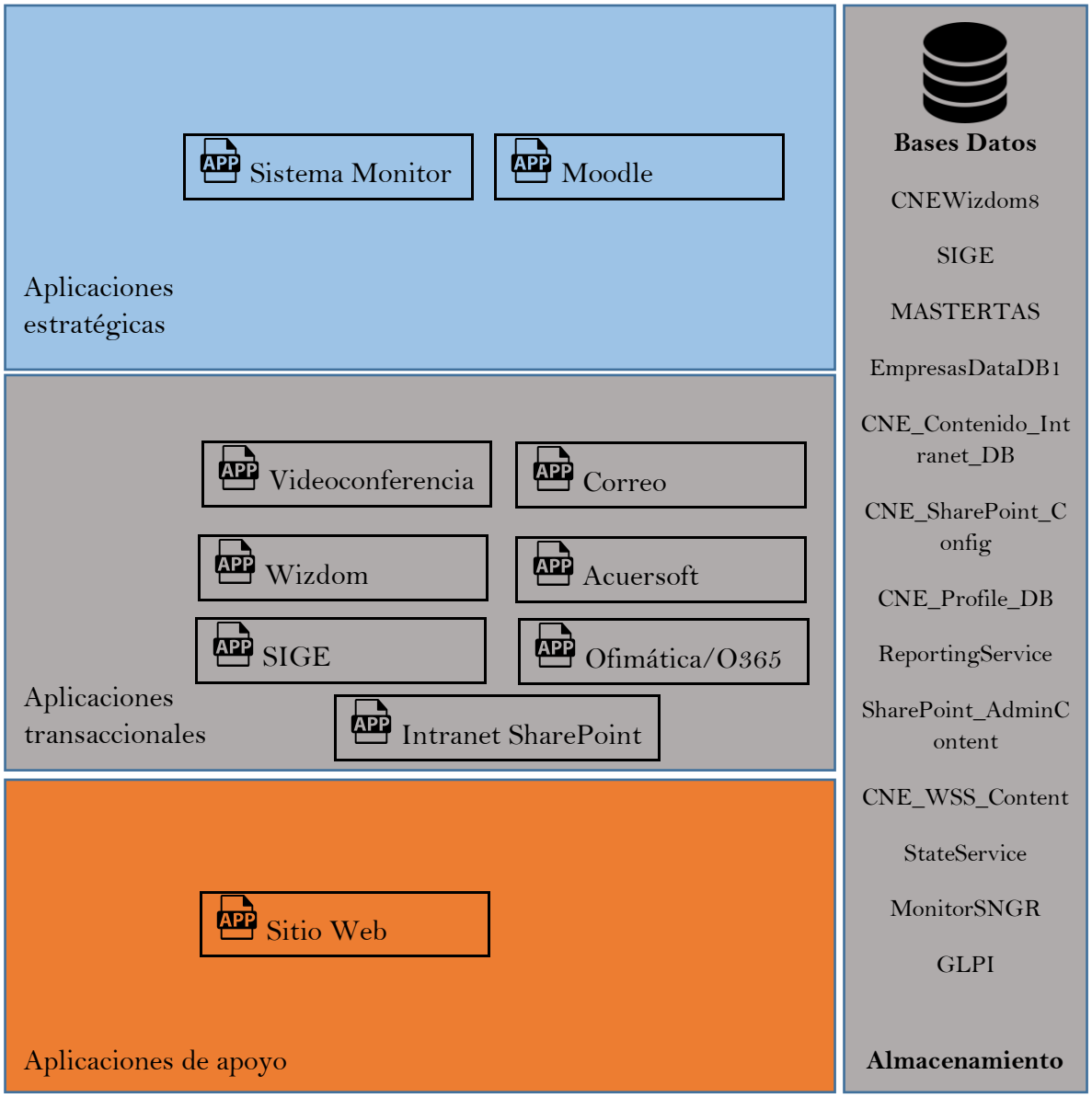
Estándares:

Tabla 30 Estándares aplicables a la Arquitectura de Aplicaciones

Normativa	Descripción
ISO-IEC 27001: 2013	Requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información.
IEC 27002: 2013	Controles de los dominios del sistema de gestión de la seguridad de la información.
ISO/IEC 9126	Calidad del Producto de Software.
NTC 5854	Accesibilidad a las Páginas WEB
CMMI (Capability Maturity Model Integration)	El modelo CMMI surge como una continuación del modelo CMM (Capability Maturity Model) y constituye un marco de referencia de la capacidad de las organizaciones de desarrollo de software en el desempeño de sus diferentes procesos, proporcionando una base para la evaluación de la madurez de éstas y una guía para implementar una estrategia para la mejora continua.
SCRUM	Estándar para necesidades de desarrollos que requieran respuestas ágiles. Scrum es un proceso en el que se aplican de manera regular un conjunto de buenas prácticas para trabajar colaborativamente, en equipo, y obtener el mejor resultado posible de un proyecto. Estas prácticas se apoyan unas a otras y su selección tiene origen en un estudio de la manera de trabajar de equipos altamente productivos. En Scrum se realizan entregas parciales y regulares del producto final, priorizadas por el beneficio que aportan al receptor del proyecto. Por ello, Scrum está especialmente indicado para proyectos en entornos complejos, donde se necesita obtener resultados pronto, donde los requisitos son cambiantes o poco definidos, donde la innovación, la competitividad, la flexibilidad y la productividad son fundamentales.

VISTA DE ARQUITECTURA DE APLICACIONES ACTUAL

A continuación, se presenta un diagrama o vista del estado actual de las aplicaciones informáticas en la Institución.



MODELO DE ARQUITECTURA DE APLICACIONES OBJETIVO

La arquitectura de aplicaciones objetivo se refiere al modelo de sistemas informáticos y su interrelación, que se recomienda aplicar en la Institución para cumplir con los objetivos estratégicos del Plan Estratégico de TIC 2019-2022. Esto implica que para el desarrollo de este

dominio de Sistemas de Información se deba invertir en proyectos de implementación de nuevas aplicaciones, o de mejora de las actuales. Para esto se deben categorizar las aplicaciones según su nivel de contribución a la Institución.

CATEGORIZACIÓN DE LA ARQUITECTURA DE APLICACIONES OBJETIVO

A continuación, se proporcionan ejemplos de categorías de aplicaciones aplicables a CNE.

Aplicaciones estratégicas: Son aquellas aplicaciones que le permiten a la Institución ofrecer servicios diferenciados a los usuarios o actores del SNGR, facilitan y promueven la estrategia a nivel institucional.

Aplicaciones transaccionales: Son aquellas aplicaciones utilizadas constantemente por usuarios (internos, externos) y que son de crucial importancia para la operación de la CNE en su conjunto.

Aplicaciones de apoyo: Son aquellos aplicativos desarrollados a la medida para Institución o aplicaciones propietarias, que consumen datos originados de las aplicaciones transaccionales, con el fin de generar nueva información para las operaciones del día a día y para la toma de decisión.

JUSTIFICACIÓN PARA LA ARQUITECTURA DE APLICACIONES OBJETIVO

Las organizaciones dependen de sus activos de información para la toma de decisiones efectivas para la adecuada ejecución de sus objetivos estratégicos. Por esta razón, se requiere de una Arquitectura de Aplicaciones en la CNE que proponga la reutilización del uso de las funcionalidades existentes y genere nuevas de conformidad con el plan estratégico de TIC. Con el diseño de una arquitectura que sugiera acoplamiento entre sus componentes y que promuevan la reutilización de éstos, favoreciendo la identificación de un conjunto de servicios de TI y proporcionando información de alta disponibilidad, confiable, oportuna.

La arquitectura de aplicaciones debe dar soporte a los siguientes aspectos:

- Alinear las aplicaciones existentes en la CNE con la infraestructura tecnológica existente y propuesta en el Plan Estratégico de TIC y procesos de TIC a las necesidades actuales requeridas por el SNGR.
- Integrar servicios de TIC para potencializar los canales de comunicación como medios de apoyo entre la CNE, colaboradores o actores del SNGR, ciudadanos y entes externos. Debe ser servicios de aplicación e información que soporten en tiempo real las operaciones brindadas de una manera ágil, segura, confiable y altamente disponible.
- Enfocarse en la generación de valor y calidad de los servicios de tecnología y comunicación que respondan a las necesidades de las funciones críticas de la CNE (tecnologías al servicio de la Institución, valor en forma de tecnologías y servicios de TIC).

- Identificar las funciones o procedimientos que actualmente operan en la Institución y que pueden ser candidatas para ser automatizadas mediante sistemas de información o servicios web.
- Permitir la comunicación de las distintas aplicaciones que actualmente se encuentran operando sobre diferentes plataformas tecnológicas.
- Una arquitectura de integración orientada a servicios permite estandarizar los reportes y definir herramientas para su generación y consulta, que respondan adecuadamente a las necesidades de los usuarios (internos y externos, actores del SNGR) de la CNE.
- Una arquitectura de integración orientada a servicios para apoyar la gestión de procesos institucionales, la implementación de estrategias y esquemas para la sincronización y centralización de la información en la CNE a partir de fuentes externas.

REQUERIMIENTOS NO FUNCIONALES QUE SOPORTARÁN LA ESTRATEGIA DE TIC

Los requerimientos no funcionales proporcionan una descripción de las características del software y hardware que debe tener el sistema de información para satisfacer las necesidades de la Institución. Estas necesidades serán una base para el análisis, diseño y pruebas del sistema al momento de la implementación (según cronograma u hoja de ruta de implementación del PETI) o ajustes a las aplicaciones transaccionales y de apoyo, enmarcados en el plan estratégico de TIC.

Tabla 31 Requerimientos no funcionales que deben considerarse para las nuevas aplicaciones

Requerimiento	Descripción requerimiento No Funcional
Escalabilidad	Categorías de requerimientos relacionados con la cantidad de usuarios (concurrentes) y dimensión de los repositorios de datos actuales, tiempo de respuesta requerido para el acceder a los diferentes contenidos (Método de acceso a los diferentes tipos de contenidos) e integración con bajo acoplamiento con módulos, componentes, aplicaciones y otros tipos de arquitectura.
Extensibilidad (Modificabilidad)	Categorías de requerimientos relacionados con flexibilidad del software a cambios de requerimientos (ajustes o nuevos requerimientos) necesarios para la integración con proveedores externos.
Plataformas	Categorías de requerimientos relacionados con el análisis de todo el entorno de hardware (tipos de servidores bases de datos, redes) actual y software (sistemas operativos, herramientas informáticas y su licenciamiento).
Protección de Datos de Carácter Personal	Categorías de requerimientos relacionados con la protección de datos personales.

Requerimiento	Descripción requerimiento No Funcional
Capacidades administrativas	Categorías de requerimientos relacionados con la gestión de flujos de información, monitorización de procesos, evaluación y optimización del rendimiento.
Estándares	Categorías de requerimientos relacionados con los marcos de referencia utilizada para identificación requerimientos de negocio.
Alta disponibilidad	Categorías de requerimientos relacionados con la alta disponibilidad, la tolerancia a fallos y su respectiva recuperación de forma autónoma.
Balance o balanceo de carga	Categorías de requerimientos relacionados con la capacidad que deben soportar los servidores Web a nivel transaccional.
Procedimiento de despliegue y gestión de versiones	Actualización de versiones y configuración de componentes.
Mecanismo de autenticación de los tipos documentales	Categorías de requerimientos relacionados con la autenticación del usuario (firmas digitales y certificados digitales).
Movilidad	Categorías de requerimientos relacionados con interoperabilidad con terminales móviles y funcionamiento "off line".
Colaboración	Capacidades en función de integraciones con diferentes herramientas propietario (alcance y limitaciones de integración).
Rendimiento	Categorías de requerimientos relacionados con los tiempos de respuesta acordados.
Fiabilidad	Tipos de requerimiento relacionado con la capacidad del usuario final para confiar en la información suministrada por el sistema.
Disponibilidad	Categorías de requerimientos relacionados con la disponibilidad del sistema frente a los usuarios finales.
Seguridad	Categorías de requerimientos relacionados con privacidad de los flujos de datos y su respectivo almacenamiento en sitio seguros, políticas de intrusiones.
Portabilidad	Categorías de requerimientos relacionados con la migración a otra plataforma tecnológicas sin afectar la operación de las operaciones del día a día de la CNE.
Mantenibilidad	Categorías de requerimientos relacionados para ejecución de controles de revisión y control de cambios sobre la funcionalidad del sistema sin incurrir en costos exagerados o fuera del presupuesto de la Institución.

Requerimiento	Descripción requerimiento No Funcional
Reusabilidad	Categorías de requerimientos relacionados con los componentes o funcionalidades del sistema que suministran servicios a otros sistemas.
Usabilidad	Categorías de requerimientos relacionados con la medida de la calidad de la experiencia del usuario en la interacción con el servicio expuesto por el aplicativo y/o el fácil uso de la aplicación (diseño gráfico enfocado con facilidad por parte del usuario final).
Interfaces	Categorías de requerimientos relacionados con la interoperabilidad con otros sistemas de información.
Capacidad de Prueba	Categorías de requerimientos relacionados con el grado en que un servicio facilita el establecimiento de criterios de prueba y su realización, para determinar si se han cumplido los criterios.
Capacidad de recursos de infraestructura tecnológica	Categorías de requerimientos relacionados con la infraestructura tecnológica requerida que permitirán al sistema funcionar correctamente y que cumpla las expectativas en temas de rendimiento, eficiencia eficacia.
Confiabilidad	Categorías de requerimientos relacionados con posibilidad del sistema de realizar las funciones para las que fue diseñado sin presentar fallos.
Visibilidad	Tipo de requerimiento que especifica el grado en que un servicio es visible.

DEFINICIÓN DE LA ARQUITECTURA DE APLICACIONES OBJETIVO

Luego de analizar la arquitectura de aplicaciones actual (Apartado Situación Actual de este documento) se establece una definición de la Arquitectura de Aplicaciones Objetivo para la CNE según los requerimientos del PETI 2019-2022 considerando además las buenas prácticas de la industria como lo es Arquitectura de Aplicaciones del Método de Desarrollo de la Arquitectura (ADM, Architecture Development Method) contenido en el marco de referencia TOGAF (The Open Group Architecture Framework).

Este análisis se apoya en los criterios de decisión diseñados dentro del desarrollo de la Arquitectura de Aplicaciones basándose en el marco de referencia TOGAF, que permiten definir la evolución de la arquitectura de aplicaciones objetivo. Los criterios de decisión que

recomendamos a la CNE utilizar para la Arquitectura de Aplicaciones Objetivo, se describen a continuación:

Figura 4 Criterios de decisión para desarrollo de la Arquitectura de Aplicaciones

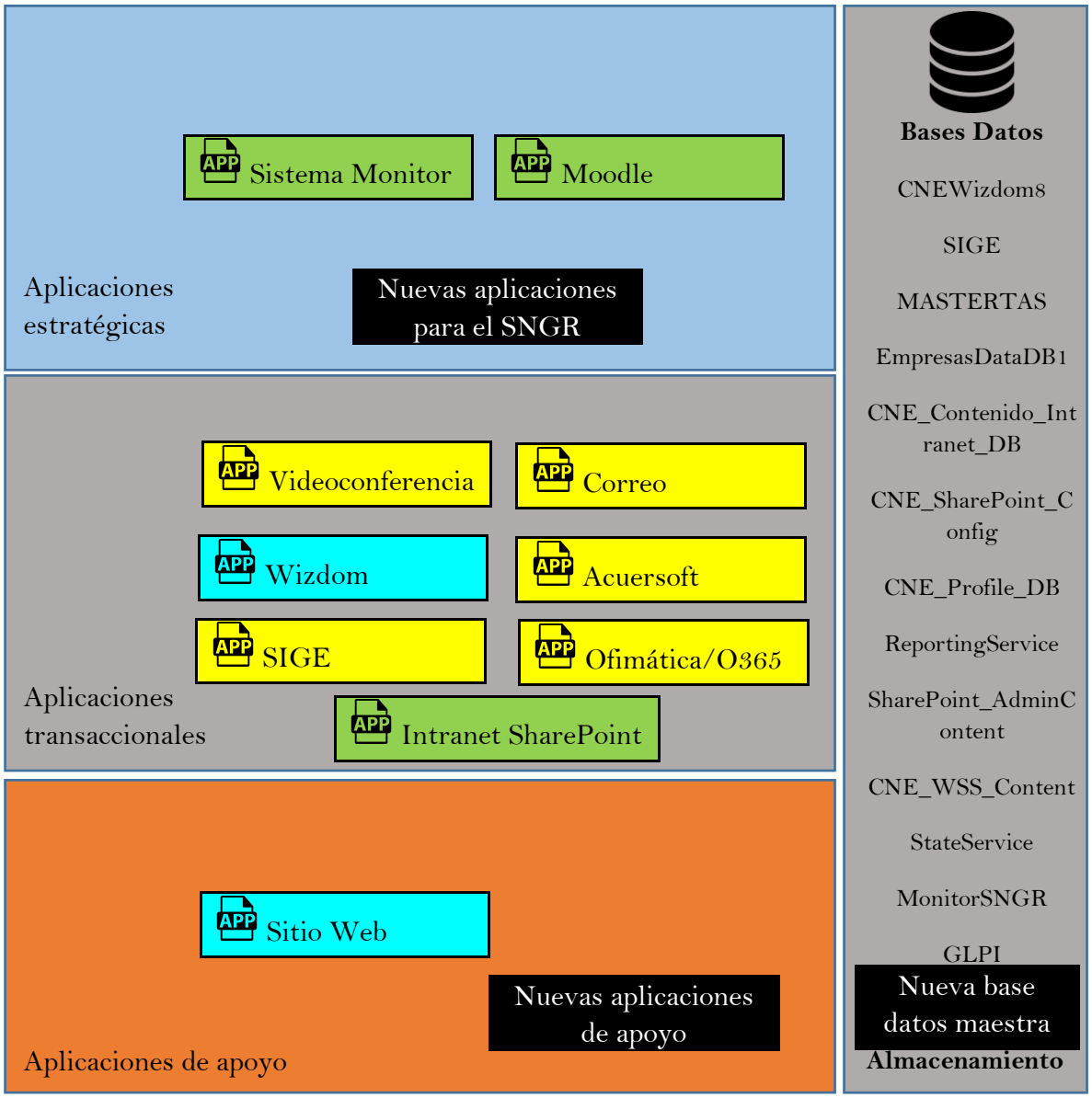
Las razones por las cuales aplicar cada uno de estos criterios no deben cumplirse en su totalidad, solo permiten generar una orientación en las decisiones.

Figura 5 Criterios de decisión para la Arquitectura de Aplicaciones Objetivo, según TOGAF

Nombre	Descripción	Justificaciones que orientan la clasificación del criterio
Incorporar	Agregar una nueva aplicación a la arquitectura de aplicaciones	•Si tiene alto nivel de cubrimiento funcional
Relevar	Retirar una aplicación de la arquitectura de aplicaciones	•No tiene alto nivel de cubrimiento funcional •No tiene alto nivel de utilización, ni alta expectativa de utilización •No tiene alto nivel de flexibilidad •No tiene inversiones recientes
Mantener	No hacer ningún cambio, ni modificación ni a la funcionalidad de la aplicación, ni a su plataforma	•Si tiene alto nivel de cubrimiento funcional •Si tiene alto nivel de utilización, o alta expectativa de utilización •Si tiene soporte por parte del fabricante e interno •Si tiene alto nivel de flexibilidad •Si tiene alto nivel de estabilidad •Si tiene inversiones recientes
Fortalecer	Mejorar una aplicación ya existente, dejarla en su plataforma actual y agregarle nuevas funcionalidades o establecer estrategias para promocionar su utilización (Ej. Mejorar la calidad de su información)	•No tiene alto nivel de cubrimiento funcional •Si tiene alto nivel de utilización, o alta expectativa de utilización •Si tiene soporte por parte del fabricante e interno •Si tiene alto nivel de flexibilidad •Si tiene inversiones recientes
Modernizar	Convertir o re-programar una aplicación "legada" o "anticuada" a una aplicación moderna, ó implantar una aplicación de algún fabricante (Ej. Implantar un ERP)	•Si tiene alto nivel de cubrimiento funcional actual •Si tiene alto nivel de utilización, o alta expectativa de utilización •No tiene soporte por parte del fabricante ni interno •No tiene alto nivel de flexibilidad •No tiene inversiones recientes

De acuerdo a los criterios mencionados la arquitectura de aplicaciones objetivo contendrá los elementos que se ilustran a continuación:

Figura 6 Aplicaciones objetivo



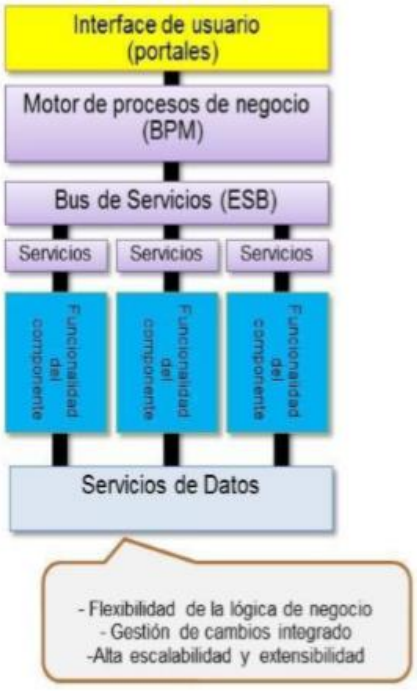
Este modelo de Arquitectura de Aplicaciones es una recomendación que no desarrolla por completo los elementos necesarios para una implementación de los sistemas requeridos por CNE

en el contexto del SNGR; será un punto de referencia o partida que le permitirá a CEN diseñar soluciones tecnológicas. También es un diseño flexible y contiene elementos base para iniciativas futuras, tanto para emprender nuevos desarrollos a la medida, como para evaluar la arquitectura de un sistema ya construido que desee incorporar.

Esta definición de la arquitectura de aplicaciones habilitará la implementación de soluciones de negocio dinámicas que responden a las actuales necesidades de escalabilidad y extensibilidad.

En el siguiente gráfico del modelo se ilustra la arquitectura de aplicaciones propuesta para las aplicaciones requeridas en el PETI para el SNGR. Las aplicaciones dinámicas tienen como fundamento una interfaz web de usuario única con elementos compartidos para los diferentes canales de acceso de la CNE (Portal internet o web, Intranet, Dispositivos Móviles, Redes sociales, medios de comunicación masivos), la automatización de procesos institucionales, un bus de servicios para centralizar las interfaces hacia los datos y hacia las demás aplicaciones tanto internas como externas a la CNE. Este enfoque supone acceso a servicios de datos, e interacción vía interfaces web, y una fuente única de datos compartida entre los distintos procesos de negocio, para evitar "islas" de información entre las áreas de la CNE.

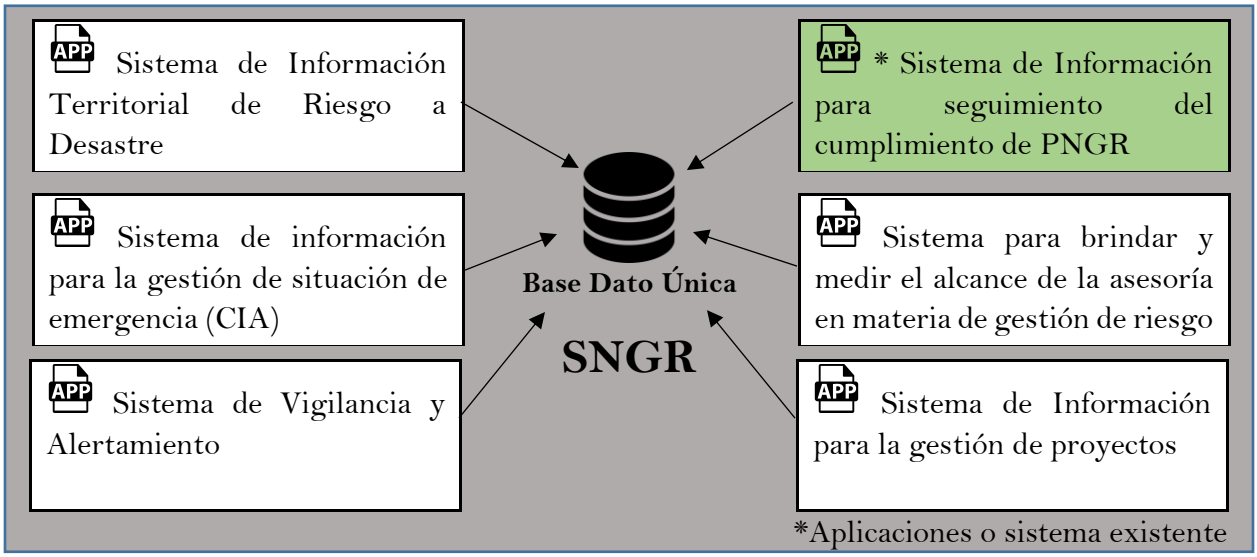
Figura 7 Aplicaciones dinámicas



Fuente: TOGAF

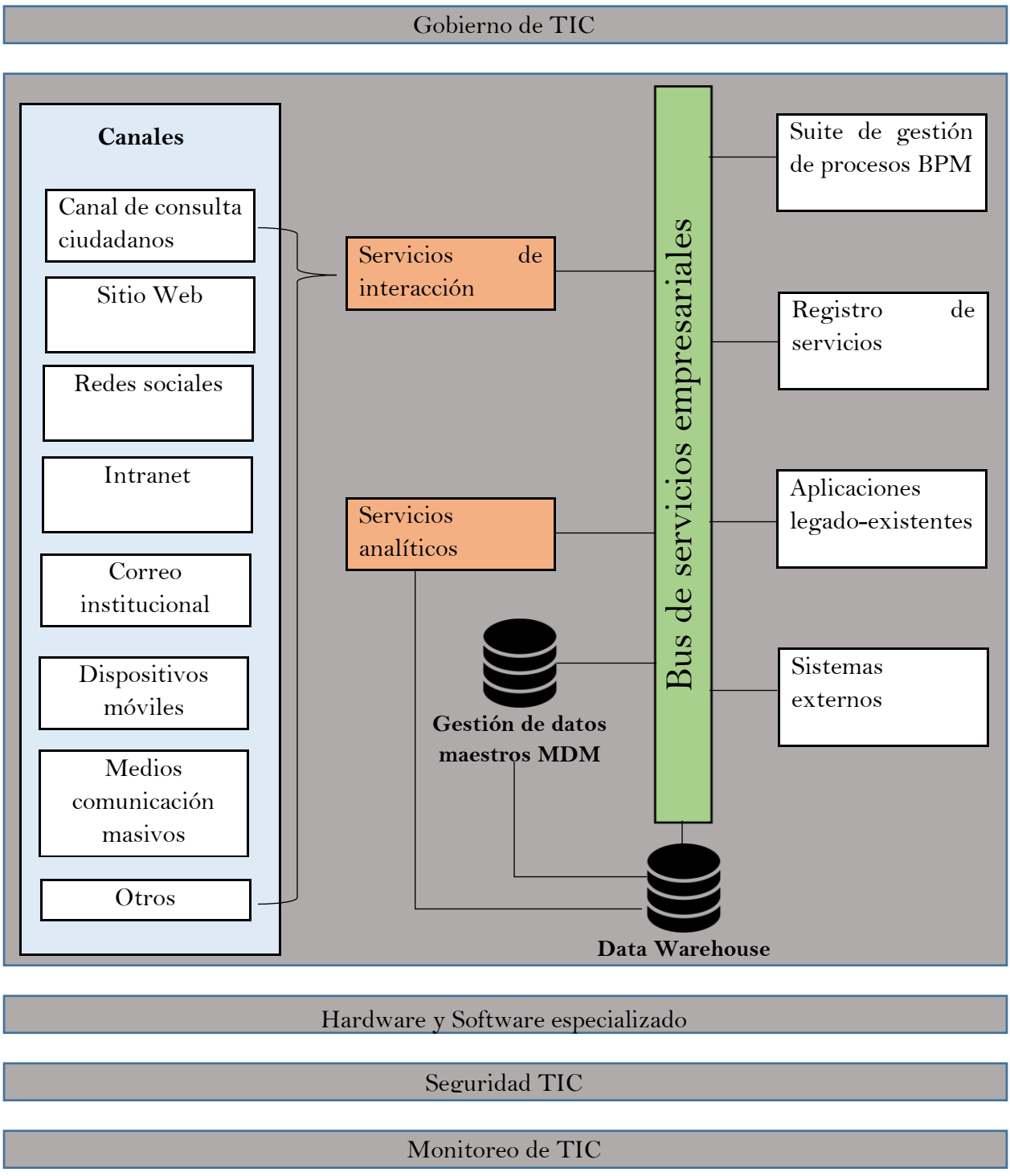
Las aplicaciones que permitan desarrollar las capacidades del SNGR para el fomento de una cultura proactiva entorno al riesgo de desastres, deberían alinearse con el modelo de la siguiente ilustración.

Figura 8 Aplicaciones del SNGR



Finalmente, recomendamos a CNE desarrollar este modelo de forma que aplique cada uno los componentes lógicos de aplicación (capa de aplicativo) que describen en la siguiente ilustración

Figura 9 Componentes del Modelo Arquitectura de Aplicaciones



A continuación, una descripción de cada componente lógico de la arquitectura recomendada.

Componente	Descripción
Aplicaciones Legadas o existentes	Aplicaciones que utiliza actualmente la CNE (a abril de 2019) y que durante la vigencia del plan PETI 2019 a 2022 no serán reemplazadas por nuevas aplicaciones dentro del SNGR. Estas aplicaciones legadas se integrarán con los demás componentes de la arquitectura por medio del Bus de Servicios.
Bus de Servicios Empresarial – ESB	ESB es el acrónimo en inglés de Enterprise Service Bus. El ESB es la columna vertebral de la arquitectura que facilita la comunicación entre los servicios expuestos por los distintos sistemas, aplicaciones y componentes de la arquitectura. Conecta a los consumidores de servicios a los proveedores de servicios, lo que simplifica el acceso a los servicios. El ESB tiene las siguientes capacidades: • Integración, enrutamiento, transformación, conversión, distribución. • Implementa el catálogo de servicios de negocios. • Consolida funciones del ciclo de vida de los servicios. • Establece una plataforma común para publicación y consumo de servicios. Cada componente tiene que consumir servicios para trabajar con otro componente.
Canal de consulta de ciudadano	Central telefónica de la CNE, módulo de consultas en sitio Web para gestionar dudas y atender a la ciudadanía
Correo Institucional	Correo electrónico en la nube de Internet (Microsoft Office 365) para los funcionarios de la CNE.
Data Warehouse	Es uno de los componentes del modelo de inteligencia de negocios (conocido como BI). Es un repositorio o colección de recursos que se puede acceder para recuperar la información de los datos almacenados en la CNE, diseñado para facilitar la presentación de informes y análisis. La fuente principal de los datos se limpia, se transforma y se cataloga y se pone a disposición para su uso por directivos y otros profesionales de la CNE o actores de la SNGR para la minería de datos, procesamiento analítico en línea, correlación de datos y apoyo a las decisiones.
Desarrollo Ágil	Componente trasversal que indica la definición e implementación del método y herramientas que cubren el ciclo de vida completo de las aplicaciones y los componentes de la arquitectura, para necesidades de desarrollos que requieran respuestas ágiles. Establece un enfoque común para cada actividad de desarrollo, mantenimiento y soporte.

Componente	Descripción
	Ver SCRUM en el apartado Estándares de la Arquitectura de Aplicaciones.
Dispositivos Móviles	Aplicaciones de la CNE para dispositivos móviles como celulares y tabletas. La CNE deberá definir la funcionalidad ofrecida en dichas aplicaciones teniendo en cuenta apoyar los objetivos estratégicos de la Institución.
Gestión de Datos Maestros – MDM	MDM es el acrónimo en inglés de Master Data Management. Define y gestiona las entidades de datos no transaccionales, como por ejemplo los Sujetos de Control. MDM tiene el objetivo de proporcionar procesos de recolección, agregación, relación, consolidación, aseguramiento de calidad, persistencia y distribución de dichos datos en toda la Institución, para asegurar la consistencia y el control en el mantenimiento y uso continuo de esta información. MDM ayuda a que la CNE no utilice múltiples versiones (potencialmente contradictorias) de los mismos datos maestros en diferentes partes de sus operaciones.
Gobierno de TIC	Son los lineamientos, principios, procesos y herramientas definidos en los distintos dominios de Arquitectura de la CNE, aplicados a los componentes de la arquitectura tecnológica.
Hardware y Software Especializado	Incluye la plataforma de hardware del centro de almacenamiento y procesamiento de datos de la CNE, la plataforma de comunicaciones y el software especializado (sistema operacional, software de comunicaciones, gestores de bases de datos, antivirus, entre otros).
Intranet	Portal para acceso exclusivo por parte de los funcionarios de la CNE.
Monitoreo de TIC	Monitoreo de Infraestructura y procesos de negocio.
Portal Web Internet	Portal oficial de la CNE en Internet. www.cne.go.cr
Redes Sociales Internet	Redes sociales en Internet en las cuales hace presencia la CNE (Twitter, Facebook, YouTube, Instagram, otros.)
Registro de Servicios	Es el punto central donde se encuentra el catálogo de servicios TIC que están desplegados, al cual pueden acudir otras aplicaciones para encontrar metadatos de dichos servicios.
Seguridad de TIC	Componente trasversal que indica la implementación de las políticas del Sistema de Gestión de Seguridad de la Información que la CNE requiere en todos los componentes de la arquitectura.
Servicios Analíticos	Es uno de los componentes del modelo de inteligencia de negocios (BI). Los datos de comportamiento de los sujetos de control de la CNE

Componente	Descripción
	que están almacenados en el componente de Data Warehouse se utilizan para ayudar a tomar decisiones clave de negocio a través de la segmentación y el análisis predictivo. Esta información sería utilizada por la CNE para mejorar los resultados de su misión. Proporciona vistas históricas, actuales y predictivas de las operaciones de la Institución. Transforma datos en información significativa y útil que se usa para activar conocimientos estratégicos, tácticos y operativos más eficaces y en la toma de decisiones.
Servicios de Interacción	Permiten la colaboración entre personas, procesos e información, por medio de la reutilización de componentes comunes de software entre las distintas aplicaciones de los canales web. Entre dichos componentes comunes están: gestión de acceso de los usuarios, gestión del perfil de los usuarios, servicios de presentación web, y gestión de contenido web
Sistemas Externos	Sistemas de información externos a la CNE, que son empleados en los procesos de clave. Por ejemplo, datos previstos por entidades técnicas.
Suite de Gestión de Procesos de Negocio – BPM Suite	BPM es el acrónimo en inglés de Business Process Management (Gestión de Procesos de Negocio). BPM Suite es un conjunto de herramientas de software que aprovecha los conceptos de gestión de procesos de negocio (BPM) para implementar procesos de negocio a través de la orquestación de actividades entre las personas y los sistemas. Un BPM Suite contiene 4 componentes críticos: • Motor de procesos: plataforma para modelar y ejecutar aplicaciones basadas en procesos, incluyendo reglas de negocio. • Analítica de negocio: permite a los directores identificar inconvenientes en los procesos, tendencias y oportunidades con reportes y tableros de control. • Gestión de contenido: provee un sistema para almacenar y asegurar documentos electrónicos, imágenes y otros archivos. • Herramientas de colaboración: provee foros de discusión, espacios de trabajo dinámicos y tableros de mensajes. Por lo anterior, una BPM Suite tiene un alcance mayor que el de un Sistema de Gestión Documental.

FACTORES CRÍTICOS DE ÉXITO

Para asegurar el éxito de consecución de los objetivos estratégicos de TIC y las iniciativas establecidos en este plan estratégico, consideramos los siguientes elementos esenciales como factores a considerar:

Se requiere de apoyo o compromiso de la administración superior de la CNE asegurando la disposición de recursos.

Las distintas áreas involucradas o a las que se les ha asignado responsabilidad deben asumirla de tal forma los requerimientos técnicos para el diseño de las soluciones y herramientas tecnológicas. Estas áreas deberán asegurar la adopción y apropiación de las soluciones o sistemas de información producto de la implementación de las iniciativas estratégicas.

La implementación de las iniciativas estratégicas del presente plan debe abordarse como proyectos (o en su efecto un conjunto de proyectos, denominado programa) que involucren distintas etapas:

- **Iniciación.** Define y autoriza el proyecto o una fase de éste. Está formado por dos procesos.
- **Planificación.** Define, refina los objetivos y planifica el curso de acción requerido para lograr los objetivos y el alcance pretendido del proyecto.
- **Ejecución.** Compuesto por aquellos procesos realizados para completar el trabajo definido en el plan a fin de cumplir con las especificaciones de éste. Implica coordinar personas y recursos, así como integrar y realizar actividades del proyecto en conformidad con el plan para la dirección del proyecto.
- **Seguimiento y Control.** Mide, supervisa y regula el progreso y desempeño del proyecto, para identificar áreas en las que el plan requiera cambios.
- **Cierre.** Formaliza la aceptación del producto, servicio o resultado, y termina ordenadamente el proyecto o una fase de éste.

Seguimiento del CGTI. Este será uno de los factores cruciales para asegurar el éxito del PETI 2019-2022, una de las responsabilidades de este comité es la revisión planificada a intervalos no mayores a tres meses del avancen en la implementación de las iniciativas y objetivos estratégicos de TIC. Para ello solicitarán informes de avance a la Jefatura de la Unidad TIC quien utilizará la herramienta ***Cuadro de Mando Integral*** que se adjunta a este plan. Se requiere de un seguimiento y cumplimiento de la **Hoja de Ruta** de implementación del plan estratégico de TIC.

El Gobierno de TI representado en última instancia por la administración superior debe demostrar su apoyo y compromiso con la aprobación de políticas, como las descritas en el apartado **Dominio de Estrategias TIC, Impacto sobre la Arquitectura de Negocio**:

- Política de gestión de servicios de tecnologías de información y comunicación.
- Política de gestión de seguridad de la información.
- Política de gestión de la continuidad de los servicios.
- Política de uso aceptable de los activos de tecnologías de información y comunicación.
- Política de gestión del riesgo de tecnologías de información y comunicación.

Es imperativo para el éxito del plan la adopción del enfoque de **Arquitectura Empresarial** del apartado **Arquitectura** de este documento. La principal responsabilidad por la **arquitectura de negocio** la tiene la administración superior ya que como ente de gobierno de TIC debe propiciar la definición de procesos y procedimientos institucionales. Le corresponderá a la Unidad de TI la formulación y definición de la arquitectura de información, arquitectura de aplicaciones contempladas en el alcance de este plan (aplicaciones futuras, vista al 2022).

Para las herramientas tecnológicas del SNGR se debe abordar un enfoque metodológico tal que se haga un diseño integral de las soluciones alineados con la arquitectura empresarial y considere distintos habilitadores:

- **Principios, Políticas y Marcos:** las políticas generales y específicas, la normativa existente, así como las distintas responsabilidades que genera el marco de trabajo del SNGR.
- **Estructuras Organizacionales:** Se debe considerar la estructura organizativa existente incluyendo comités, roles y responsabilidades asignadas a cada miembro o actor en el SNGR.
- **Cultura, Ética y Comportamiento:** La cultura, ética y comportamiento de los individuos, muchas veces es un factor de éxito subestimado en las actividades de gobierno y gestión de un sistema. La concientización o entrenamiento del recurso humano es un factor definitivo que considerar durante la implementación.
- **Información:** Será importante reconocer la información que se gestiona en los procesos del SNGR, los dueños de la información, sus requerimientos de seguridad e inclusive los criterios de clasificación de ésta.
- **Servicios, Infraestructura y Aplicaciones:** Este apartado incluye la evaluación del estado actual de los componentes de infraestructura, la tecnología y las aplicaciones que proveen el soporte a la información que debe gestionar el SNGR.
- **Personas, Habilidades y Competencias:** Se refiere a las habilidades y competencias del personal o actores que interactuaran en el SNGR.

Para las distintas iniciativas, éstas deberán ser evaluadas en conjunto con el CGTI. Para esto la jefatura de TIC deberá utilizar instrumentos como los ejemplificados en el Anexo C (Plantilla de documentación de iniciativas) y el Anexo D (Plantilla de caso de negocio). Este tipo de instrumentos sirven como insumo al CGTI para la evaluación de las alternativas de implementación de las iniciativas estratégicas.

ANEXO A: PROCESOS DE LA CNE

PROCESOS SUSTANTIVOS/OPERATIVOS.

Fuente: Los nombres de procesos y procedimientos de este anexo fueron tomados de la identificación inicial realizada por la CNE, extraídos del documento Excel denominado **10-Integración de Procesos (DGR y ADSCRITAS).**

Procesos Sustantivos/Operativos de la Dirección de Gestión del Riesgo.	
Procesos	**Procedimientos**
Gerenciamiento de las unidades adscritas a la dirección de gestión del riesgo	• Planificación del trabajo de las Unidades. • Programación, planificación seguimiento y resultados de las actividades del trabajo, de las 5 Unidades. • Elaboración seguimiento y control presupuestario de la Dirección de Gestión del Riesgo. • Supervisión de las responsabilidades asignadas. • Evaluación del plan de la Dirección.
Coordinación del centro de operaciones de emergencia (COE).	• Seguimiento al Subsistema de Preparativos y Respuesta mediante las acciones establecidas en el Plan Nacional de Gestión del Riesgo. • Coordinación y conducción del Centro de Operaciones de Emergencias (COE). • Aplicación del Manual de Control de Operaciones de Emergencias (MACOE).
Asesoría en gestión del riesgo.	• Orientación técnica en gestión del riesgo al Sistema Nacional de Gestión del Riesgo (SNGR). • Asesoría a Instancias de Coordinación del Sistema Nacional de Gestión del Riesgo (SNGR) en el uso de información de riesgos.

	• Generación de información para otras unidades de la Comisión Nacional de Prevención del Riesgo y Atención de Emergencias (CNE). • Emisión de criterio técnico acorde al perfil de la unidad según las consultas de los entes de fiscalización.
Coordinación y participación en instancias de coordinación del sistema nacional de gestión del riesgo.	• Organización y funcionamiento de las instancias de coordinación del SNGR. • Estrategia de abordaje de las instancias de coordinación del SNGR. • Coordinación del Subsistema de Preparativos y Respuesta. • Participación y apoyo en Comisiones Especiales vinculados de los 3 subsistemas.
Gestión de proyectos.	• Gerenciamiento de proyectos para la gestión de recursos. • Asignación de proyectos según atinencia y prioridad a las unidades adscritas. • Seguimiento a proyectos nacionales y de cooperación internacional desde propuesta, seguimiento y ejecución.
Gestión de documentación e inforamción.	• Sistematización de Información en materia de Gestión del Riesgo. • Divulgación de la Gestión de Información del Riesgo que administra el Centro de Documentación (CEDO). • Atención a Solicitudes de Información en materia de Gestión del Riesgo. • Gestión digital de documentos referentes a la temática de Gestión del Riesgo.

Procesos Sustantivos/Operativos de Normalización y Asesoría	
Procesos	**Procedimientos**

Normalización en gestión de riesgo.	• Orientación sobre el proceso de emisión de resoluciones vinculantes ante el Sistema Nacional de Gestión del Riesgo (SNGR). • Verificación del cumplimiento de las resoluciones vinculantes emitidas por el ente rector. • Orientación sobre la organización y funcionamiento de las instancias de coordinación del Sistema Nacional de Gestión del Riesgo (SNGR). • Elaboración de esquema de certificación de competencias para gestores en la elaboración y evaluación de planes de preparativos y respuesta ante emergencias para centros laborales o de ocupación pública. • Implementación de esquema de certificación de competencias para gestores en la elaboración y evaluación de planes de preparativos y respuesta ante emergencias para centros laborales o de ocupación pública.
Asesoría en gestión del riesgo.	• Elaboración de la Estrategia de Capacitación en gestión del riesgo para las Instancias de Coordinación del Sistema Nacional de Gestión del Riesgo (SNGR). • Implementación de la Estrategia de Capacitación en gestión del riesgo. • Asesoría en la inclusión del Plan Nacional de Gestión del Riesgo en la dinámica de planificación y presupuestación de las instituciones. • Actualización del archivo de gestión de la oferta educativa en gestión del riesgo a nivel nacional. • Asesoría para la incorporación de la gestión integral del riesgo en la planificación y presupuestación de las instituciones públicas y las empresas privadas. • Asesoría a Instancias de Coordinación del Sistema Nacional de Gestión del Riesgo (SNGR) en el uso de información de riesgos. • Generación de información para otras unidades de la Comisión Nacional de Prevención del Riesgo y Atención de Emergencias (CNE). • Emisión de criterio técnico acorde al perfil de la unidad según las consultas de los entes de fiscalización. • Elaboración de programa de promoción de la gestión del riesgo en comunidades vulnerables. • Implementación de programa de promoción de la gestión del riesgo en comunidades vulnerables.

Coordinación y participación en instancias de coordinación del sistema nacional de gestión del riesgo	• Apoyo a los Subsistemas del Sistema Nacional de Gestión del Riesgo (SNGR). • Participación y apoyo en Comisiones Especiales.

Proceso Sustantivo / Operativo del Investigación, Análisis del Riesgo	
Proceso	**Procedimientos**
Investigación en gestión del riesgo	• Priorización de los ejes de investigación. • Gestión de recursos a los proyectos de investigación. • Promoción de la investigación en gestión del riesgo. • Implementación y seguimiento de los resultados de las investigaciones.
Gestión de información sobre riesgo	• Identificación de la información requerida en gestión del riesgo. • Integración y actualización de la información de riesgos en una sola base de datos. • Actualización y elaboración de Bases de datos cartográficas en gestión del riesgo.
Análisis en gestión del riesgo	• Evaluaciones especificas en riesgos (Inspecciones de riesgo). • Apoyo técnico y acompañamiento al desarrollo de los Sistemas de Alerta Temprana (SAT). • Emisión de criterio técnico para las resoluciones vinculantes. • Emisión de criterios técnicos especializados.
Asesoría en gestión del riesgo	• Pasantías especializadas.

	• Asesoría a Instancias de Coordinación del Sistema Nacional de Gestión del Riesgo (SNGR) en el uso de información de riesgos. • Generación de información para otras unidades de la Comisión Nacional de Prevención del Riesgo y Atención de Emergencias (CNE). • Emisión de criterio técnico acorde al perfil de la unidad según las consultas de los entes de fiscalización.
Coordinación y participación en instancias de coordinación del sistema de gestión del riesgo.	• Coordinación y participación de CAT ´s. • Coordinación del Subsistema de Reducción del Riesgo. • Participación y apoyo en Comisiones Especiales.

Procesos Sustantivos/Operativos	
Procesos	**Procedimientos**
Asesoría en gestión del riesgo	• Asesoría en el régimen de excepción en el marco de las declaratorias de emergencias. • Asesoría para la elaboración de informes de pérdidas y daños. • Atención de solicitudes de información referente a los Informes de los PGE (interno y externo). • Asesoría a Instancias de Coordinación del Sistema Nacional de Gestión del Riesgo (SNGR) en el uso de información de riesgos. • Generación de información para otras unidades de la Comisión Nacional de Prevención del Riesgo y Atención de Emergencias (CNE).

	• Emisión de criterio técnico acorde al perfil de la unidad según las consultas de los entes de fiscalización.
Coordinación y participación en instancias de coordinación del sistema nacional de gestión del riesgo	• Coordinación del Subsistema de Recuperación. • Participación y apoyo en Comisiones Especiales.
Análisis en gestión del riesgo	• Inspecciones de riesgo en infraestructura. • Contrataciones de Estudios Técnicos para el desarrollo de Obras.
Contrataciones por emergencias no declaradas	• Solicitud de contratación de maquinaria por Primeros Impactos. • Seguimiento y tramites de facturas de contrataciones de emergencias no declaradas. • Fiscalización de contrataciones de maquinaria por Primeros Impactos.
Recuperación por extrema urgencia	• Adquisición de bienes o servicios por extrema urgencia (Art. 40 Ley 8488). • Ejecución y Fiscalización de contrataciones por Extrema Urgencia. • Trámite de pagos por contrataciones en Extrema Urgencia. • Cierre de las contrataciones por Extrema Urgencia. • Resolución Contractual en contrataciones PI-CNE.
Gestión del plan general de la emergencia	• Elaboración del Plan General de la Emergencia • Acompañamiento técnico en la aprobación del Plan General de la Emergencia • Inclusión Extemporánea al Plan General de la Emergencia • Criterio técnico para la inclusión extemporánea al Plan General de la Emergencia

	• Acompañamiento técnico en la aprobación de Inclusión Extemporánea • Solicitud de información para el seguimiento del Plan General de la Emergencia (interno y externo) • Elaboración del Informe de Seguimiento del Plan General de la Emergencia • Acompañamiento técnico en la aprobación del Informe de Seguimiento de los PGE. • Elaboración del finiquito de los PGE. • Acompañamiento técnico en la aprobación del finiquito de los PGE. • Promoción de los PGE. • Acompañamiento para la elaboración de los planes de inversión. • Revisión técnica del Plan de Inversión por Emergencia Declarada. • Solicitud de Contratación por Emergencia Declarada Proveeduría Institucional -CNE. • Fiscalización previa de Contratación por Emergencia Declarada Proveeduría Institucional -U.E. • Fiscalización posterior del Proceso de Contratación por Emergencia Declarada Proveeduría Institucional -U.E. • Gestión documental de planes de inversión. • Actualización y elaboración de bases de datos de los estudios realizados. • Inspección y fiscalización de la ejecución contractual. • Trámites de ordenes de servicio y modificación. • Resolución Contractual en contrataciones PI-CNE. • Trámite de pagos por contrataciones por PGE.

Procesos Sustantivos/Operativos DESNGR	
Procesos	**Procedimientos**
Politica nacional de gestión del riesgo.	• Elaboración de la Política Nacional de Gestión del Riesgo. • Acompañamiento técnico en la aprobación de la Política Nacional de Gestión del Riesgo. • Presentación y difusión de la Política Nacional de Gestión del Riesgo. • Articulación de la Política Nacional de Gestión del Riesgo en la dinámica sectorial. • Seguimiento y monitoreo de la Política Nacional de Gestión del Riesgo. • Evaluación de la Política Nacional de Gestión del Riesgo. • Elaborar la metodología de monitoreo, seguimiento y evaluación de la política.
Plan nacional de gestión del riesgo.	• Elaboración del Plan Nacional de Gestión del Riesgo. • Acompañamiento técnico en la aprobación del Plan Nacional de Gestión del Riesgo. • Presentación y difusión de Plan Nacional de Gestión del Riesgo. • Seguimiento y monitoreo del Plan Nacional de Gestión del Riesgo. • Generar compromisos institucionales. • Socializar el Plan Nacional de Gestión del Riesgo. • Revisión y ajustes de metas del PNGR.
Foro nacional sobre el riesgo.	• Convocatoria del Foro Nacional sobre el Riesgo. • Desarrollo del Foro Nacional sobre el Riesgo.

	• Elaboración del informe de resultados del Foro Nacional sobre el Riesgo. • Seguimiento a los acuerdos del Foro Nacional Sobre el Riesgo.
Asesoría en gestión del riesgo.	• Emisión de criterios técnicos en materia de política de gestión del riesgo a nivel nacional, regional e internacional. • Asesoría a Instancias de Coordinación del Sistema Nacional de Gestión del Riesgo (SNGR) en el uso de información de riesgos. • Generación de información para otras unidades de la Comisión Nacional de Prevención del Riesgo y Atención de Emergencias (CNE). • Emisión de criterio técnico acorde al perfil de la unidad según las consultas de los entes de fiscalización.
Coordinación y participación en instancias de coordinación del sistema nacional de gestión del riesgo.	• Apoyo a los Subsistemas del Sistema Nacional de Gestión del Riesgo (SNGR). • Seguimiento y monitoreo al Sistema Nacional de Gestión del Riesgo (SNGR). • Participación y apoyo en Comisiones Especiales.
Monitoreo del plan nacional de gestión de riesgo.	CNE-DGR-DESNGR-NRIPNGR-6.1. Notificar las responsabilidades institucionales ante el Plan Nacional de Gestión del Riesgo CNE-DGR-DESNGR-GNPMPNGR-6.2 Generar notificaciones del proceso de monitoreo del Plan Nacional de Gestión del Riesgo. CNE-DGR-DESNGR-AAGI-6.3 Administrar el archivo de gestión institucional.

	CNE-DGR-DESNGR-LCCEID-6.4 Logística y convocatoria para la capacitación de los enlaces institucionales designados. CNE-DGR-DESNGR-CEIVP-6.5 Capacitar a los enlaces institucionales vía presencial. CNE-DGR-DESNGR-CEIVT-6.6 Capacitar a los enlaces institucionales vía telefónica. CNE-DGR-DESNGR-ACAEC-6.7 Atender consultas y asesorar a los enlaces capacitados. CNE-DGR-DESNGR-ARIGEI-6.8 Aprobación de reportes institucionales generados por los enlaces institucionales. CNE-DGR-DESNGR-SRIA-6.9 Sistematizar los reportes institucionales aprobados.
Seguimiento del plan nacional de gestión del riesgo.	• Elaboración de informes de seguimiento.

Procesos Sustantivos/Operativos GO	
Procesos	**Procedimientos**
Preparativos ante emergencias	• Acreditación. • Capacitación/Asesoría. • Procedimientos/Protocolos. • Organización (N-R-M-C-I) CATs.

	• Planes (Emerg-Contin-Respuesta).
Coordinación instancias técnicas	• Coordinación CATs. • Coordinación CE. • Solicitud Criterios a los CATs. • Participación Comisiones Especiales.
Respuesta ante emergencias	• Manejo de Información. • Manejo Operativo. • Atención de incidentes. • Inspecciones. • Activación por Alertas. • Manejo de Logística en la respuesta. • Comunicaciones en la Respuesta. • Coordinación interinstitucional. • Disponibilidad. • Gestión de créditos. • Primeros impactos. • Cierre operativo (Informe de Cierre). • Cierre administrativo (Informe evaluación).
Asesoría en gestión del riesgo	• Asesoría a Instancias de Coordinación del Sistema Nacional de Gestión del Riesgo (SNGR) en el uso de información de riesgos. • Generación de información para otras unidades de la Comisión Nacional de Prevención del Riesgo y Atención de Emergencias (CNE). • Emisión de criterio técnico acorde al perfil de la unidad según las consultas de los entes de fiscalización.

Coordinación y participación en instancias de coordinación del sistema nacional de gestión del riesgo	• Apoyo al Subsistema de Preparativos y Respuesta. • Participación y apoyo en Comisiones Especiales.
Logística ante emergencias	• Instalaciones. • Comunicaciones. • Equipos/Suministros (inventarios, Activos, Portafolio, Mantenimiento, Control asignaciones, Compras). • Transportes. • Seguridad.
Info-Comunicaciones ante emergencias	• Monitoreo/Vigilancia. • Alerta/Activación. • Procesamiento de datos. • Gestión de Redes de radio. • Gestión de Redes Telefónicas (TIC).
Sistemas de alerta temprana (SAT)	• Organización/Preparación (N-R-M-C-I) CATs. • Monitoreo. • Activación.

Procesos Sustantivos/Operativos Respuesta ante emergencias	
Procesos	**Procedimientos**

Vigilancia y seguimiento de amenazas/Eventos	• Monitoreo de las amenazas. • Análisis técnico del aviso oportuno. • Seguimiento del evento. • Emisiones de alertas. • Coordinación con grupos especializados.
Activación institucional e interinstitucional	• Activación de la CNE. • Activación del CIA. • Activación de los CATs. • Activación de las instancias de coordinación regional y municipal. • Activación del COE.
Gestión de información	• Información o comunicación pública. • Información del SNGR. • Incidentes 911. • Informes de situación de emergencia. • Incidentes informales. • Elaboración de informes.
Gestión de las operaciones	• Activación de comité de emergencias. • Movilización de personal al campo. • Identificación de necesidades de emergencias. • Activación del COE. • Activación de la sala de situación.
Recursos financieros	• Pago de créditos. • Giros de gastos de operación.

	• Giros de gastos de funcionarios.
Logística	• Abastecimiento de suministros a la emergencia. • Activación de contratos por demandas. • Autorizaciones de crédito por primer impacto. • Contrataciones de maquinaria por primer impacto. • Contrataciones de servicios por primer impacto. • Contrataciones para adquisición de suministros por primer impacto. • Voluntariado. • Donaciones. • Articulación del SNGR (Donaciones, por ejemplo, camiones).
Cooperación internacional	• Recepción de AHT. • Tránsito de AHT. • Envío de AHT.

Procesos de apoyo	
Procesos	**Procedimientos**
Planificación operativa institucional	• Elaboración de insumos para el POI. • Seguimiento semestral del POI. • Seguimiento y evaluación del POI. • Insumos para el Informe de evaluación de metas del PND • Reuniones de Seguimiento del POI.

	• Revisión del Mapa de Procesos de la unidad. • Levantamiento/reingeniería de los procedimientos. • Evaluación del Sistema de Control Interno. • Valoración de riesgos de la unidad.
Presupuesto operativo	• Elaboración de insumos para el Presupuesto Operativo y Plan de Compras. • Modificaciones presupuestarias y al plan de compras. • Seguimiento del Presupuesto Operativo. • Informe de avance de ejecución presupuestaria.
Contratación de bienes y servicios	• Solicitud de contratación de bienes/servicios (diferentes modalidades de contratación). • Análisis y búsqueda previa de ofertas. • Elaboración del cartel. • Presentación de la solicitud de contratación en SICOP. • Solicitud de aclaraciones. • Elaboración del estudio técnico de las ofertas. • Seguimiento de las contrataciones. • Solicitud de pago a proveedores (transferencia, cheque o caja chica). • Ejecución y devolución de garantías.
Gestión de archivo	• Elaboración de oficios. • Correspondencia enviada (interna y externa). • Correspondencia recibida (interna y externa). • Archivo de minutas, informes especiales, entre otros. • Traslado de correspondencia.

Gestión administrativa general	• Solicitud de vehículos. • Solicitud de viáticos. • Liquidación de viáticos. • Control de suministros. • Solicitud de suministros. • Traslado de activos. • Traslado de equipo fuera de la institución. • Soporte de activos. • Pago de horas extra por tiempo extraordinario. • Autorización de capacitación. • Justificaciones de control de asistencia. • Solicitud de boletas de viajes al exterior (póliza, informe de viaje). • Solicitud de vacaciones. • Respuesta a solicitudes administrativas (externas, internas). • Evolución de desempeño anual. • Inducción a nuevo personal contratado. • Criterio técnico en los procesos de contratación de recurso humano. • Asignación de responsable de la Unidad en caso de ausencia. • Elaboración plan de giras. • Elaboración de informes de giras, elaboración de los informes de participación en actividades en el exterior. • Liquidación de combustible/tiquetes. • Solicitud de permisos especiales (con y sin goce de salario). • Logística para eventos nacionales e internacionales (capacitaciones, reuniones, entre otros). • Resoluciones para el otorgamiento de becas o subsidios. • Autorización de créditos. • Pago de créditos.

Servicio al cliente	• Mediante vía telefónica. • Mediante vía presencial (interno y externo). • Mediante correo electrónico. • Mediante redes sociales o medios de prensa. • Atención a medios de comunicación. • Traslado de solicitudes. • Visibilidad de las actividades CNE, SNGR. • Trazabilidad de las quejas.

ANEXO B: NECESIDADES DE LAS PARTES INTERESADAS

Esta tabla se puede usar para establecer y priorizar metas corporativas específicas o relacionadas con TI, basadas en las necesidades de las partes interesadas. Deben tomarse las mismas precauciones cuando se usen estas tablas que cuando se usen las otras tablas de metas en cascada, es decir, la situación de cada empresa es diferente y no deben usarse estas tablas de forma mecánica, sino sólo como sugerencia de un conjunto genérico de relaciones. En la figura, la intersección entre la necesidad de un interesado y una meta corporativa está coloreada si esa necesidad debe ser considerada para esa meta.

NECESIDADES DE LAS PARTES INTERESADAS	Valor para los Interesados de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basada en Información	Optimización de los costes de los procesos de negocio	Optimización de la funcionalidad de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Cumplimiento con políticas internas	Personas preparadas y motivadas	Cultura de innovación de producto y negocio
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
¿Cómo se consigue valor mediante el uso de TI? ¿ Está el usuario final satisfecho con la calidad del servicio de TI?	■	■				■	■						■			■	■
¿Cómo se gestiona el rendimiento de TI?		■			■				■	■	■	■		■			
¿Cómo se puede explotar mejor la tecnología de red para conseguir nuevas oportunidades estratégicas?	■	■						■					■			■	■
¿Cómo puedo construir y estructurar mejor mi departamento de TI?								■		■	■	■		■	■	■	
¿Cuánto dependo de mis proveedores externos? ¿Cómo de bien están siendo gestionados los acuerdos de externalización de TI? ¿Cómo puedo verificarlos sobre proveedores externos?			■	■						■							
¿Cuáles son los requisitos (de control) para la información?				■					■						■		
¿He contemplado todo los riesgos relacionados con TI?			■				■		■						■		
¿Estoy ejecutando una operación de TI eficiente y robusta?					■		■										
¿Cómo se controla el coste de TI? ¿Cómo se usan los recursos de TI en la manera más efectiva y eficiente? ¿Cuáles son las opciones de aprovisionamiento más efectivas y eficientes?										■		■		■			

¿Tengo suficiente personal para TI? ¿Cómo puedo desarrollar y mantener sus habilidades y cómo gestiono su rendimiento?										■		■		■			
¿Cómo consigo confianza sobre TI?				■											■		
¿Está bien securizada la información que se está procesando?				■			■								■		
¿Cómo se puede mejorar la capacidad de respuesta del negocio mediante un entorno de IT más flexible?	■							■								■	■
¿Fracasan los proyectos de TI en proporcionar lo que habían prometido? Si es así, ¿por qué permanece la TI en el camino de ejecutar la estrategia de negocio	■	■	■					■			■	■	■				
¿Cómo es de crítica la TI para para la sostenibilidad de la empresa? ¿Qué pasaría si la TI no estuviera disponible?	■	■					■										
¿Qué procesos de negocio críticos dependen de TI y cuáles son los requerimientos de los procesos de negocio?	■	■									■	■					
¿En cuánto han excedido de media los presupuestos de operación de TI? ¿Con qué frecuencia y cuánto se salen del presupuesto los proyectos de TI?					■					■		■		■			
¿Qué parte del esfuerzo de TI se dedica a apagar fuegos en lugar de facilitar las mejoras del negocio?		■	■									■					
¿Son suficientes los recursos y la infraestructura de TI disponibles para conseguir los objetivos estratégicos de empresa requeridos?		■			■					■		■					
¿Cuánto se tarda en la toma de decisiones importantes de TI?	■	■			■			■									
¿Son transparentes el esfuerzo y las inversiones totales en TI?		■		■	■										■		
¿Respalda TI a la empresa en el cumplimiento de la normativa y los niveles de servicio? ¿Cómo puedo saber si se cumple con				■											■		

<table>
<tr><td>Iniciativa:
Nombre</td><td colspan="4">Objetivos:
Objetivos</td></tr>
<tr><td>Requisitos funcionales</td><td>Especificaciones técnicas</td><td colspan="3">Esfuerzo</td></tr>
<tr><td rowspan="4">Se requiere…</td><td rowspan="4">Resumas las especificaciones técnicas requeridas por la iniciativa</td><td>Plan de trabajo:

1. Actividad macro
2. Actividad macro
3. Actividad macro</td><td>Costos:

Los costos tendrán en cuenta …</td><td>Dificulta de implementación:
1. Ejemplo: Resistencia al cambio...
2.
3.</td></tr>
<tr><td colspan="3">Implicaciones en la organización:

Se deberá ...</td></tr>
<tr><td colspan="3">Impacto</td></tr>
<tr><td colspan="2">Económico:

Se reducirán los costos de …</td><td>Estratégico:

Describa alineación con PETI</td></tr>
</table>

El caso de negocio es una herramienta usada para demostrar la generación de valor de las inversiones en TIC.

	Especificación general	Especificación por nivel		
		Capacidad tecnológica	Capacidad operativa	Capacidad de negocio
Resultados (intermedios y finales)				
Alineación				
Beneficios financieros				

	Especificación general	Especificación por nivel		
		Capacidad tecnológica	Capacidad operativa	Capacidad de negocio
Beneficios no financieros				
Recursos y gastos				
Riesgos				
Suposiciones y limitaciones				

GLOSARIO

ACRÓNIMO	SIGNIFICADO
ADM	Por siglas en inglés: Architecture Development Method
BI	Inteligencia de negocios
BPM	Gestión de Procesos de Negocio
CIA	Centro de Información y Análisis
CNE	Comisión Nacional de Emergencias
CGTI	Comité Gerencial del TI
COBIT	Por siglas en inglés: Control Objectives for Information and Related Technologies
ESB	Por siglas en inglés: Enterprise Service Bus
FODA	Fortalezas, Oportunidades, Debilidades, Amenazas
ITIL	Por siglas en inglés: Information Technology Infrastructure Library
LAN	Red de área local
MDM	Por siglas en inglés: Master Data Management
MICITT	Ministerio de Ciencia, Tecnología y Telecomunicaciones
PEI	Plan Estratégico Institucional
PETI	Plan Estratégico de Tecnologías de Información
PNGR	Política Nacional de Gestión de Riesgo
SCRUM	Metodología ágil de desarrollo de software
SEVRI	Sistema Específico de Valoración del Riesgo Institucional
SINART	Sistema Nacional de Radio y Televisión
SNGR	Sistema Nacional de Gestión de Riesgo
TIC	Tecnologías de Información y Comunicación
TOGAF	Por siglas en inglés: The Open Group Architecture Framework
UTI	Unidad de Tecnologías de Información
VLAN	Red LAN Virtual
ADM	Por siglas en inglés: Architecture Development Method