PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN - PETI

2019-2022

FASE 2

OFICINA ASESORIA DE INFORMATICA

Enero de 2020

Elaborado por: Julián Adolfo Vásquez Ospina – Asesor de Informática

José Luis Brand Portilla – Contratista

Revisado Por: Comité de Gobierno Digital – INCIVA

Aprobado Por: Jonathan Velásquez Álzate

Tabla de contenido

INTRODUCCION

En la Actualidad las empresas están comenzando a reconocer la importancia que la tecnología tiene para realizar sus procesos misionales, lo que la ha llevado a dejar de ser un factor de apoyo para convertirse en un parte fundamental que soporte todas las áreas de la organización.

El INCIVA como ente descentralizado de la Gobernación del Valle, está en la obligación de cumplir la política de gobierno digital impuesta en el decreto No 1008 del 14 de junio del 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. Es por eso que nace la necesidad de generar un plan de TI acorde con los lineamientos y exigencias del Ministerio de tecnologías de la información y las comunicaciones. (MinTic).

El presente documento genera las bases en la búsqueda de llegar al éxito en la implementación de una Arquitectura Empresarial articulada con el marco de referencia propuesto por el Ministerio de Tecnologías de la información y Comunicaciones (MinTic).

Es de entender que este documento estará sometido a constantes mejoras y documentación de los dominios de AE en la medida que estos se vayan Implementando.

OBJETIVOS

El objetivo Principal del Plan Estratégico de las tecnologías de la información – PETI del Instituto para la Investigación y la Preservación del Patrimonio Cultural y Natural del Valle del Cauca – INCIVA es promover la modernización de la administración de la entidad apoyados en el uso de las TIC para contribuir en la difusión de la información que esta misma provee.

Objetivos Específicos

- Implementar los lineamientos para una correcta gestión de recursos tecnológicos e infraestructura de la información.
- Generar estrategias que lleven a la correcta implementación de una Arquitectura Empresarial de acuerdo al marco de referencia de MinTIC y las buenas prácticas de TI.
- Generar conciencia del valor y el uso estratégico de TI en la entidad.

ALCANCE

El plan estratégico de tecnologías de la información “PETI” se presenta para el periodo comprendido entre los años 2019 – 2022 y busca generar estrategias que lleven a la correcta implementación de una Arquitectura Empresarial (AE) de acuerdo a los lineamientos propuestos por el marco de referencia de Min TIC.

Inicialmente se darán las bases para la implementación de los dominios del marco de referencia AE:

- Estrategia de TI
- Gobierno de TI
- Sistemas de Información
- Servicios Tecnológicos
- Uso y apropiación

Es de anotar que el presente documento aplica para todas las áreas de la entidad y presentará actualizaciones y/o mejoras de acuerdo a las necesidades, Y demás factores que se generen durante la actual vigencia. Teniendo en cuenta que el INCIVA cuenta con una sede central y 5 centros operativos, los cuales 4 se encuentran fuera de la ciudad de Cali, el alcance de este plan estratégico será para la sede central del INCIVA y el Museo de Ciencias Naturales Federico Carlos Lehmann, ubicado en la Avenida Roosevelt # 24-80 de la ciudad de Cali, Valle del Cauca

MARCO NORMATIVO

El presente plan está regido por las siguientes normas y/o decretos y lineamientos del orden nacional:

- Que la ley 1753 de 2015, Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país” en el artículo 45 establece:” Estándares, modelos y lineamientos de tecnologías de la información y las comunicaciones para los servicios al ciudadano”
- Que mediante el decreto 1008 de 2018, se define la política de Gobierno Digital, por el cual se establecen los lineamientos generales de la política de Gobierno Digital, la cual tiene por objeto promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.
- Que mediante Decreto N°415 de 7 de marzo 2016, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones
- Que la Ley 1341 de 2009, en el Parágrafo de su artículo 38 establece que: “Las autoridades territoriales implementarán los mecanismos a su alcance para gestionar recursos a nivel nacional e internacional, para apoyar la masificación de las TIC, en sus respectivas jurisdicciones”.
- Que la Ley 1474 de 2011, Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública, hace referencia al uso obligatorio de los sitios web de las entidades públicas como mecanismo para la divulgación de información pública.
- Que, a su turno, el artículo 232 de la Ley 1450 de 2011 prevé, sobre la Racionalización de trámites y procedimientos al interior de las entidades públicas. Que: los organismos y entidades de la Rama Ejecutiva del Orden Nacional y Territorial procederán a identificar, racionalizar y simplificar los procesos, procedimientos, trámites y servicios internos, con el propósito de eliminar duplicidad de funciones y barreras que impidan la oportuna, eficiente y eficaz prestación del servicio en la gestión de las organizaciones.
- Que a su turno el Decreto – Ley 019 de 2012, por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública, estableció en su artículo 4, en relación con la celeridad en las actuaciones administrativas, que: “Las autoridades tienen el impulso oficioso de los procesos administrativos; deben utilizar: formularios gratuitos para actuaciones en serie, cuando la naturaleza de ellas lo haga posible y cuando sea asunto de

su competencia, suprimir los trámites innecesarios, sin que ello las releve de la obligación de considerar y valorar todos los argumentos de los interesados y los medios de pruebas decretados y practicados; deben incentivar el uso de las tecnologías de la información y las comunicaciones a efectos de que los procesos administrativos se adelanten con diligencia, dentro de los términos legales y sin dilaciones injustificadas; y deben adoptar las decisiones administrativas en el menor tiempo posible".

- Que en concordancia con lo anterior, el artículo 63 del Decreto 067 del 31 de Julio de 2009, mediante el cual se creó el estatuto básico de la Administración Municipal, consagra que con el fin de mejorar la atención de los servicios y cumplir con eficacia y eficiencia los objetivos, políticas y programas de las dependencias centrales, el alcalde, previo estudio de viabilidad y conveniencia emitido por el DAFP, podrá organizar con carácter permanente o transitorio, grupos internos de trabajo que sean necesarios. También podrá con el mismo procedimiento, fusionar o suprimir los que hayan creado, cuando el desarrollo de los procesos, competencias y funciones de las dependencias así lo exija.
- Que mediante Decreto No 2573 de 2014, se reglamenta parcialmente la Ley 1341 de 2009 y que en el mismo decreto se define el componente de Privacidad y Seguridad de la información que incluye el modelo de seguridad y privacidad de la información (MSPI), y para ello cuenta con una serie de guías anexas que ayudan a las entidades a cumplir con lo solicitado permitiendo abordar de manera detallada cada una de las fases del modelo, buscando a su vez comprender cuales son los resultados a obtener y como desarrollarlos.
- Que mediante el CONPES - Política Nacional de Seguridad Digital, se tiene como objetivo: "Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país".
- Que mediante Resolución No 0002405 de 25 de noviembre de 2016, por el cual se adopta el sello de la excelencia Gobierno en Línea y se conforma su comité.
- Que mediante Resolución No 0002710 del 3 de octubre de 2017, "Por la cual se establecen lineamientos para la adopción del protocolo IPv6"
- Que mediante el decreto 415 de 2016, se adiciona al decreto único reglamentario de la función pública la definición de lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

- Que mediante el decreto 1499 de 2017, se modifica el decreto 1083 de 2015 y se definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública.

RUPTURAS ESTRATÉGICAS

El Instituto para la Investigación y la Preservación del Patrimonio Cultural y Natural del Valle del Cauca – INCIVA, busca ser una organización alineada con las nuevas tecnologías y marcos de trabajo de TI.

Por lo anterior se considera, que la gestión de TI ha sido tradicionalmente un proceso de apoyo, hoy en día es necesario convertirlo en un pilar fundamental en la consecución de sus objetivos, ayudando a presentar una organización moderna, con mejores prácticas , de cara a dar un servicio de la mejor calidad al ciudadano y publico interno, por lo cual es necesario plantear la inquietudes que surgen del análisis de madurez de TI, con el fin de fomentar el cambiar paradigmas y adoptar pensamientos que consideren la tecnología como un área fundamental:

- La gestión de tecnología debería ser más que un proceso de soporte, reparación y de provisión de equipos de cómputo, en el mundo de hoy TI es un factor estratégico para la organización.
- Se hace evidente la necesidad del Plan Estratégico de TI
- Realizar desarrollos al interior de la organización es tan viable como contratar o comprar soluciones de software, sin embargo, hay que definir muy bien el alcance de ambas opciones.
- Se requiere la implementación de indicadores para la medición de los servicios de TI y del uso y apropiación de los sistemas.
- Definir los estándares de integración de sistemas con el fin de facilitar la transferencia de información entre ellos.
- Es necesario definir estándares para la gestión de la calidad en la información.
- Fortalecer el análisis de la información en todas las áreas.
- Promover la disponibilidad de la información como factor fundamental en la toma de decisiones.
- Desarrollar e implementar soluciones de cara al ciudadano que den valor agregado y permitan mejorar la imagen de eficiencia y buen servicio.

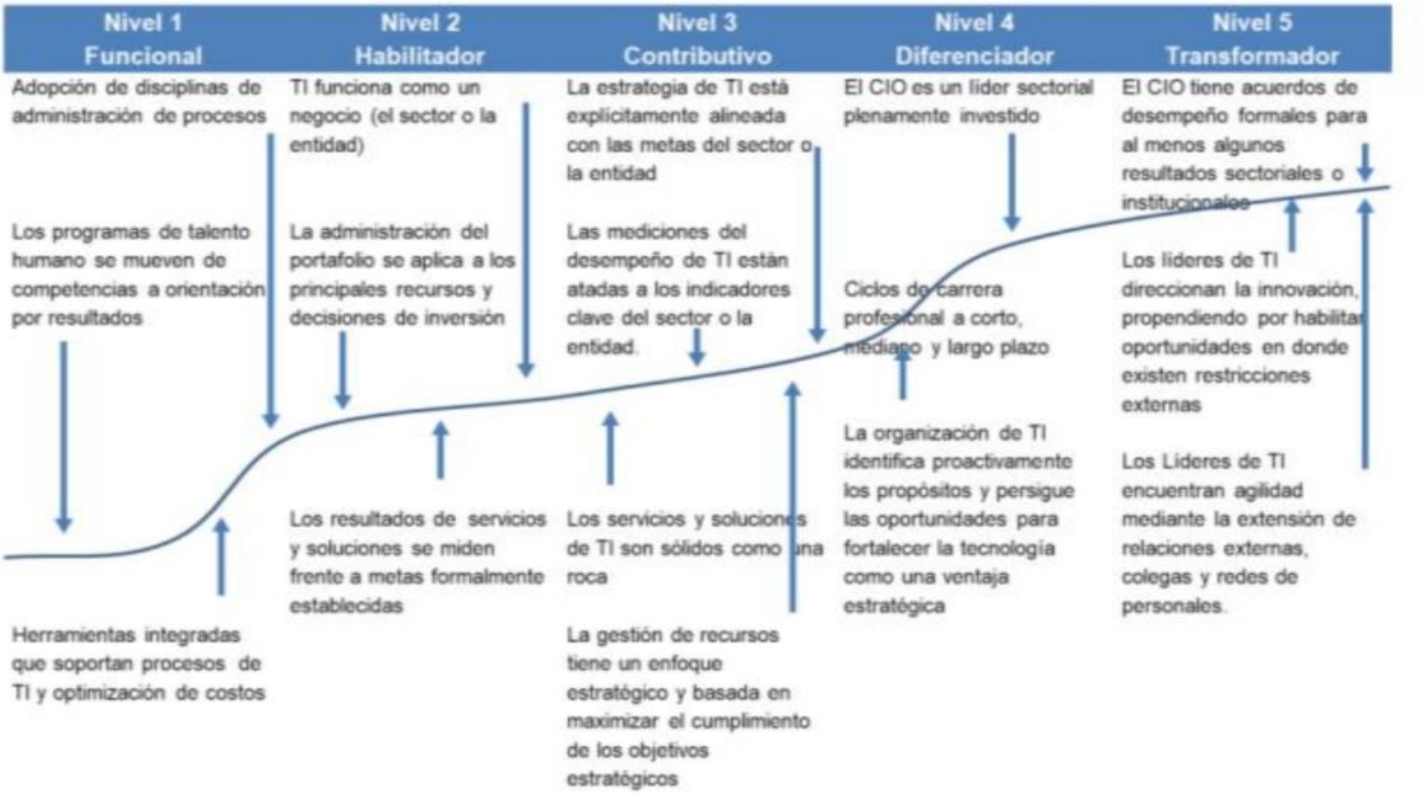


Imagen: Niveles de madurez de la Gestión - Gartner

ANÁLISIS DE LA SITUACIÓN ACTUAL

Estrategia de TI

El Instituto para la Investigación y la Preservación del Patrimonio Cultural y Natural del Valle del Cauca –INCIVA, por ser una entidad del estado, está regida por la normatividad de orden nacional y territorial y en muchas ocasiones por decisiones de la administración que se encuentra en ese momento no se va más lejos del cumplimiento de la ley.

Sin embargo, hoy en día aún no se ha dado un rol fundamental completamente a TI, aún falta dar ciertos pasos para crear un área estratégica de TI en lugar de ser un área netamente de apoyo y soporte.

Uso y apropiación de la tecnología

Sistemas de información

- Nombre: Sistema de administración Financiera ERP Vigente

  Descripción: Tiene como objetivo ser un instrumento para la rendición de cuentas, viabilizar la gestión contable y generar condiciones de transparencia sobre el uso, gestión y conservación de los recursos y su patrimonio.
  permite la administración y seguimiento de los diferentes tipos de ingresos o egresos que posee la entidad.
  Se lleva el registro de todos los datos básicos como características tributarias de los funcionarios y proveedores de la entidad además permite mediante el programa de facturación el registro y cuentas por pagar a los mismos.
  Genera los correspondientes registros contables y presupuestales.

  Administración y soporte: la administración, actualización, mantenimiento, soporte, seguimiento y control del sistema, es realizado por la empresa desarrolladora contratista.

- Nombre: Sigecem (sistema de gestión documental)

  Descripción: Es un sistema de gestión documental que permite administrar el flujo de documentos y todo tipo para apoyar la labor del área de Gestión documental y de la Radicación de documentos en la entidad, permitiendo llevar a cabo la administración de los documentos de una forma más eficiente, eficaz y con menores costos.
  -Agiliza los trámites de los procesos documentales.
  -Controla el cumplimiento de los términos de vencimiento.
  -Minimiza el riesgo de pérdida de documentos.
  -Mejora la conservación e integridad de los documentos evitando su manipulación.
  -permite la consulta de la información de los documentos radicados y sus imágenes digitalizadas.

  Administración y soporte: la administración, mantenimiento, soporte, seguimiento y control de Sigecem, es realizado por la empresa proveedora contratista.

- Nombre: GLPI (Mesa de Servicios)

  Descripción: Es una herramienta que permite la recolección de solicitudes de soporte en todas las áreas en la entidad, permitiendo la comunicación entre el usuario solicitante y le área de sistemas.
  La solicitud se lleva a cabo por medio del diligenciamiento de un formulario.

  Administración y soporte: la administración, mantenimiento, soporte, seguimiento y control de, es realizado por el asesor de informática.

- Nombre: Portal web oficial del INCIVA

  Descripción: El sitio web de la entidad es un portal público que permite que el ciudadano tenga entera información de la entidad, no solo de los servicios y recursos que presta sino de todo lo perteneciente a la institución. como lo es: Directorio de funcionarios,
  Organigrama, Mapa de procesos. Y la gestión institucional: Rendición de cuentas, Planes y programas, Informes, Metas e indicadores de gestión, Información financiera y contable, Mapa institucional de riesgos, Proyectos de inversión, Acuerdo laboral, Organizaciones sindicales, Entes de control.

  Administración y soporte: la administración, actualización, de la página es realizado por el área de divulgaciones, y el mantenimiento, soporte, seguimiento y control, de es realizado por la empresa diseñadora contratista.

- Nombre: Google Apps

  Descripción: Google Apps es la plataforma utilizada para la aplicación de correo institucional y almacenamiento en la nube en la entidad, con el fin de identificar de manera oficial a la institución; confirma que el remitente es una entidad formal y de confianza. (@INCIVA.GOV.CO)
  Además de ser utilizado como medio de comunicación oficial y evidenciado dentro de la misma institución.

  El almacenamiento en la nube se utiliza como una herramienta de manejo y administración de archivos oficiales de la institución entre

funcionarios y también para la realización de Backup de la información importante que los funcionarios manejen con respecto a la institución.

Administración y soporte: la administración de cuentas, y gestión de pagos del servicio es realizado por el asesor de informática. El mantenimiento, soporte, seguimiento y control, de es realizado por la empresa dueña de la plataforma y prestadora el servicio.

Servicios Tecnológicos

Estrategia y gobierno (Condiciones generales)

- El mantenimiento preventivo de equipos debe realizarse con una periodicidad de 12 meses.
- El área de sistemas es la encargada de la programación y ejecución del mantenimiento preventivo de los equipos de cómputo.
- La información respaldada de la sede central se almacena inicialmente en el servidor de almacenamiento en la nube.
- Los usuarios deben trabajar la información de la entidad en los equipos institucionales que están dentro del dominio de la misma, y no deben almacenar información personal.
- Los usuarios deben realizar backup de la información de la entidad en el almacenamiento en la nube con una periodicidad de 30 días, quedando constancia de su realización firmando el formato, FO-PNIF-04
- A los usuarios que se retiran de la entidad se les realiza un backup completo de la información almacenada en la nube y correo electrónico.
- Todos los requerimientos a sistemas se deberán tramitar a través de la mesa de servicios en el link de soporte a sistemas en la cual se diligencia el formulario para él envió de ticket, una vez recibido el ticket el personal de sistemas atenderá el requerimiento.
- La información backup de la información será custodiada por el proveedor del almacenamiento en la nube.

Descripción del procedimiento

Adquisición, instalación y soporte de software y hardware.

No	DESCRIPCION DE LA ACTIVIDAD	RESPONSABLE	REGISTRO	PUNTOS DE CONTROL
1	GESTION DE COMPRA DE SOFTWARE y HARDWARE: -El área respetiva presenta al área de sistemas los requerimientos de software o hardware con la respectiva sustentación de la necesidad. - El asesor de informática perteneciente área mencionada evalúa la necesidad, elabora y pasa el oficio de requerimiento explicando la necesidad a la dirección. Acorde a los procedimientos vigentes del Sistema de Gestión. -Si se aprueba, el oficio de requerimiento va a presupuesto donde se elabora la disponibilidad (CDP). - Con el CDP el asesor de informática elabora los Estudios Previos y se Pide el producto por Licitación o por el sistema de “Colombia compra Eficiente” -Cuando llega el producto es recibido por área de sistemas y la factura pasa	-Área de sistemas -Dirección -Presupuesto -Jurídica -Comité evaluador -Almacén -Contabilidad -Tesorería	-Requerimiento -CDP -Estudios Previos -Licitación -Factura -CRP	x

	a Presupuesto donde elaboran el “CRP”, tanto el CRP como una copia de la factura son enviados a Almacén para darle Ingreso al hardware, o a sistemas en caso de software. -El CDP y la factura también pasan a Contabilidad y después a Tesorería para su respectivo ingreso contable.			
2	PUESTA EN OPERACIÓN DEL SOFTWARE O HARDWARE: -El personal del área de sistemas instala el software o hardware en la respectiva área requerida. -Se migra la información del área pertinente desde otros sistemas, si la hay. -se ejecutan pruebas del sistema. -se realiza la capacitación del uso el sistema a los usuarios del área. -se estabiliza el sistema y se entrega al usuario encargado.	-Área de sistemas. -Área pertinente.	-Formato de capacitación o inducción -FO-PINF-01 Hoja de vida de equipos	x
3	OPTIMIZACION DEL SOFTWARE O HARDWARE: -El área pertinente al sistema instalado genera una solicitud por medio de	-Área de sistemas. -Área pertinente.	-Ticket de la mesa de servicios	x

	un ticket en la mesa de servicios. -Personal del área de sistemas atiende el ticket. -se inicia la operación de las funcionalidades que no se incluyeron en la instalación o pruebas del sistema de acuerdo a lo solicitud del usuario del área pertinente, optimizando los servicios que presta el sistema. -Al estar resuelta la solicitud, el ticket se da por cerrado y solucionado.			
	LICENCIAMIENTO DEL SOFTWARE: - Todos los softwares de la entidad están licenciados y deben renovarse, para ello se suscribe un contrato de mantenimiento con el proveedor, este a su vez da soporte y asistencia en caso de fallas o de mejoras.	-Área de sistemas. -Área pertinente. -Empresa contratista del software o proveedor	-Contrato.	x

Mantenimiento de equipos de cómputo

No	Descripción de la actividad	RESPONSABLE	REGISTRO	PUNTOS DE CONTROL
1	PROGRAMACIÓN DE MANTENIMIENTO: El asesor de Informática realiza el cronograma de mantenimiento preventivo de los equipos de cómputo.	-Asesor de informática	-Cronograma del mantenimiento preventivo de computadores de la sede central del INCIVA	x
2	COORDINACIÓN DE FECHAS DE MANTENIMIENTO: El Asesor de informática por medio del correo institucional informa y envía el cronograma y el Plan de mantenimiento preventivo a los usuarios de la entidad que son encargados de sus respectivos equipos de computo	-Asesor de informática -Usuario encargado de equipo de cómputo de áreas pertinentes.	-Correo informativo -Cronograma del mantenimiento preventivo de computadores de la sede central del INCIVA -Plan de mantenimiento de computadores de la sede central el INCIVA	x
3	EJECUCION DEL MANTENIMIENTO: -El auxiliar de sistemas siguiendo el cronograma, solicita el equipo de cómputo al usuario encargado del equipo del área pertinente. -lleva el equipo al área de sistemas donde	-Auxiliar de sistemas -Usuario encargado de equipo de cómputo de áreas pertinentes.	-FO-PINF-01 Hoja de vida de equipos	x

	verifica que lo reportado en la hoja de vida sea correcto y toma la información (seriales de periféricos y unidades internas, etc.) para posteriormente actualizar la hoja de vida si es necesario. -posteriormente el equipo es desensamblado y se realiza mantenimiento de hardware completo como está estipulado en el Plan de mantenimiento. -acto seguido el equipo es ensamblado y se traslada al área del usuario encargado, donde se realiza mantenimiento preventivo y actualización de software -el equipo se le entrega al usuario encargado, se le muestra la hoja de vida actualizada para que este la revise junto con la ficha del informe del mantenimiento. Esta es firmada por el usuario encargado.			

Backup de información de los funcionarios de la entidad.

No	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO	PUNTOS DE CONTROL
1	INDUCCIÓN Y CONFIGURACION DE BACKUP EN LA NUBE: -El área de sistemas se encarga de dar la inducción de: la realización de copia de seguridad en la nube a los usuarios de la entidad por medio de sus respectivas cuentas de correo institucional en la plataforma de GOOGLE. por medio de GOOGLE DRIVE. Donde cada usuario posee 30GB de almacenamiento para uso exclusivo de copias de seguridad e información institucional. -los usuarios deben firmar la respectiva asistencia a la inducción. -después de la realización del mantenimiento de los equipos de cómputo, a los usuarios se les realiza reinducción para la realización de copia de seguridad en la nube.	-Área de sistemas -funcionarios de la entidad	-asistencia de inducción o reinducción	x
2	REALIZACION Y DEL BACKUP: -El asesor de informática envía recordatorios e la	-Asesor de informática -funcionarios de la entidad	-correos informativos -registro de backup en la plataforma	

	realización del backup en la nube a los funcionarios por medio del correo institucional a menos 2 veces al mes. -los funcionarios de la entidad deberán realizar copias de seguridad de su información institucional en la nube por medio de la plataforma de GOOGLE DRIVE del correo institucional al menos una vez al mes.		GOOGLE DRIVE	

Seguimiento y verificación del almacenamiento y backup de la información de los funcionarios

no	DESCRIPCION DE LA ACTIVIDAD	RESPONSABLE	REGISTRO	PUNTOS DE CONTROL
1	VERIFICACION DEL BACKUP – AUXILIAR DE SISTEMAS: -El área de sistemas efectúa una revisión mensual de la información almacenada por los funcionarios de la entidad en las cuentas institucionales de GOOGLE DRIVE una a una, donde por medio del formato FO–PINF-04 “REGISTRO DE CONTROL DEL BACKUP O COPIA DE SEGURIDAD” registra las fechas de la realización del backup.	-Área de sistemas -funcionarios de la entidad	-Formato FO–PINF-04 “REGISTRO DE CONTROL DEL BACKUP O COPIA DE SEGURIDAD”	x

	Y toma las firmas de los respectivos funcionarios al final de la revisión.			
2	SOLICITUD POR PARTE DEL AREA DE SISTEMAS. -Si el funcionario hace caso omiso al correo recordatorio del backup o a la revisión mensual, se le informará al Asesor de sistemas para que reitere la solicitud.	-Área de sistemas	-correos informativos -Formato FO–PINF-04 “REGISTRO DE CONTROL DEL BACKUP O COPIA DE SEGURIDAD”	x

Backup de los sistemas de información

no	DESCRIPCION DE LA ACTIVIDAD	RESPONSABLE	REGISTRO	PUNTOS DE CONTROL
1	BACKUP SISTEMA DE INFORMACIÓN-FIRSTSOFT: -El backup es realizado por el software Syncbackup Free v.8.2 configurado en el equipo de sistemas. -el backup es realizado dos veces al día, a las 1:00pm y a las 7:00pm Esto con el fin de respaldar los datos ingresados por los usuarios después de que terminan labores al medio día y al final el día respectivamente. El backup es realizado atreves de la red de	-Asesor de Sistemas -Auxiliar De sistemas	-registro de copia de seguridad	

	domino, y respaldado en disco duro externo.			
2	REALIZACION DEL BACKUP DE SERVIDOR ES: -El servidor de dominio realiza una copia de seguridad del sistema operativo renovada diariamente, configurado en el mismo sistema operativo. -el back up del servidor de Gestión documental es hecho por la empresa contratada.	-Asesor de sistemas -Auxiliar de sistemas -Empresa contratista	-registro de copia de seguridad	
3	VERIFICACIÓN DEL BACKUP: El backup de FIRSTSOFT es enviado semanalmente a la empresa de soporte contratada, para mantenimiento y actualizaciones, donde el backup es verificado.	-Asesor de sistemas -Auxiliar de sistemas -Empresa contratista	-registro de copia de seguridad	

Solicitudes de soporte y resoluciones en general.

No	DESCRIPCION DEL ACTIVIDAD	RESPONSABLE	REGISTRO	PUNTOS DE CONTROL
1	INDUCCION DEL USO DE LA MESA DE SERVICIOS: -El personal del área de sistemas realiza inducción a cada uno de los funcionarios vinculados al servidor de dominio, donde se les explica el modo de acceso a la mesa de servicios por medio del link: https\\: helpdesk.inciva.gov.co:81. -también se les explica el modo de hacer una solicitud por medio de un ticket	-Área de sistemas -funcionarios de la entidad		
2	SOLICITUDES DE SOPORTE: El funcionario: que desee ayuda o soporte debe ingresar al link de la mesa de servicios y diligenciar el formulario para envió del ticket. -TIPO: se indica el tipo de solicitud entre: INCIDENCIA O REQUERIMIENTO -CATEGORIA: se indica la categoría deseada entre: Instalación configuración de hardware o software. -USUARIO EN SEGUIMIENTO: usuario que manda la solicitud -CORREO ELETRONICO: correo electrónico institucional del solicitante. -URGENCIA: se indica la urgencia de la	Área de sistemas	-Ticket de la mesa de servicios	

	solicitud: muy alta, alta, baja o muy baja. -TITULO: se indica el tema a tratar en la solicitud -DESCRIPCION: se da una corta explicación de la solicitud. -ADJUNTAR: se sube información referente a la solicitud, máximo 120mb Por último, de le da al botón de ENVIAR. El asesor de informática recibe el ticket en su interfaz de administración de la mesa de servicios.			
3	RESOLUCION DE LAS SOLICITUDES: -Una vez el asesor de informática recibe el ticket, procede a darle solución a la solicitud o a informar al auxiliar de sistemas. -cuando el funcionario da por solucionada la solicitud, se cierra el ticket y se marca como “resuelto”	-Área de sistemas -funcionarios de la entidad	-Ticket de la mesa de servicios	

Infraestructura

Entre los componentes de la infraestructura se cuentan con:

-Servidores y equipos: Actualmente la entidad cuenta con 2 servidores de diferentes marcas (IBM y DELL) funcionando, de los cuales ninguno cuenta con garantía.

Descripción	Marca	Memoria RAM	Disco Duro	Tarjeta de video	Fecha	Garantía	Condición	Número de Equipos
Powers Edge T130 INTEL XEON	DELL	2 módulos DE 4 GBS, 8GB en total	2 TERA	1 GIGA	DESDE 2017	No tiene garantía	En buen estado y funcionando	22
SYSTEM X3400 M3 INTEL XEON	IBM	2 módulos DE 4 GBS, 8GB en total	500 GIGAS Y 300 GIGAS	N/A	DESDE 2011	No tiene garantía	En buen estado y funcionando	22

Periféricos:

Periférico	Número
Impresoras	4
Multifuncionales	2
scanner	3

Seguridad

Dominio Y Directorio activo:

El directorio activo de la entidad está configurado en el servidor de Dominio el cual funciona en Windows server 2016, adicionalmente posee servicios de DNS, DHCP (virtual y físico).

La Red de la entidad tiene alrededor de 150 usuarios indiferente del tipo de vinculación. Y 22 usuarios vinculados al servidor de Dominio.

Navegación segura y sana:

El servidor de dominio navega bajo un DNS con filtro donde restringe el acceso a las siguientes categorías de páginas web:

-Películas
-televisión
-Radio stream
-proxy/navegación anónima
-desnudos
-sexualidad
-pornografía

El objetivo de estas restricciones es asegurar la disponibilidad y productividad de la red, evitando el cuello de botella y otros inconvenientes que pueden ocasionar el uso de las paginas restringidas.

Firewalls y seguridad perimetral:

Se tiene un antivirus con firewall en alta disponibilidad como esquema de seguridad perimetral. Para seguridad de acceso remoto se cuenta con accesos VPN para opciones de revisión y soporte y gestión de ancho de banda.

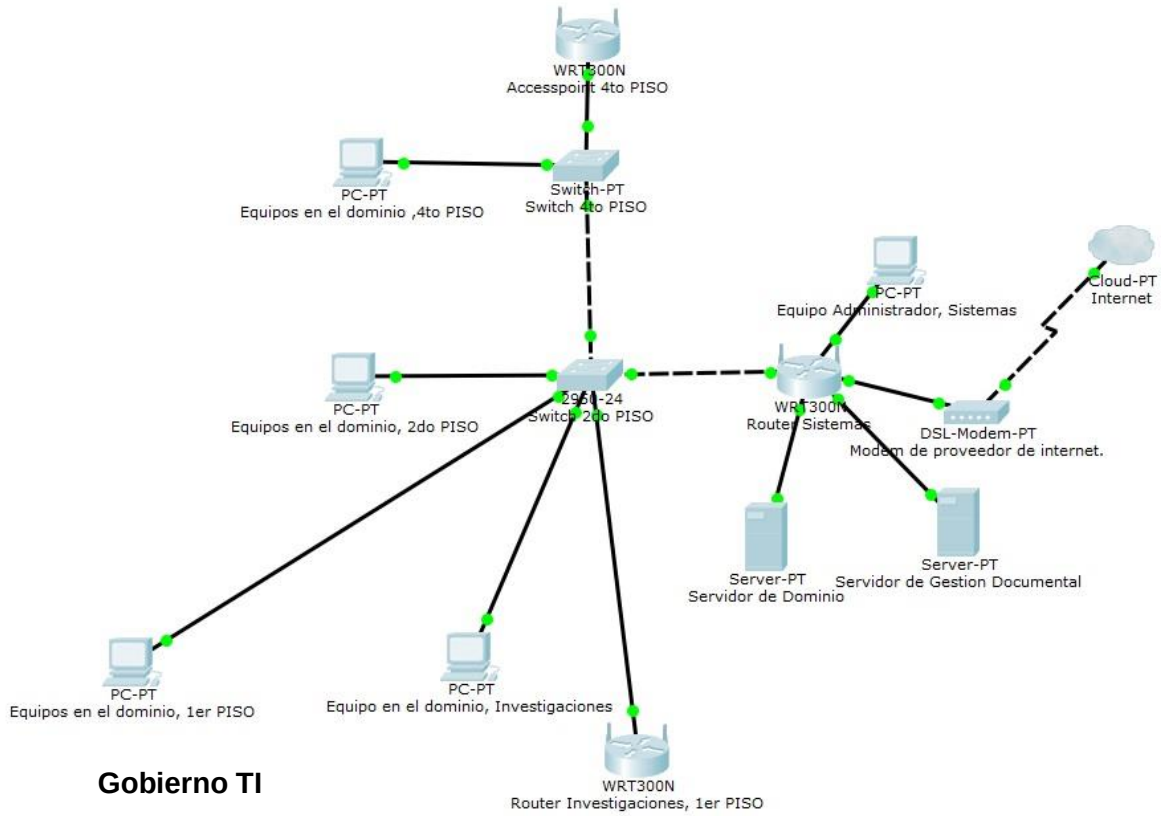
Para el control de antivirus se tiene licencias para todas las estaciones de trabajo del antivirus, ESET NOD, que es controlado y actualizado desde cada equipo de manera automática y desde la estación central del servidor de dominio.

Respecto a los esquemas de back up se cuenta con el procedimiento anteriormente mencionado en servicios tecnológicos.

Redes

Clase de usuarios	Número de Usuarios	Conectividad	Internet
Administración Inciva, sede central	21	Alámbrica/vinculados al dominio	CORREO E INTERNET BANDA ANCHA 20MB
Laptops usuarios de Inciva, sede central	3	WIFI/vinculados al dominio	
Laptops personales, teléfonos de usuarios de Inciva y de contratistas.	Alrededor de 175	WIFI	

Mapa de redes



Organigrama INCIVA.

Actualmente La entidad no ha establecido una estructura organizacional de gobierno TI de acuerdo a los lineamientos del dominio propuesto por el ministerio de tecnologías de la información y las comunicaciones (MinTic)., a continuación, se enlistarán los cargos del área de sistemas perteneciente a los Órganos de asesoría y coordinación del INCIVA y se describirá de manera resumida la estructura funcional que forma el área.

Cargo	Profesión
Asesor de informática	Ingeniero de sistemas
Auxiliar de sistemas	Ingeniero de sistemas, contratista

Se distribuyen las siguientes funciones en el Asesor de Informática y el Auxiliar de sistemas:

Asesor de Informática: Lidera la definición de las políticas de seguridad de la institución, estrategias, sistemas de información, las telecomunicaciones, seguridad informática y acciones relacionadas con las plataformas tecnológicas para garantizar la disponibilidad de los servicios tecnológicos de la entidad, mejorar la prestación del servicio y facilitar la toma de decisiones. También posee la experiencia técnica, y la flexibilidad de interactuar con una variedad de usuarios y actores de todos los niveles; internamente (funcionarios, directores, finanzas, etc.) y externamente (auditores, clientes, proveedores y asociaciones de profesionales). Además de coordinar el mantenimiento de infraestructura y Backup de la Información.

Auxiliar de sistemas: Se encarga de ejecutar el soporte, mantenimiento, actualización y crecimiento de la infraestructura de tecnología de información en lo que corresponde a la instalación de software, hardware, redes y seguridad informática. Además, recolecta información para la actualización del plan de contingencia de la entidad y hojas de vida de los equipos de cómputo y periféricos.

Análisis financiero

A continuación, se resumirá el manejo presupuestal con respecto al Área de sistemas con respecto a TI en la siguiente tabla:

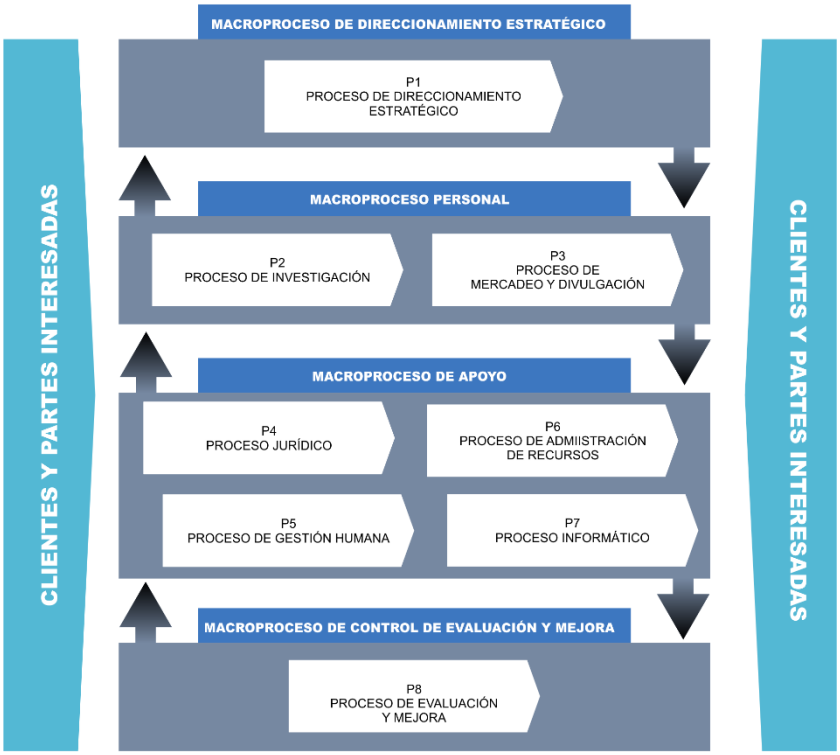
Bien, Obra o Servicio	Presupuesto
Contrato de soporte de software: FIRSTSOFT	$26.340.000
Contrato de software de Gestión Documental	$35.000.000
Servicio de internet ERT	$25.000.000
Servicio de correo, Drive en la nube y demás aplicaciones: GOOGLE APPS	$17.000.000
Actualización soporte Antivirus: ESET ENDPOINT	$1.616.000
Página WEB, hosting y dominio	$23.832.000
Suministros de computo	$50.000.000
Suministros de mantenimiento y demás elementos	$500.000

A este presupuesto se le hacen ajustes periódicamente de acuerdo a los requisitos y necesidades de los diferentes proyectos de la entidad.

ENTENDIMIENTO ESTRATÉGICO

Modelo operativo

-
- El Inciva tiene implementado un modelo de operación por procesos el cual permite una articulación entre dependencias, Actualmente contempla 8 procesos distribuidos en 4 macro procesos:



Mapa de procesos INCIVA

Como se mencionó en el análisis de la situación actual, no existe un área tecnológica como tal, sin embargo, los proyectos tecnológicos y uso de los sistemas de la información competen a todos los procesos de la institución.

Necesidades e la información

Actualmente la entidad no cuenta con un mapa de información definido para toda la entidad acorde con la Guía Técnica propuesta por Min Tic,

Imagen: *Pasos para desarrollar e implementar la gestión del ciclo de vida del dato.* Fuente*: MinTIC.*

A continuación, se presenta una caracterización de la información de la entidad donde actividades de tecnologías de la información se relacionan con los procesos que le compete actualmente.

Procesos Proveedores	Entradas	P / V	H / A	Actividades	Salidas	Procesos Clientes
Todos los procesos	Directrices, Normatividad, Actualización Tecnológica	P		Determinar los lineamientos en materia de TIC para la entidad	Plan Estratégico Tecnología de la información	Todos los procesos
Todos los procesos	Necesidad de adquisición de bienes y servicios	P		Identificar los recursos necesarios para el sostenimiento de la infraestructura tecnológica de la entidad	Estudios previos, Necesidades de contratación	P1 P4 P7
P7	Inventario de equipos con necesidades de mantenimiento y backup	V		Elaborar programa de mantenimiento de equipos y backup	Programación de mantenimiento y backup	Todos los procesos

P5 P7	Necesidades de capacitación en sistemas de información	H	Capacitar en el manejo de sistemas de información de acuerdo a las necesidades de las diferentes áreas.	capacitaciones	Todos los procesos
P1	Aprobación de estudios previos y necesidades de contratación	P	Gestionar los procesos de contratación para el mantenimiento e innovación de la infraestructura tecnológica de la entidad	Contrato Estudios previos	P1 P4 P7
P7	Programación de manteamiento y backup	V	Ejecutar el Programa de mantenimiento de equipos de cómputo y realización de Backup	Mantenimiento de equipos de cómputo y realización de backup	Todos los procesos
P1 P7	Análisis de procesos	V	Evaluar y analizar indicadores de gestión	Informes de gestión, cumplimiento de planes de acción y programas	P1 P7 P8
P1 P7	Análisis de procesos	V	Realizar seguimiento a los planes de acción y programas establecidos	Informes de gestión, cumplimiento de planes de acción y programas	P1 P7 P8
P1 P7	Análisis de procesos	H	Implementar acciones para el mejoramiento del proceso.	Planes de mejoramiento	P1 P7 P8

Alineación de TI con los procesos

SISTEMAS DE INFORMACIÓN	PROCESOS							
	Direccionamiento Estratégico	Personal		Apoyo				Control de Evaluación y Mejora
	P1. Direccionamiento estratégico	P2. Investigación	P3. Mercadeo y Divulgación	P4. Jurídico	P5. Gestión Humana	P6. Administración de Recursos	P7. Informático	P8. Evaluación y Mejora
Correo y Cloud Drive	X	X	X	X	X	X	X	X
Sis. Admin. Financiero					X	X		
Gestión Documental	X	X	X	X	X	X	X	X
Mesa de servicios	X	X	X	X	X	X	X	X
Página WEB	X		X				X	X

MODELO DE GESTIÓN DE TI PROPUESTO

Estrategia de TI

SI bien en el organigrama del INCIVA, TI no es un área con estructura definida, en el mapa de procesos tampoco se define un proceso Tecnológico como tal, por lo tanto, para un mayor apoyo al llevar acabo las iniciativas de TI se debe optar por formar un área enteramente de TI, estar encabezado por un CIO o Jefe de oficina TIC que sea el segundo en orden del comité de Gobierno Digital, que tenga asiento en el Institucional de Evaluación y Gestión. Permitiendo tener voz y voto en las decisiones que al área de TI competen, además cada área de la entidad debe estar representada por amenos un funcionario en el comité de Gobierno Digital. A partir de ello se propone innovar el proceso de informática actual a un proceso de estratégica de TI donde se debe implementar del marco de referencia de Arquitectura Empresarial propuestos por MinTIC los 6 dominios, realizando ajustes periódicos tanto del PETI, como de los avances en la Arquitectura Empresarial, realizando una medición constante en dicho proceso

Es de notar que en el análisis del estado de madurez se refleja la baja calificación en la Estrategia de TI debido a una ausencia o falta de la misma, es entonces que se hace necesario a partir de este documento plantear los objetivos y las actividades que lleven a la consecución de las metas de tecnología como área fundamental en la Institución, donde se estandaricen

procesos y se generen propuestas de mejoramiento.

Objetivos estratégicos de TI

- Definir el marco de trabajo del gobierno de TI

- Adoptar un marco de trabajo en gobierno, tomando elementos de las diferentes prácticas y teniendo como resultado un proceso de gestión de TI bien definido.
  - Entregable: Documento guía para la toma de decisiones de TI, donde se incluyan elementos de planificación y organización, adquisición, soporte, seguimiento, evaluación y mejora, además que se especifique el rol que tiene el área de información y tecnología en los diferentes proyectos que involucren TI definiendo los respectivos indicadores de desempeño.
- Definir los roles del personal de TI de acuerdo con su perfil profesional y capacidades técnicas, planeación, innovación y mejora el proceso de TI
  - Entregable: Definición de roles para el documento guía de gobierno de TI
- Definir el mecanismo en que el responsable del área de información y tecnología va formar parte de los diferentes proyectos donde exista la necesidad de inversión de TI, obligaciones y actividades que debe realizar.
  - Entregable: Capítulo para el documento de gobierno, rol del área e información y Tecnología en lis proyectos.
- Generar mecanismos que permitan hacer seguimiento a las capacidades de TI a nivel de recursos y talento humano con el fin de mejorar el soporte a los procesos de la entidad
  - Entregable: Encuesta e seguimiento y satisfacción de los procesos con respecto a TI.
- Definir el modelo de adquisición de tecnología con el fin de optimizar recursos, tomando decisiones basadas en la necesidad real de la compra y adopción de TI
  - Entregable: Manual guía para la adquisición de TI.
- Definir el mecanismo de evaluación costo beneficio de la adopción de TI, tomando en cuenta el apalancamiento que estas den a los diferentes procesos de la entidad y el entendimiento que en muchos casos no van a tener un retorno monetario.
  - Entregable: Recomendaciones para el Manual guía de adquisición de TI
- Definir los indicadores de seguimiento a la contratación y satisfacción, diferenciando entre los tipos de proveedores sea de servicio, plataforma, entre otros.

- Entregable: Capítulo de gestión de proveedores de TI para el documento de gobierno, en el que se plasme el esquema de seguimiento a la contratación de TI, indicadores de desempeño y de recibo de satisfacción.

- Definir el marco de trabajo para los sistemas de información y servicios tecnológicos.

- Adoptar un marco para la gestión de las TI, que tome elementos de las buenas prácticas generando como resultado un proceso bien definido.
  - Entregable: Documento donde se define el rol de los sistemas de información VS los procesos, el marco de trabajo de las etapas de implementación, soporte y mantenimiento de software y hardware, el ciclo de vida para cada uno de los sistemas y sus necesidades de actualización y/o mejora e innovación, indicadores de desempeño de los sistemas, acuerdos de servicio y operación, además de especificar los diferentes contratos de soporte.

- Definir el estándar de los sistemas con el fin de buscar la integración de estos con los demás existentes en la entidad
  - Entregable: Recomendaciones para el documento de adquisición done se defina software libre, desarrollo o de propietario, al momento de decidir la implementación de un nuevo sistema (para el tema de inversión), de igual forma para el documento de gobierno apartado que oriente la toma de decisiones entre los tipos de sistemas; capitulo para el documento de sistemas de información donde se listen los estándares de usabilidad, diseño y requisitos de infraestructura, plataformas, seguridad, privacidad y trazabilidad que deben tener los aplicativos.
- Determinar los requisitos en lo que a servicios tecnológicos se refiere de cada uno de los procesos con el fin de generar un directorio de estos para identificar las necesidades de implementar nuevos servicios
  - Entregable: Directorio de servicios con los componentes tecnológicos necesarios para la operación de dichos servicios.
- Definir los indicadores de desempeño de los servicios de TI de acuerdo a lo que la entidad requiere
  - Entregable: Definición de los indicadores de TI.
- Definir las estrategias y planes de mejoramiento de los servicios y sistemas de TI
  - Entregable: Planes de mejoramiento.
- Definir el plan de capacitaciones de TI

- Analizar los indicadores de desempeño de los servicios y sistemas con el fin de determinar las necesidades de capacitación del personal basado en el tipo de incidentes reportados, periodicidad y recurrencia de los mismos
  - Entregable: Plan periódico de capacitaciones.
- Determinar las necesidades para las capacitaciones e los diferentes sistemas y servicios de la entidad
  - Entregable: Parámetros técnicos y de conocimiento para el plan de capacitaciones.

- Definir los lineamientos para un correcto uso de las TI
- Definir la caracterización de los usuarios de las TI, perfil y conocimiento con el fin de determinar el impacto que tendría la implementación de nuevos servicios, plataformas, entre otros
  - Entregable: Necesidades de capacitación y conocimientos previos a la implementación de un sistema (plan de capacitaciones), caracterización de usuarios.
- Definir los incentivos para promover el uso y apropiación de las TIC
  - Entregable: Esquema de incentivos
- Definir los indicadores del uso de las TI que permitan medir la adopción y satisfacción de las tecnologías
  - Entregable: Indicadores de uso y apropiación de los TI.
- Definir los lineamientos para administrar los impactos resultado de la adopción de TI
  - Entregable. Plan para la medición y administración de impactos.
- Diseñar acciones de mejora de resultado del uso y adopción de nuevas tecnologías
  - Entregable: Planes de mejoramiento.

- Generar iniciativas de fortalecimiento a los procesos que tiene poco apoyo de los sistemas de información.
- Definir los procesos que tienen poca participación de sistemas de información mediante el análisis de la tabla de alineación e TI con los procesos
  - Entregable: Propuestas de mejora de los procesos en los que se define la motivación de la propuesta, tipo de sistemas o infraestructura, estudio de mercado, presupuesto, tiempos de implementación, usuarios afectados, mejora esperada.

- Documentar las normas del gobierno nacional y territorial a las cuales se debe dar cumplimiento en relación a TI.

- Definir las normas que aplican a la entidad y documentar las acciones y requerimientos que se deben presentar para su cumplimiento
  - Entregable: Marco normativo de TI.
- Definir los proyectos de TI necesarios para dar cumplimiento a la norma
- Apoyar en la generación de un plan de comunicaciones para el conocimiento y apropiación del PETI

- Alineación de la estrategia de TI con la estrategia de la institución pública.

La entidad debe definir a TI como un proceso estratégico, también se debe empezar a desarrollar proyectos desde un área enteramente dedicada a TI en busca de mejorar y apalancar la gestión de los procesos de la entidad.
Las Propuestas de nuevos desarrollos: Disposición de residuos tecnológicos, toma de decisiones basadas en evidencias, transformando servicios digitales y sociedad participativa, hacen parte de algunas iniciativas propuestas en gobierno digital que se debe adoptar a los procesos de la entidad.

- Disposición de residuos tecnológicos:

Objetivo: Generar capacidades para impulsar un programa que promueva la correcta disposición final de los residuos tecnológicos en las entidades públicas.

- Toma de decisiones basadas en evidencia

Objetivo: Generar capacidades para gestionar información a partir preguntas analíticas y selección de fuentes que permitan extraer datos, transformarlos, visualizarlos y facilitar procesos de toma de decisiones.

- Transformando mis servicios digitales

Objetivo: Generar capacidades para mejorar la accesibilidad y usabilidad de los servicios digitales

- Sociedad participativa

Objetivo: Generar capacidades para el desarrollo de ejercicios de participación ciudadana que promuevan el empoderamiento ciudadano.

FASE 2 DEL PETI

CUMPLIMIENTO DE OBJETIVOS ESTRATÈGICOS DE TI.

Marco de trabajo de gobierno y gestión de ti para garantizar la continuidad del negocio.

Introducción

Las instituciones deben garantizar la calidad de los servicios que prestan a la ciudadanía y a través de la gestión de la continuidad se identifican los impactos potenciales que amenazan la continuidad de las actividades que apoyan la gestión de las instituciones gubernamentales. El diseño de un marco de gobierno de TI les da la capacidad a estas entidades de responder de forma efectiva a disrupciones, con base a herramientas de seguimiento y control, y es un referente para el cumplimiento de los objetivos de la administración pública mediante la preparación de las áreas de tecnología para la continuidad, elevando los niveles de competitividad y ofreciendo disponibilidad de los servicios a los ciudadanos.

El modelo propuesto puede ser tomado como modelo de referencia para la oficina de informática de la institución, aplicado a procesos del INCIVA, para proteger los intereses de la entidad y para dar cumplimiento a las actividades definidas por el Gobierno Nacional, a través de la guía de continuidad del negocio del Modelo de Seguridad y Privacidad de la Información, como parte integral de la estrategia Gobierno Digital, liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. Este componente estratégico es de obligatorio cumplimiento para entidades territoriales y nacionales, con implementaciones progresivas, con el fin de fortalecer la seguridad de la información pública y garantizar el restablecimiento y recuperación de las operaciones y

actividades esenciales.

La correcta implementación de un gobierno y una gestión que incluya la gestión de la continuidad del negocio es un reto para las Entidades Gubernamentales y resulta necesaria para disminuir la posibilidad de ocurrencia de incidentes y, en caso de producirse, estar preparada para responder en forma adecuada y oportuna.

Descripción del problema

La necesidad de reconocer la seguridad y privacidad de la información en las entidades territoriales y demás organizaciones en general, como un factor primordial para la apropiación de las TIC, hace que el Gobierno Nacional plantee un modelo de seguridad y privacidad de la información el cual debe ser respaldado por una gestión. Dicha gestión debe involucrar la implementación de un proceso de preservación de la información pública ante situaciones disruptivas para minimizar el impacto y recuperación por perdida de activos de información mediante la combinación de controles preventivos y de recuperación.

La oficina de Informática de INCIVA es responsable de salvaguardar la información digital de la entidad, también es consciente de que existen diferentes tipos de amenaza, cuyo origen puede ser natural, accidental o intencionado y puede repercutir en la operación tributaria y en el sistema de procesamiento de la información, impactando la continuidad, la imagen del gobierno local, en aspectos financieros y legales, y en las personas, como entidad y contribuyente, lo que crea la necesidad de recuperación en el menor tiempo posible, garantizando la continuidad de los servicios de TI. Consciente de esto nace la necesidad de formalizar la administración de tecnología, teniendo como base modelos de gobierno

de TI que permitan su adaptación de manera natural a las particularidades propias de las entidades públicas.

Objetivo general

Diseñar un modelo de gobierno y gestión de TI que garantice la continuidad de los servicios que soportan los procesos entidad, basándose en buenas prácticas internacionales ajustada a la infraestructura local.

Objetivos específicos

- Identificar los procesos de gobierno TI para soportar procesos de gestión de la continuidad de procesos en la institución, basada en estudios de mejores prácticas internacionales y guías nacionales.
- Proponer el marco de gobierno de TI para la gestión de la continuidad de procesos de la entidad.
- Diseñar el plan de implementación y despliegue para el caso de estudio de la entidad.

METODOLOGÍA

El diseño del modelo de gobierno y gestión de TI para garantizar la continuidad de los servicios en las entidades públicas está compuesto por las siguientes fases:

Objetivo Específico	Fase	Descripción
Identificar los procesos de gobierno TI para soportar procesos de gestión de la continuidad de procesos en la institución, basada en estudios de mejores prácticas internacionales y guías nacionales.	1. Revisión y análisis de conceptos de Gobierno y Gestión.	▪ Revisión de conceptos de Gobierno y Gestión. ▪ Estudio de marcos y mejores prácticas de Gobierno y Gestión: *Revisión de marcos y estándares existentes de Gobierno y Gestión y modelo de Gobierno y Gestión de TI del Ministerio de las Tecnologías de la Información y las Comunicaciones. Durante esta fase se realizan revisiones de marcos de trabajo de Cobit5, ITIL V3 y la Guía No.10 Preparación de las TIC para la Continuidad del negocio – MinTIC.* ▪ Revisión de guías y casos de éxito del gobierno y gestión de la continuidad del negocio.
	2. Revisión de componentes de Gestión de la Continuidad.	▪ Revisión de componentes asociados a la gestión de la continuidad en entidades territoriales.

Proponer el marco de gobierno de TI para la gestión de la continuidad de procesos de la entidad.	3. Diseño del modelo de gobierno y gestión de TI	▪ *Modelo de gobierno y gestión de TI para garantizar la continuidad de los servicios de los procesos de las entidades públicas.* En esta fase se plantea el modelo de gobierno y gestión de TI con base a mapeos de procesos y metodologías revisadas en la fase anterior. Contiene por proceso, las prácticas, las actividades con las entradas y salidas, las métricas y los indicadores.
		Aplicación de una metodología para realizar el análisis de impacto del negocio de los riesgos en procesos críticos. El desarrollo de la metodología estará soportado por un documento guía de escenarios donde se definirán categorías de impacto de acuerdo al proceso crítico elegido.

Diseñar el plan de implementación y despliegue para el caso de estudio de la entidad.	4. Elaboración de la guía de implementación del modelo propuesto.	Elaboración del plan de implementación del modelo propuesto. *En esta fase final se lleva a cabo el plan de implementación del modelo.*

Marco teórico

Gobierno Corporativo y Gobierno de TI

Hitt, Ireland y Hoskisson definieron la estrategia como un conjunto de compromisos que indican lo que se pretende hacer y lo que no, de forma que se aproveche al máximo las competencias y se obtenga una ventaja competitiva. Determinar y controlar el direccionamiento de la estrategia, al igual que gestionar el desempeño y las relaciones de las partes interesadas es como se define el gobierno corporativo. Los aspectos claves en las que se centra el Gobierno Corporativo incluyen principalmente: Funciones de la Junta Directiva y Ejecutivos, Cumplimiento normativo, Derechos de los accionistas, Operación y Control del negocio, Contabilidad Financiera y Reportes, Gestión de riesgos.

Así, gobierno de TI resulta ser una parte integral del gobierno corporativo y se refiere a alinear la estrategia de TI con la estrategia corporativa.

Gobierno de TI se define como una integración de la gestión, la planificación de políticas y prácticas y un proceso de revisión de

desempeño, que permite alinear las inversiones y prioridades del negocio, mantiene una utilización responsable de recursos y activos, establece y aclara la responsabilidad y la toma de decisión, mejora el rendimiento de las organizaciones y defiende la innovación. Su alcance abarca temas como: Principios de TI, arquitectura de TI, arquitectura orientada al Servicios (SOA), Infraestructura de TI, las necesidades de la aplicación del negocio, las inversiones de TI y su priorización, el desarrollo del talento humano y las políticas, procesos, mecanismos, herramientas y métricas.

Se debe reconocer la diferencia existente entre el Gobierno Corporativo, el Gobierno empresarial o del negocio y el Gobierno de TI:

Gobierno Corporativo	Gobierno Empresarial	Gobierno de TI
Separación de propiedad y control	Dirección y Control del Negocio.	Dirección y Control de TI.

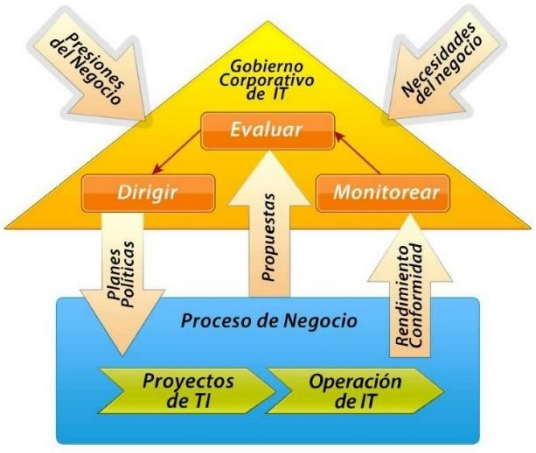
Funciones del Directorio y Ejecutivos. Cumplimiento normativo. Derechos de los Accionistas. Operaciones y Control de Negocios. Contabilidad financiera e Informes. Gestión de riesgos.	Estrategia de negocios, Planes y Objetivos. Procesos y actividades empresariales. Innovación e Investigación. Capital intelectual. Gestión de recursos humanos. Métricas de rendimiento y Controles. Gestión de activos.	Estrategia de TI, Planes y Objetivos. Alineación con Planes de Negocios y Objetivos Recursos y recursos de TI. Gestión de la demanda. Entrega y Ejecución de Valor. Gestión (PM y ITSMD) Riesgo, Cambio y Rendimiento Administración.

Tomado de “Implementing IT Gobernance (2008) Dr. Gad J Selig PMP COP. Varen Harén Publising.

De acuerdo a la ilustración, se puede observar que el Gobierno de TI es tarea de todos, la Junta Directiva y el CEO de la organización toman un lugar importante en cuanto al liderazgo, la estructura organizativa y los procesos que aseguren que la función de TI esté alineada con las metas corporativas. Además, son los directivos los que toman decisiones en materia de inversiones y tienen la visión empresarial revisando y aprobando los planes estratégicos, programas y proyectos importantes que generan valor a la organización. El CIO además de aumentar la eficiencia y reducir costos, utilizan la TI como un estímulo principal para la innovación empresarial.

Gobierno y gestión de TI

Es necesario hacer una distinción de lo que es gobierno y gestión. Gobierno Corporativo de TI es el sistema por el cual se dirige y supervisa el estado actual y futuro del uso de TI (ISO/IEC 38500). El modelo de gobierno de TI presentado en ISO/IEC 38500 se enfoca en tres tareas claves de gobierno – evaluar, dirigir, controlar, como la clave para dar dirección y controlar el desempeñó de los roles de gestión en la conducción de la organización para la planificación, implementación y utilización operacional de TI. Por su parte, gestión se define como el sistema de controles y procesos para lograr los objetivos estratégicos establecidos por la dirección de la organización y está sujeta a monitorización establecida mediante el gobierno corporativo. Para tener una imagen visual de los conceptos, el modelo de gobierno de TI según la norma, lo representa claramente:



Modelo de Gobierno IT Tomado de ISO/IEC 38500

Los componentes principales del Gobierno de TI son:

- Estrategia, Plan y Objetivos Corporativos
- Estrategia, Plan y Objetivos de TI
- Plan de Ejecución
- Gestión del Rendimiento y Controles de Gestión
- Gestión de Proveedores y Gestión de outsourcing
- Desarrollo de Talento Humano, Mejora Continua y Aprendizaje.

Áreas de Trabajo	Descripción de componentes
Plan de negocios/	Plan de Negocios Estratégico - Visión, Objetivos, Finanzas, Operaciones, DOFA. • Planificación de Capital / Planificación de Gastos y Presupuesto • Gestión del Desempeño Empresarial (Key Metrics) • Conseio Eiecutivo v Otros Conseios Directivos v de
Plan de TI, Objetivos, Portafolio de inversiones Y aprobaciones **administración Y alineamiento)**	El Plan de TI está alineado con el Plan de Negocios - IT Capital / Expense Presupuesto • Inversión en cartera de TI, racionalización, selección, Priorización, financiación y **(Demanda** aprobación (Gestión de la cartera Modelo (para Nuevos Programas de Cambio y Proyectos y / o Iniciativas Operacionales y Funciones de Infraestructura) • Financiar iniciativas importantes • Gestión del rendimiento de TI (Definir métricas y Criterios de medición)
Ejecución de Planes de TI & Entrega (Recurso & Ejecución Administración)	• Planes de Programas, Proyectos y Operativos (Planes de Capital, Planes y Presupuestos) • Políticas, Estándares, Directrices y Procesos (por ejemplo, Control de Gestión, Arquitectura Empresarial, Seguridad, PMO, ITIL, Arquitectura Empresarial, etc.) • Procesos (PMO, Help Desk, Seguridad, SOPs Administrativos, Flujos de Trabajo, Cambio, Riesgo, etc.) • Financiación, programa, proyecto, aplicación, mantenimiento y Responsabilidad operacional
Actuación, Administración, Controles, Riesgo, Cumplimiento y proveedor Gestión (Ejecución Administración)	• Gestionar y medir planes, programas presupuestarios, proyectos, Operaciones y riesgos • Definir y rastrear indicadores clave de rendimiento (KPI) • Comparar los planes con los reales y tomar las medidas correctivas comportamiento • Outsourcing y Selección de Proveedores, Seguimiento, Medición • Continuidad de Negocios y TI, Seguridad, Contingencia y Desastre Recuperación
Gente Desarrollo, Continuo Proceso Mejoras & Aprendizaje	• Desarrollo del capital humano • Modelos de madurez organizacional, de proyectos y de operaciones Estándares • Gestión del cambio y la transformación (por ejemplo, cultura, Interoperabilidad) • Capacitación y certificación (por ejemplo, Organización)

Framework integrado de Gobierno de Ti. Tomado de “Implementing IT Gobernance 2008) Dr. Gad J Selig PMP COP. Varen Haren Publising [3]

El alcance del Gobierno de TI comprende:

a. Principios de TI
b. Arquitectura de TI
c. Arquitectura orientada al Servicios (SOA)
d. Infraestructura de TI
e. Necesidades de aplicación del negocio
f. Inversiones de TI y su priorización
g. Desarrollo del talento humano
h. Políticas, procesos, mecanismos, herramientas y métricas.

Se plantea que el éxito de la implementación se basa en pilares fundamentales: Liderazgo, organización y toma de decisiones, y que los procesos sean flexibles y escalables y tenga una tecnología innovadora. Si alguno de los pilares anteriores falla o es ineficaz, la iniciativa del Gobierno de TI no será eficaz ni sostenible y puede atraer múltiples problemas que pueden desencadenar hasta el fin de una organización por pérdidas irrecuperables.

Asimismo, la aplicación de unas buenas prácticas sobre el Gobierno de TI obtendrá, además de los objetivos anteriormente expuestos, una serie de beneficios para la organización entre los que se puede destacar:

- La conformidad con los estándares de seguridad, de privacidad, de prácticas comerciales, de regulación medioambiental, y de responsabilidad social.
- Garantizar los derechos de propiedad intelectual, incluyendo acuerdos de licencia de software.

- Apropiada implementación y operación de los activos de TI.
- Clarificación de las responsabilidades y rendición de cuentas en lograr los objetivos de la organización.
- Continuidad y sostenibilidad del negocio.
- Asignación eficiente de los recursos.
- Innovación en servicios, mercados y negocios.
- Buenas prácticas en las relaciones con las partes interesadas (stakeholders).
- Reducción de costes.
- Materialización efectiva de los beneficios esperados de cada inversión en TI.

Toma de decisiones.

Los roles indispensables en un modelo efectivo de Gobierno de TI son el director ejecutivo, Chief Executive Officer – CEO, y el director de tecnologías de la información, Chief Information Officer – CIO.

El CEO es el responsable de hacer realidad el Gobierno de TI, es el encargado del establecimiento del direccionamiento estratégico, políticas, estructura global, presupuesto e inversión; el CEO debe conseguir que toda la organización comprenda y esté alineada con la visión estratégica, manteniendo siempre una buena comunicación interna.

El papel del CEO y el equipo de gestión ejecutiva requieren un equilibrio entre mantener el crecimiento y la rentabilidad mientras se optimiza la efectividad de la organización, además de cumplir con los requisitos regulatorios.

Ejecutar iniciativas estratégicas para toda la empresa y administrar operaciones comerciales efectivas es un negocio complejo que requiere

un gobierno corporativo y de TI efectivo para que el CEO y el equipo ejecutivo implementan la estrategia de la organización.

El gobierno efectivo es un componente prominente para el crecimiento y la rentabilidad efectivos y los atributos que deben abordarse para cumplir estos objetivos respectivamente son:

Crecimiento (maximizar propuesta de valor)	Optimizar la efectividad y eficiencia
▪ Velocidad (reducir tiempo) al mercado. ▪ Minimizar los riesgos y la incertidumbre. ▪ Ejecución perfecta. ▪ Facilitación de mejores prácticas. ▪ Reducir costos. ▪ Reducir los gastos de capital. ▪ Reducir obstáculos. ▪ Reducir defectos. ▪ Aumentar la lealtad del cliente. ▪ Gobernabilidad e indicadores clave de rendimiento. ▪ Código ético.	▪ Aumentar la gestión / competencia / capacitación de los empleados. ▪ Implementar el cambio estratégico de una manera planificada, coordinada y controlada. ▪ Mejorar los resultados de los esfuerzos de implementación. ▪ Mejore la dinámica de creación de equipos y el comportamiento empresarial. ▪ Conformidad.

Tomado de “Implementing IT Gobernance (2008) Dr. Gad J Selig PMP COP. Varen Haren Publising

El Gobierno de TI es tarea de todos, la Junta Directiva y el CEO de la organización toman un lugar importante en cuanto al liderazgo, la estructura organizativa y los procesos que aseguren que la función de TI esté alineada con las metas corporativas. Además, son los directivos los que toman decisiones en materia de inversiones y tienen la visión empresarial revisando y aprobando los planes estratégicos, programas y proyectos importantes que generan valor a la organización. El CIO además de aumentar la eficiencia y reducir costos, utilizan la TI como un

estímulo principal para la innovación empresarial.

El CIO es el líder de Tecnologías de la información dentro de la organización, es el encargado de establecer la estrategia de TI, obtener presupuestos, gestionar proyectos de TI, y definir la gestión de TI.

El CIO debe abordar aspectos claves y estratégicos, que incluyen:

- Cultura interna de la unidad de TI.
- Innovación, exploración de formas de tecnología actual y evolución, aprovechamiento de tecnologías emergentes.
- Gestión de Riesgos de TI.
- Identificación, valoración y gestión de activos.
- Planeación e implementación Estratégica de las TI.
- Aseguramiento del funcionamiento de operaciones dentro de la unidad de TI.
- Automatización de procesos y calidad de servicios, contribuyendo a la eficiencia y eficacia de la organización.
- Cumplimiento normativo.
- Seguridad y Privacidad de la Información.

Marcos de referencia

Estándares y marcos de trabajo de gobierno y gestión de ti

Las organizaciones requieren adoptar buenas prácticas para las operaciones de TI, incluyendo la continuidad del negocio. La gestión de la continuidad del negocio puede ser diseñada a través marcos de referencia ampliamente utilizados que proporcionan

controles medibles. Para la propuesta de marco de gobierno de TI para llevar a cabo esa gestión, que sea compatible con los estándares y mejores prácticas de la industria, se consideran algunos marcos metodológicos internacionales y nacionales que ofrecen mayor probabilidad de garantizar un resultado exitoso, especialmente tras una interrupción no planificada de los servicios de TI.

Marco de referencia Arquitectura TI de Colombia - Ministerio de las Tecnologías y las Comunicaciones MinTIC.

Este Marco de Referencia es el principal instrumento para implementar la Arquitectura TI de Colombia y habilitar la Estrategia de Gobierno en línea, liderado por el Ministerio de las Tecnologías y las Comunicaciones. Se busca habilitar las estrategias de TIC para servicios, TIC para la gestión, TIC para el gobierno abierto y para la Seguridad y la privacidad [8]. Está dirigido a las instituciones del Estado, las empresas privadas, la academia y los ciudadanos en general.

Principios

✓ Excelencia del servicio al ciudadano: Propender por fortalecer la relación de los ciudadanos con el Estado.

✓ Inversión con buena relación Costo/beneficio: Busca propender porque las inversiones de TI tengan un retorno medido a partir del impacto de los proyectos.

✓ Racionalización: Para optimizar el uso de los recursos, teniendo en cuenta criterios de pertinencia y reutilización.

✓ Estandarización: Para brindar un modelo estandarizado para la

definición de los lineamientos, políticas y procedimientos de gestión de TI del Estado colombiano.

✓ Interoperabilidad: Para fortalecer los esquemas de Interoperabilidad que estandaricen y faciliten el intercambio de información entre entidades y sectores, manejo de fuentes únicas de información y la habilitación de servicios entre entidades y sectores.

✓ Viabilidad en el mercado: Busca motivar al mercado a plantear y diseñar soluciones según las necesidades del Estado colombiano.

✓ Neutralidad tecnológica: Busca garantizar la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, también busca garantizar la libre y leal competencia y que la adopción de tecnologías sea armónica con el desarrollo ambiental sostenible.

✓ Federación: Se debe definir y establecer, a través del Marco de Referencia de AE, estándares, lineamientos y guías para el gobierno y la gestión de TI.

✓ Co-creación: Permitir componer nuevas soluciones y servicios sobre lo ya construido y definido, con la participación de todas aquellas personas u organizaciones, que influyen o son afectadas por el Marco de Referencia AE.

✓ Escalabilidad: Permitir la evolución continua y adición de todos los componentes y dominios que integran el Marco de Referencia AE, sin perder calidad ni articulación.

✓ Seguridad de la información: Busca la definición, implementación y verificación de controles de seguridad de la información.

✓ Sostenibilidad: Aportar al equilibrio ecológico y cuidado del medio

ambiente a través de las TI.

El Marco de Referencia está organizado en seis dominios, donde cada dominio tiene ámbitos, que agrupan lineamientos, además de roles, una normatividad, indicadores e instrumentos para la adopción. Estos dominios son:

Dominios Arquitectura TI	Descripción
Estrategia TI	Apoyar el proceso de diseño, implementación y evolución de la Arquitectura TI en las instituciones, para de manera que esté alineada con las estrategias organizacionales y sectoriales.
Gobierno TI	Brindar directrices para implementar esquemas de gobernabilidad de TI y para adoptar políticas que permitan alinear los procesos y planes de la institución con los del sector.
Información	Definir el diseño de los servicios de información, la gestión del ciclo de vida del dato, el análisis de información y el desarrollo de capacidades para el uso estratégico de la
	misma.
Sistemas de Información	Planear, diseñar la arquitectura, el ciclo de vida, las aplicaciones, los soportes y la gestión de los sistemas que facilitan y habilitan las dinámicas en una institución.
Servicios Tecnológicos	Gestionar con mayor eficacia y transparencia la infraestructura tecnológica que soporta los sistemas y servicios de información en las instituciones.
Uso y Apropiación	Definir la estrategia y prácticas que apoyan la adopción del Marco y la gestión TI que requiere la institución para implementar la Arquitectura TI.

El dominio de Servicios Tecnológicos busca gestionar la infraestructura

tecnológica que sostiene los sistemas y servicios de información en las instituciones. Las direcciones de Tecnología y Sistemas de Información deben garantizar su disponibilidad y operación permanente, que beneficie a todos los usuarios.

La estrategia de servicios tecnológicos contempla el desarrollo de los siguientes aspectos:

- Arquitectura de infraestructura tecnológica.
- Procesos de gestión: capacidad, puesta en producción y operación.
- Servicios de conectividad.
- Servicios de administración y operación.
- Soporte técnico y mesa de ayuda.
- Seguimiento e interventorías.

Dentro del ámbito de Operación de los Servicios Tecnológicos contiene el elemento de Operación y continuidad de los Servicios Tecnológicos que entrega un modelo de Seguridad y Privacidad de la Información y a su vez presenta una guía de preparación para la continuidad del negocio, que será considerada en esta propuesta de trabajo.

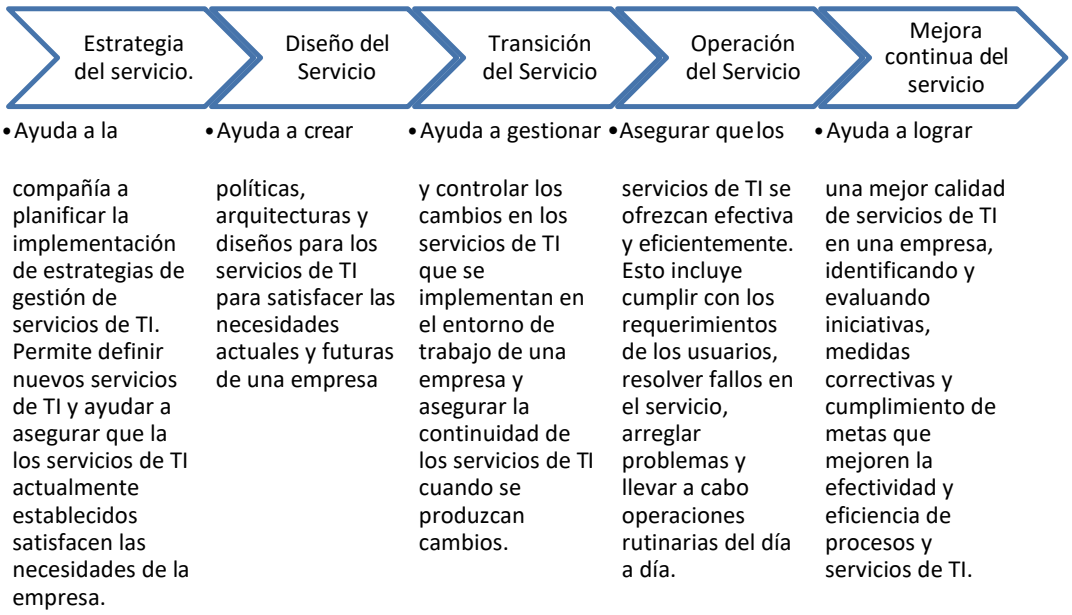
ITIL V3- Information Technology Information Library

ITIL V3 es un marco para la gestión de servicios de TI desarrollado en el Reino.

Unido por la Oficina de Comercio del Gobierno (Office of Government Commerce - OGC), el marco de trabajo ITIL describe los métodos, funciones, roles y procesos sobre los que las organizaciones pueden desarrollar y evaluar sus propias actividades de TI [6].

ITIL implementa diferentes procesos de Gestión de Servicios de TI, tales

como la gestión del ciclo de vida y solicitud de gestión para mejorar la calidad de los servicios de TI. El componente básico contiene cinco estrategias de gestión del marco de ITIL, que representan el ciclo de vida de servicios de TI. Las diferentes estrategias de manejo son:



ITIL avala un marco de trabajo denominado Gestión de la Continuidad del Servicio de TI (ITSCM TI Service Continuity Management). El ITSCM se ocupa de los riesgos que podrían causar un impacto en la infraestructura de TI, de manera que una interrupción de los mismos podría poner en peligro la continuidad del funcionamiento de la organización. La ITSCM se concentra en la protección de la infraestructura tecnológica, mientras que la continuidad del negocio se enfoca en los riesgos que podrían generar una interrupción de las operaciones de negocio.

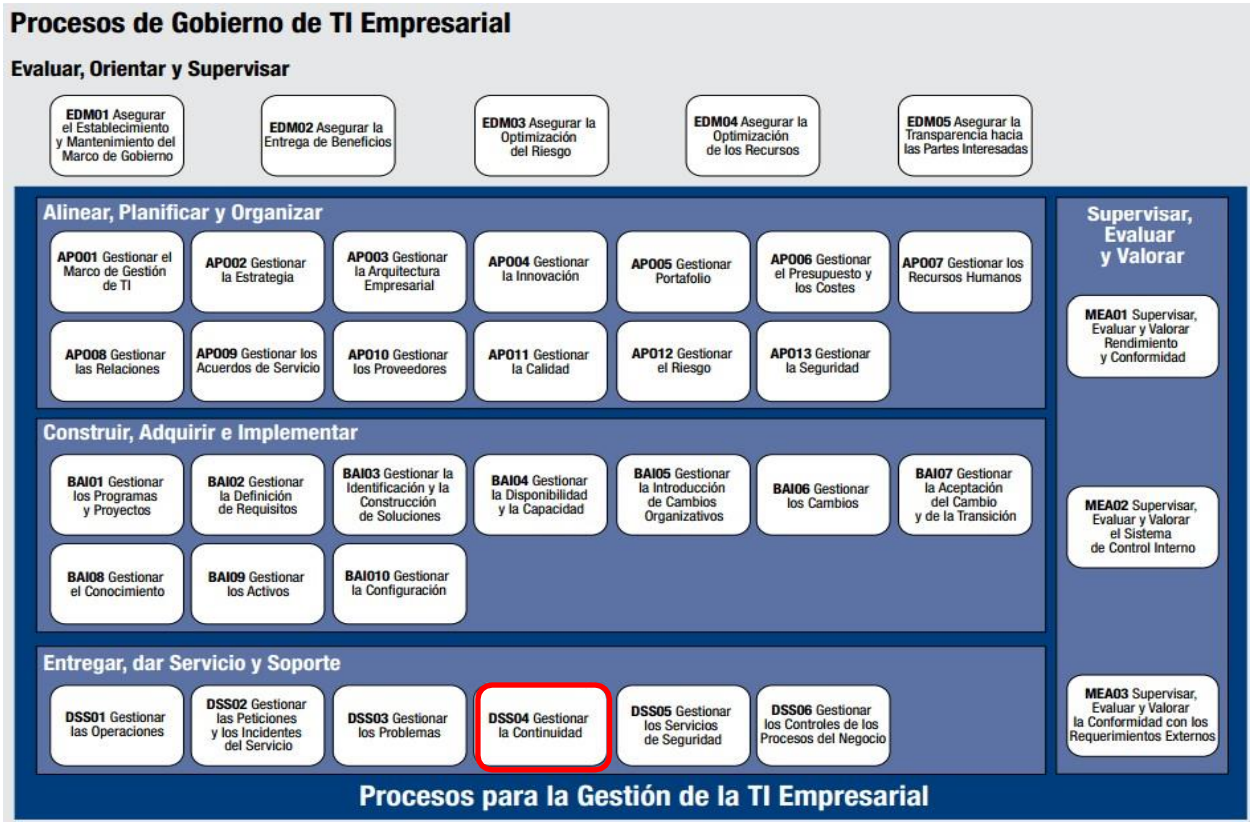
COBIT 5 - Control Objectives for Information and related Technology.

Es una guía de mejores prácticas para el control y supervisión de las tecnologías de la información - TI, mantenido por ISACA (Information Systems Audit and Control Association) y el ITGovernance Institute. COBIT es un marco de gobierno de las tecnologías de información que proporciona herramientas de control de las tecnologías en la organización y su alineamiento con los objetivos del negocio.

COBIT 5 provee de un marco de trabajo integral que plantea reglas claras apoyando a las organizaciones en la creación de valor desde TI lo cual significa generar beneficios a un coste óptimo de los recursos optimizando los niveles de riesgo [7]. COBIT 5 puede ser aplicado por diferentes modelos de negocio y sectores, ya sea en el público o privado y ayuda a la alta dirección y a ejecutivos a gestionar las inversiones en TI durante todo su ciclo de vida proporcionando un método para evaluar si los servicios de TI y las nuevas iniciativas están cumpliendo con las exigencias corporativas y si cumple con las expectativas de beneficios.

Los principios básicos de COBIT 5 habilitan a cualquier organización para construir un marco de gobierno y gestión para optimizar los recursos y hacer uso estratégico de las TI beneficiando a las partes interesadas, estos son:

COBIT 5 está organizado en 37 objetivos de control, agrupados en 5 dominios:



Dentro del marco está definido en el proceso Entregar, dar Servicio y Soporte DSS04, que se enfoca en establecer y mantener un plan para permitir al negocio y a TI, responder a los incidentes y las interrupciones del servicio para la operación continua de los procesos críticos para el negocio y los servicios TI, y mantener la disponibilidad de la información a un nivel aceptable para la empresa. De acuerdo a la definición de Cobit, es un proceso de gestión integral para establecer y mantener un plan que permita al negocio y a TI responder a incidentes e interrupciones de servicios para la operación continua de los procesos críticos para el negocio y los servicios de TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para las empresas.

Gobierno en línea-Gobierno digital

En el año 2010, en el marco del congreso de ANDICOM, el Gobierno Nacional anunció el plan de Tecnologías de la Información y las Comunicaciones, denominada Vive Digital, cuyo objetivo es que el país dé un gran salto tecnológico mediante la masificación de Internet y el desarrollo del ecosistema digital nacional en cuanto a infraestructura, los servicios, las aplicaciones y los usuarios. Dentro de las aplicaciones del plan Vive Digital se encuentra la estrategia de Gobierno en Línea, GEL, que es la estrategia de gobierno electrónico (e-government) en Colombia. El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), a través de la Dirección de Gobierno Digital, presentó la política de Gobierno Digital -expresada en el Decreto 1008 del 14 de junio de 2018-, cuyo objetivo es incentivar el uso y aprovechamiento de las TIC para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital, y busca construir un Estado más eficiente, más transparente y más participativo gracias a las TIC y cuyos ejes temáticos son:

TIC para el Gobierno Abierto: Busca construir un Estado más transparente y colaborativo, donde los ciudadanos participan activamente en la toma de decisiones gracias a las TIC.

TIC para servicios: Busca crear los mejores trámites y servicios en línea para responder a las necesidades más apremiantes de los ciudadanos.

TIC para la gestión: Busca darle un uso estratégico a la tecnología para hacer más eficaz la gestión administrativa.

Seguridad y privacidad de la información: Busca guardar los datos de los ciudadanos, garantizando la seguridad de la información.

Para el desarrollo del componente de Seguridad y Privacidad de la Información, el Ministerio de Tecnologías de la Información y las Comunicaciones, MinTIC, ha definido los lineamientos a través del decreto 1078 de 2015[2], único reglamentario del sector de tecnologías de información y las comunicaciones, y es de obligatorio cumplimiento para las entidades del estado de orden territorial[3]:

Componente/Año	Entidades A (%)					
	2015	2016	2017	2018	2019	2020
TIC para ser servicios	70%	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para Gobierno abierto	80%	95%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para la Gestión	20%	45%	80%	100%	Mantener 100%	Mantener 100%
Seguridad y Privacidad de la Información	35%	50%	80%	100%	Mantener 100%	Mantener 100%

Componente/Año	Entidades B (%)					
	2015	2016	2017	2018	2019	2020
TIC para ser servicios	45%	70%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para Gobierno abierto	65%	80%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para la Gestión	10%	30%	50%	65%	80%	100%
Seguridad y Privacidad de la Información	10%	30%	50%	65%	80%	100%

Componente/Año	Entidades C (%)					
	2015	2016	2017	2018	2019	2020
TIC para ser servicios	45%	70%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para Gobierno abierto	65%	80%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para la Gestión	10%	30%	50%	65%	80%	100%
Seguridad y Privacidad de la Información	10%	30%	50%	65%	80%	100%

Plazos implementación de actividades Manual de Gobierno en Línea- Gobierno Digital. *Tomado de "Modelo de seguridad y privacidad de la Información" MinTIC.*

El modelo está compuesto por lineamientos, políticas, normas, procesos en 16 anexos de apoyo y está basado en el ciclo PHVA, alineado con el estándar NTC: ISO/IEC 7001:2005 y complementado con otras iniciativas y estándares nacionales e internacionales, tales como MECI-Modelo Estándar de Control Interno; COBIT, ITIL, entre otros.

ISO 22301

La ISO 22301 es la nueva norma internacional de gestión de continuidad de negocio. Esta ha sido creada en respuesta a la fuerte demanda internacional que obtuvo la norma británica original, BS 25999-2 y otras normas.

ISO 22301 identifica los fundamentos de un sistema de gestión de continuidad de negocio, estableciendo el proceso, los principios y la terminología de gestión de continuidad de negocio. Esta norma proporciona una base de entendimiento, desarrollo e implantación de continuidad de negocio dentro de su organización y le da la confianza de negocio a negocio y de negocio a cliente. Se usa para asegurar a las partes interesadas clave que su empresa está totalmente preparada y que puede cumplir con los requisitos internos, regulatorios y del cliente.

.
ISO 22301 se compone de 10 cláusulas principales, las primeras corresponden al alcance, referencias normativas y términos y definiciones. Los capítulos principales de los que se compone la norma son:

4. Contexto de la organización.

El primer paso es conocer la organización, sus necesidades internas y externas, y establecer límites para el alcance del sistema de gestión. Esto requiere que la organización entienda las necesidades de los stakeholders pertinentes.

5. Liderazgo

ISO22301 hace especial énfasis en la necesidad de un liderazgo apropiado en la Gestión de la Continuidad del Negocio. Es útil para que la alta dirección asegure que se proporcionan los recursos necesarios, nombra a los responsables que implementan y mantienen el SGCN y establece la política.

6. Planificación

Es necesario que la empresa identifique los riesgos para poder implementar el sistema de gestión e instaure los criterios y objetivos a seguir.

7. Soporte

Para llegar al éxito en la continuidad del negocio, se debe tener en la organización personas con los conocimientos, experiencia y habilidades pertinentes, para que apoyen al SGCN y respondan a los incidentes, así como servicios de soporte, recursos de formación y toma de conciencia, comunicaciones internas y externas y control de la documentación.

8. Operaciones

La empresa debe realizar el análisis de impacto en el negocio para comprender cómo su negocio se vería afectado por una interrupción y

cómo cambia con el tiempo. Por otro lado, la evaluación de riesgos se encargará de tratar los riesgos para el negocio de forma estructurada e informar de éstos en el desarrollo de la estrategia de continuidad del negocio. En esta cláusula se instauran los requisitos para la continuidad de negocio, hace referencia a los ejercicios y pruebas, parte esencial en el SGCN, ISO 22301.

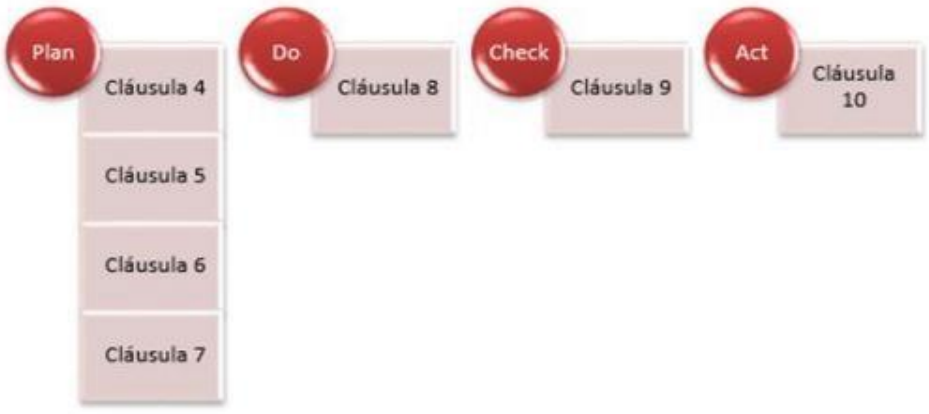
9. Evaluación

Es imprescindible contar con auditorías internas, con la revisión y seguimiento permanente de los SGCN por parte de la organización y actúe sobre dichas revisiones.

10. Mejora

Ante el cambio constate de las organizaciones y sus entornos, aquí se definen las acciones para mejorar el SGCN para aumentar permanentemente la eficacia del sistema de continuidad del negocio.

La norma ISO 22301 trabaja sobre el ciclo dinámico PHVA: Planear – Hacer – Verificar – Actuar. Este ciclo nos ayuda a la realización de actividades, de una manera más organizada y eficaz. Por tanto, aceptar la metodología de trabajo ofrecido por el ciclo PHVA es una guía básica para la gestión de actividades y procesos, ofreciéndonos una estructura ejemplar de un sistema que es aplicable para cualquier organización.



Cláusulas de la Norma ISO 22301 dentro del modelo PHVA. Adaptado ISO, 2012

Buenas prácticas y casos de éxito

Seguridad y Privacidad de la Información – Guía No. 10 guía para la preparación de las TIC para la continuidad del negocio. Ministerio de las Tecnología y las comunicaciones MinTIC – Gobierno Nacional de Colombia. 2010.

La guía liberada por MinTIC es un complemento del modelo de seguridad y privacidad de la información y se constituye en un referente de la continuidad del negocio para las entidades del Estado para la construcción de la resiliencia y la capacidad de una respuesta efectiva, que le permita proteger los intereses de las Entidades debido a disrupciones.

El modelo de operación de Continuidad del Negocio para el Modelo de Seguridad y Privacidad de la Información, contempla su implementación en las cuatro fases del ciclo del Modelo para que las Entidades puedan gestionar la seguridad y privacidad de la información, con el fin de fortalecer la protección de los datos y dar cumplimiento a lo establecido en la Estrategia de Gobierno en Línea, dentro del Marco de Referencia Arquitectura TI, cubriendo de una manera integral cada uno de sus componentes.

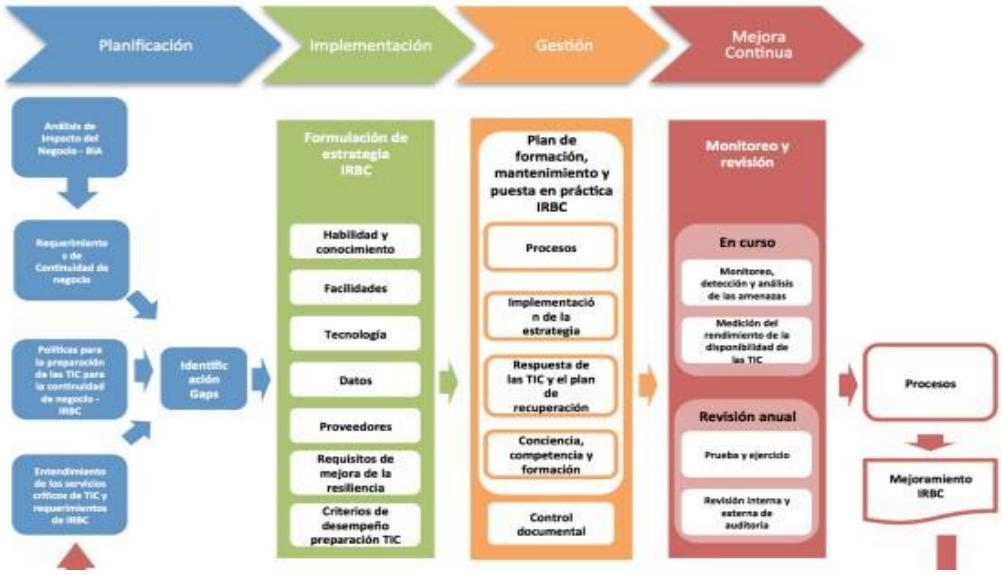


Ilustración 9. Marco Continuidad del Negocio para Seguridad y Privacidad de la Información – Tomado de MinTIC

Este modelo hace referencia a un sistema de gestión que complementa y soporta la continuidad del negocio de la organización y los programas de Sistemas de Gestión de Seguridad de la Información (SGSI). Este marco indica lo que se debe hacer y cumplir, el cómo se debe hacer es criterio de la entidad, apoyándose en la adopción de mejores prácticas.

Metodología para la Gestión de la Continuidad del Negocio. Rodrigo Ferrer V

Este artículo publicado en 2015 [12] expone los pasos requeridos para diseñar e implementar un proceso de Gestión de la Continuidad del Negocio orientado a diversas organizaciones en Colombia, basada en los estudios realizados por el Business Continuity Institute (BCI) y el Disaster Recovery Institute International (DRII) los cuales han sido las organizaciones líderes a nivel mundial en esta campaña de formación en los temas relacionados con la continuidad del negocio ante diferentes tipos de incidentes. La Gestión de la Continuidad del Negocio (GCN) se considera como parte fundamental del Gobierno y de la gestión del riesgo y se considera el proceso por fases de planeación, implementación, verificación y mejoras, conformando así el conocido ciclo PHVA. La norma internacional ISO 22301 sirvió de consulta permanente para la realización del artículo.

Plan de Continuidad de Negocio. Banco de la República. 2017

Una organización con experiencia en continuidad del negocio es el Banco de la República de Colombia, que cuenta con un Sistema de Gestión de Continuidad (SGC), el cual le brinda la las herramientas para continuar prestando las funciones asignadas al Banco por la Constitución Política, la Ley o sus Estatutos en niveles considerados como aceptables, garantizando la estabilidad al sistema financiero del país. Mediante un plan de continuidad proporciona el marco para construir la resiliencia organizacional, de manera que, después de un incidente perjudicial, se pueda continuar con la entrega de productos y servicios en los niveles considerados como aceptables. El SGC está conformado por: Marco de referencia, Sistema de prevención y atención de emergencias, Planes de contingencia tecnológicos y operativos, Plan de administración de crisis e Iniciativas de integración con sector financiero y Gobierno.

La información de estados de servicios, esquemas y pruebas de contingencia se encuentran publicados en la página web institucional.

Plan institucional de respuesta a emergencias "PIRE". Secretaría Distrital de Hacienda. Alcaldía Mayor de Bogotá D.C. 2013

La Secretaría Distrital de Hacienda -SDH- de Bogotá publicó en 2013 el Plan institucional de respuesta a emergencias, el cual se encuentra en el proceso de implementación y desarrollo como parte del proyecto de Riesgo Operacional y Continuidad del Negocio que contempla, dentro de sus escenarios de evaluación, la falla total sobre las instalaciones físicas y tecnológicas de la entidad, generando repercusiones en la operación, en los sistemas de procesamiento de información y en el personal. Por lo anterior, adoptó como metodología las prácticas profesionales expuestas por el DRII (The Institute for Continuity Management) para garantizar la disponibilidad de estrategias de continuidad que permitan anticiparse a cualquier trastorno que pueda poner en peligro la supervivencia de la Secretaría. Para el efecto, teniendo en cuenta la metodología mencionada, las necesidades de la entidad y los requerimientos normativos, la -SDH- dentro de su Plan de Continuidad del Negocio - PCN- incluye el Plan Institucional de Respuesta a Emergencias -PIRE- en el cual se expone el esquema organizacional que operaría para la atención de la emergencia, y cuyo objeto principal es dar respuesta y cumplimiento a los protocolos Distritales que conforman el Plan de Emergencias de Bogotá -PEB-, adoptado mediante la resolución 004 de 2009.

Mapeo entre estándares y frameworks enfocados a la gestión de la continuidad.

COBIT 5 e ITIL V3

COBIT 5		ITIL V3	
Evaluar, Orientar y Supervisar (EDM)	EDM01. Asegurar el establecimiento y mantenimiento del marco de gobierno	**N/A**	
	EDM02. Asegurar la entrega de beneficios	**Estrategia del Servicio**	Gestión del Portafolio de Servicios
	EDM03. Asegurar la optimización del riesgo	**N/A**	
	EDM04. Asegurar la optimización de recursos	**Estrategia del Servicio**	Gestión de la Demanda
	EDM05. Asegurar la transparencia hacia las partes interesadas	**Estrategia del Servicio**	Gestión de las relaciones de negocios
Alinear, Planificar y Organizar (APO)	APO01. Gestionar el marco de gestión de las TI	**Mejora Continua del Servicio**	Proceso de Mejora
	APO02. Gestionar la estrategia	**Estrategia del Servicio**	Gestión de la Estrategia del Servicio
	APO03. Gestionar la arquitectura empresarial	**N/A**	
	APO04. Gestionar la innovación	**N/A**	
	APO05. Gestionar el portafolio	**Estrategia del Servicio**	Gestión del Portfolio de Servicios
			Gestión del Catálogo de Servicios
	APO06 Gestionar el presupuesto y los costes	**Estrategia del Servicio**	Gestión Financiera de los Servicios
	APO07 Gestionar los Recursos Humanos	**Diseño del Servicio**	Gestión de la Capacidad
	AP008 Gestionar las relaciones	**Estrategia del Servicio**	Gestión de la Demanda
			Gestión de las Relaciones de Negocios
	AP009 Gestionar los acuerdos de servicio	**Estrategia del Servicio**	Gestión del Portfolio de Servicios
			Gestión de la Demanda Diseño del Servicio
			Gestión del Catálogo de Servicios
			Gestión de Niveles de Servicio
		Mejora Continua del Servicio	Gestión de Informes
	APO10 Gestionar los Proveedores.	**Diseño del Servicio**	Gestión de Proveedores

	APO11 Gestionar la calidad	**Mejora Continua del Servicio**	Proceso de Mejora
	APO12 Gestionar el riesgo	**Diseño del Servicio**	Gestión de la Seguridad de la Información
	APO13 Gestionar la seguridad.	**Diseño del Servicio**	Gestión de la Seguridad de la Información
Construir, adquirir e implementar (BAI)	BAI01 Gestión de programas y proyectos	**N/A**	
	BAI02 Gestionar la definición de requisitos	**Diseño del Servicio**	Gestión de Niveles de Servicio
	BAI03 Gestionar la identificación y construcción de soluciones	**N/A**	
	BAI04 Gestionar la disponibilidad y la capacidad	**Diseño del Servicio**	Gestión de la Disponibilidad
			Gestión de la Capacidad
	BAI05 Gestionar la facilitación del cambio organizativo	**N/A**	
	BAI06 Gestionar los cambios.	**Transición del Servicio**	Gestión del Cambio
	BAI07 Gestionar la aceptación del cambio y la transición	**Transición del Servicio**	Planificación y soporte a la Transición
			Gestión de Entregas y Despliegues
			Evaluación del Cambio.
			Gestión del Conocimiento
	BAI08 Gestionar el conocimiento	**Transición del Servicio**	Gestión del Conocimiento
	BAI09 Gestionar los activos	**Transición del Servicio**	Gestión de la Configuración y Activos del Servicio
	BAI10 Gestionar la configuración	**Transición del Servicio**	Gestión de la Configuración y Activos del Servicio
Entrega, Servicio y Soporte (DSS)	DSS01 Gestionar operaciones	**Operación del Servicio**	Gestión de Eventos
	DSS02 Gestionar peticiones e incidentes de servicio	**Operación del Servicio**	Gestión de Incidentes
			Cumplimiento de Solicitudes
	DSS03 Gestionar problemas	**Operación del Servicio**	Gestión de Problemas
	DSS04 Gestionar la continuidad	**Diseño del Servicio**	Gestión de la Continuidad del Servicio
	DSS05 Gestionar servicios de seguridad.	**Diseño del Servicio**	Gestión de Seguridad de la Información
	DSS06 -Gestionar controles de procesos de negocio	**Operación del Servicio**	Gestión de Acceso
Supervisar,	MEA01 -Supervisar, evaluar y valorar el rendimiento y la conformidad	**Mejora Continua del Servicio**	Gestión de Informes

Evaluar y Valorar (MEA)	MEA02 -Supervisar, evaluar y valorar el sistema de control interno.	**Mejora Continua del Servicio**	Proceso de Mejora
	MEA03. Supervisar, evaluar y valorar la conformidad con los requerimientos externos.	**Mejora Continua del Servicio**	Proceso de Mejora

COBIT 5 – ISO 22301

	PLANEAR				HACER	VERIFICAR	ACTUAR
Cláusulas ISO 22301 / Sub Procesos COBIT 5 - DSS04	**Cláusula 4: Contexto de la organización**	**Cláusula 5: Liderazgo**	**Cláusula 6: Planificación**	**Cláusula 7: Soporte**	**Cláusula 8: Operaciones**	**Cláusula 9: Evaluación de desempeño**	**Cláusula 10: Mejora**
DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance	X						
DSS04.02 Mantiene una estrategia de continuidad.		X	X				
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.			X	X	X		
DSS04.04 Ejercitar, probar y revisar el plan de continuidad.					X		
DSS04.05 Revisar, mantener y mejorar el plan de continuidad.					X	X	
DSS04.06 Proporcionar formación en el plan de continuidad.						X	
DSS04.07 Gestionar acuerdos de respaldo							X
DSS04.08 Ejecutar revisiones pos reanudación.						X	X

COBIT 5 – ISO 27002:2013

Práctica COBIT 5 - DSS04	Control ISO27002:2013		
DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance	A.17.1.1	Planificación de la continuidad de la seguridad de la información.	17.1 Continuidad de la seguridad de la información
DSS04.02 Mantiene una estrategia de continuidad.	A.17.1.1	Planificación de la continuidad de la seguridad de la información.	
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.	A.17.1.2	Implantación de la continuidad de la seguridad de la información.	
DSS04.04 Ejercitar, probar y revisar el plan de continuidad.	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
DSS04.05 Revisar, mantener y mejorar el plan de continuidad.	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
DSS04.06 Proporcionar formación en el plan de continuidad.	N/A		
DSS04.07 Gestionar acuerdos de respaldo	A.12.3.1	Copias de seguridad de la información.	12.3 Copias de seguridad
	A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	17.2 Redundancias.
DSS04.08 Ejecutar revisiones pos reanudación.	N/A		

Continuidad del negocio

Componentes del modelo

La guía para la Preparación de las TIC para la Continuidad de Negocio (MINTIC, Guía para la Preparación de las TIC para la Continuidad del Negocio, 2010), descrito en el ítem 5.2.1., es fundamental para el desarrollo de este trabajo, donde se realizaron los cambios a las políticas generales de acuerdo a las necesidades corporativas y tecnológicas actuales de las entidades colombianas.

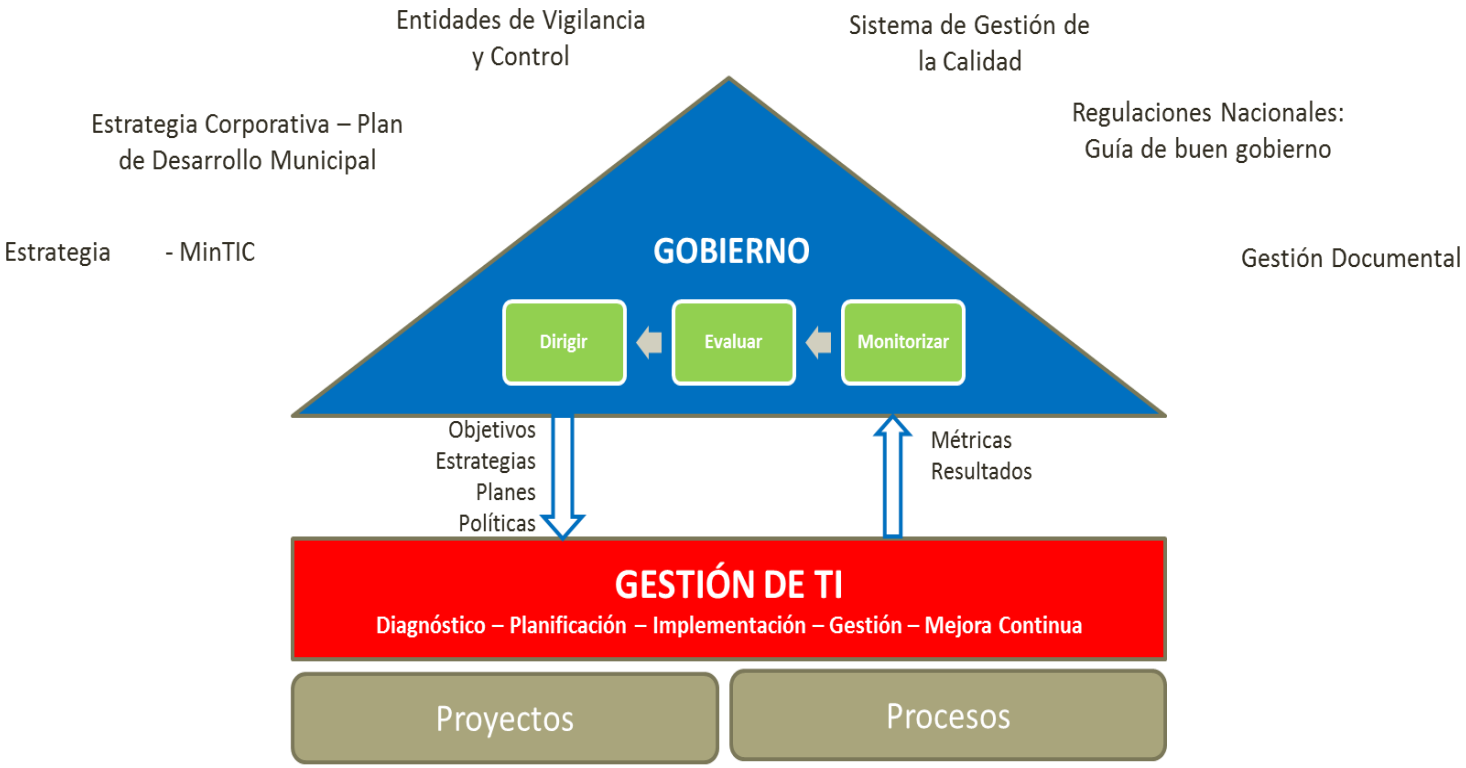
La guía fue diseñada con base al Marco de Seguridad y Privacidad de la Información, el cual define un ciclo de funcionamiento del modelo de operación de continuidad del negocio. Las fases que comprenden el modelo de operación contienen objetivos, metas y herramientas que permiten que la continuidad del negocio sea un sistema sostenible dentro de las entidades.

Las fases del modelo propuesto fueron desarrollas con base a los lineamientos de COBIT 5.0 en su dominio DSS - Entrega, Servicio y Soporte, proceso:

DSS04 Gestión de la continuidad (Todas las prácticas)
DSS05 Gestionar Servicios de Seguridad (Supervisar la Infraestructura de TI frente a eventos de seguridad)
DSS06 Gestionar Controles de Proceso de Negocio (Asegurar los activos de información)

Para esto se definió un marco de continuidad para la recuperación de procesos de tecnología en las entidades públicas, donde a cada fase o componente se le relacionan las prácticas aplicables del proceso de Gestión de la continuidad de Cobit5.

El modelo genérico de gobierno y gestión de TI está dado por:



Continuidad :

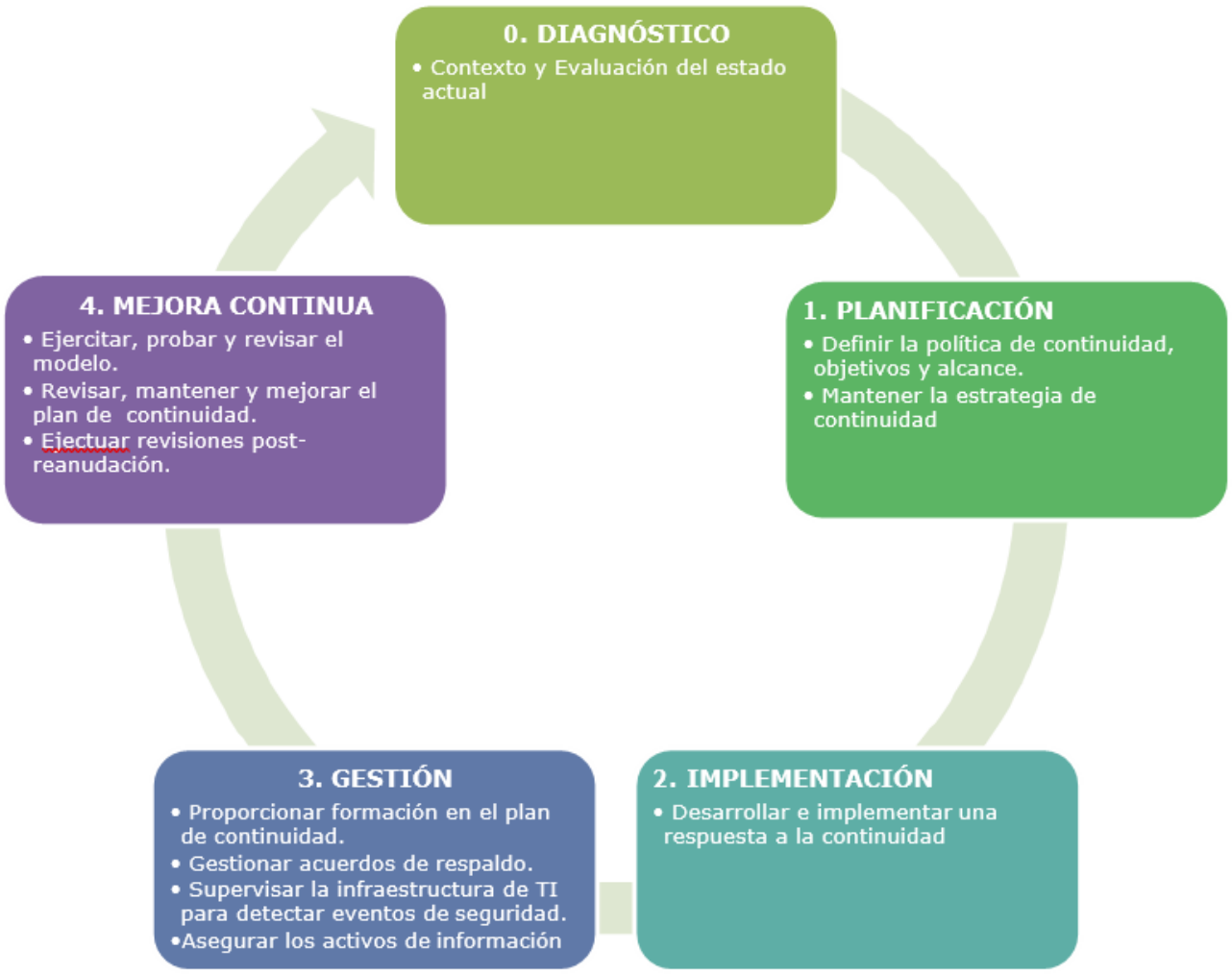
- COBIT 5 – DSS04
- Marco de Referencia Arquitectura TI - Modelo de Seguridad y Privacidad de la Información – MSPI – MINTIC

Gestión de proyectos

Mantenimiento de soluciones de software

Gestión de Infraestructura Tecnológica Servicios y soporte en TI.

Administración de TI



Modelo propuesto de gobierno y gestión de TI para garantizar la continuidad del negocio en las Entidades Públicas.

De acuerdo al modelo planteado y teniendo como base el modelo de cascada de metas de Cobit5, se alinean las metas de TI, del negocio y los Objetivos de gobierno partiendo de los procesos que involucran la gestión de la continuidad:

			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
GOBIERNO Y GESTIÓN DE LA CONTINUIDAD Metas TI / Procesos de COBIT 5			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructuras de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	Disponibilidad de información útil y fiable para la toma de decisiones	Cumplimiento de TI con las políticas internas	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			Financiera						Cliente		Interna							Aprendizaje y Crecimiento	
Entregar, Dar Servicio y Soporte	DSS04	Gestionar la Continuidad				P			P							P			
	DSS05	Gestionar los Servicios de Seguridad		P		P						P							
	DSS06	Gestionar los Controles de los Procesos del Negocio				P			P										

COBIT5 Mapeo entre las Metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI

		Objetivos de Gobierno																	
		1. Valor para las Partes	2. Cartera de productos y	3. Riesgos de negocio	4. Cumplimiento	5.	6. Cultura de servicio	7. Continuidad	8. Respuestas ágiles a un	9. Toma estratégica	10. Optimi	11. Optimización	12. Optimización	13. Programas gestionados	14. Productividad	15. Cumplimie	16. Personas preparadas y	17. Cultur
Dimensión	**Metas de TI**	**Financiera**					**Cliente**					**Interna**					**Aprendizaje y**	
Financiera	01 - Alineamiento de TI y la estrategia de negocio	P	P				P		P	P		P		P				
	02 - Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas				P											P		
	03 - Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P												P				
	04 - Riesgos de negocio relacionados con las TI gestionados			P				P			P							
Cliente	07 - Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P				P		P			P						
Interna	10 - Seguridad de la información, infraestructuras de procesamiento y aplicaciones			P	P			P								P		
	14 - Disponibilidad de información útil y fiable para la toma de decisiones							P		P								

COBIT5 Relación Primaria Metas Negocio con Metas TI

		Objetivos de Gobierno		
Dimensión	Objetivo de negocio relacionado de Cobit 5	Entrega de beneficios	Optimización de riesgos	Optimización de recursos
Financiera	1. Valor para las Partes Interesadas de las Inversiones de Negocio.	P		
	2. Cartera de productos y servicios competitivos	P	P	
	3. Riesgos de negocio gestionados (salvaguarda de activo)		P	
	4. Cumplimiento de leyes y regulaciones externas		P	
Cliente	6. Cultura de servicio orientada al cliente	P		
	7. Continuidad y disponibilidad		P	
	8. Respuestas ágiles a un entorno de negocio cambiante	P		
	9. Toma estratégica de decisiones basadas en información	P	P	P
	10. Optimización de costes de entrega del servicio	P		P
Interna	11. Optimización de la funcionalidad de los procesos de negocio	P		P
	13. Programas gestionados de cambio en el negocio			
	15. Cumplimiento con las políticas internas		P	

COBIT5 - Relación Objetivos de Negocio con Objetivos Gobierno

OBJETIVOS ESTRATÉGICOS DE GOBIERNO DE LAS ENTIDADES PUBLICAS.

Entrega de Beneficios	Optimización del riesgo	Optimización de recursos
• **Optimizar los procesos de la entidad y adoptar sistemas de información modernos, seguros, ágiles y bajo estándares internacionales que contribuyan a la efectividad del servicio.**	• Implementar nuevos estándares de gestión financiera y fiscal orientados a la eficiencia del ingreso, el gasto bajo parámetros de evaluación y seguimiento de riesgos en un ambiente de control.	• Implementar nuevos mecanismos de recaudo que faciliten el pago de las obligaciones. • Orientar el talento humano al logro de los objetivos institucionales, fortaleciendo las competencias, la calidad de vida laboral y afianzando el • sentido de pertenencia con la entidad.

Diagnóstico

Esta es el componente inicial o la fase preliminar para desarrollar el diagnóstico de la organización en cuanto a gobierno y gestión de la continuidad enfocada a servicios críticos. Se listaron las ocho prácticas de COBIT 5 del proceso DSS04 - Gestión de la Continuidad, con las actividades mínimas para su cumplimiento y registro de cumplimiento. Cada actividad tiene un peso dentro de la práctica total, lo cual al final de la resolución de la encuesta genera un valor numérico porcentual de cumplimiento de la práctica.
La medición de la capacidad de la entidad, respecto a la gestión de la continuidad, fue desarrollada con el enfoque de evaluación de capacidad de procesos basado en el estándar ISO/IEC 15504. A cada subproceso se le genera una evaluación por rango y por niveles de capacidad.

Evaluación por Rango

ID	NOMBRE	RANGO
N	No alcanzado	0% al 15%
P	Parcialmente alcanzado	15% al 50%
L	Ampliamente alcanzado	50% - 85%
F	Completamente alcanzado	85% - 100%

Diagnóstico - Evaluación por Rango

Nivel de Capacidad

La evaluación por nivel de capacidad, está dada por el nivel de implementación de la práctica, en cuanto a las actividades del proceso. Está basada en la escala de evaluación utilizada en el MSPI.

Tabla de Escala de Valoración de la Práctica		
Descripción	Calificación	Criterio
No Aplica	N/A	No aplica.
Inexistente	0	Total, falta de cualquier proceso reconocible. La Entidad no ha reconocido que hay un problema a tratar. No se aplican las prácticas de los procesos del Gobierno y Gestión.
Inicial	20	Hay una evidencia de que la Entidad ha reconocido que existe una situación y que hay que tratarla. No hay procesos estandarizados. La implementación de una actividad depende de cada individuo y es principalmente reactiva. Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y las actividades siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares.
Efectivo	60	Los procesos y las actividades se documentan y se comunican. Las actividades son efectivas y se ejecutan casi siempre. Es poco probable la detección de desviaciones cuando las actividades no se ejecutan oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Las actividades se monitorean. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Diagnóstico - Nivel de Capacidad

Así mismo, el cumplimiento de los atributos del proceso predeterminará el nivel de capacidad.

	Práctica		Diagnóstico Situación Actual Gobierno y Gestión de la Continuidad					
		Descripción	Actividades	Calificación Actual	Peso Actividad	Valor Práctica	Calificación Objetivo	GAP
PLANIFICACIÓN	DSS04.01	**Definir la política de continuidad del negocio, objetivos y alcance.**	¿Se encuentran identificados los procesos internos y subcontratados y actividades de servicios que son críticos para la Institución?		30%	0	100	100
			¿Están identificados los roles y responsabilidades para definir la política de continuidad del negocio?		30%			
			¿La política de continuidad del negocio se encuentra definida y documentada?		40%			
	DSS04.02	**Mantener una estrategia de continuidad.**	¿Se realiza un análisis de impacto en el negocio para evaluar el impacto en tiempo de una disrupción en funciones críticas de la entidad y su efecto?		50%	0	100	100
			¿Se hace algún análisis de la probabilidad de amenazas que pueden causar pérdidas de continuidad de negocio y se identifican las medidas para reducir la probabilidad y el impacto?		25%			
			¿Se tiene aprobación del Director o CEO para implementar las estrategias identificadas?		25%			
IMPLEMENTACI		**Desarrollar e implementar una respuesta**	¿Se encuentran definidos las condiciones y procedimientos de recuperación que permitan la reanudación de los procesos críticos de la Institución?		50%			

	DSS04.03	**a la continuidad del negocio.**	¿Los proveedores clave tienen implantados planes de continuidad efectivos?		20%	0	100	100

			¿Están definidos y documentados los recursos necesarios para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI?		20%			
GESTIÓN	**DSS04.06**	**Proporcionar formación en el plan de continuidad.**	¿Existen planes de formación para quienes realicen de manera continuada planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes?		100%	0	100	100
	DSS04.07	**Gestionar acuerdos de respaldo**	¿Se realizan copias de seguridad de los sistemas?		40%	0	100	100
			¿Las aplicaciones, sistemas o datos mantenidos por terceras personas se encuentran respaldadas?		30%			
			¿Se realizan pruebas periódicamente de las copias de seguridad?		30%			
	DSS05.07	**Supervisar la infraestructura TI para detectar eventos de seguridad.**	¿Se registró de los eventos relacionados con la seguridad reportada por las herramientas de monitorización de la seguridad de la infraestructura?		100%	0	100	100

	DSS06.06	**Asegurar los activos de información.**	¿Se aplican las políticas de clasificación de datos y seguridad y los procedimientos para proteger los activos de información bajo el control interno de la entidad?		100%	0	100	100

MEJORA CONTINUA	**DSS04.04**	**Ejercitar, probar y revisar el plan de continuidad.**	¿Se encuentran definidos los objetivos para probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio?		30%	0	100	100
			¿Existe un procedimiento de asignación de roles y responsabilidades para realizar ejercicios y pruebas del plan de continuidad?		30%			
			¿Existe un plan de ejercicios y actividades de prueba, tal como está definido en el plan de continuidad?		40%			
	DSS04.05	**Revisar, mantener y mejorar el plan de continuidad.**	¿Se revisa el plan de continuidad regularmente teniendo en cuenta cambios nuevos en la secretaría de hacienda, ya sea en los procesos de negocio, tecnologías, infraestructura, sistemas operativos y sistemas de aplicaciones?		50%	0	100	100
			¿Se comunican los cambios para la aprobación del Director o CEO?		50%			
	DSS04.08	**Ejecutar revisiones post-reanudación.**	¿Existe un plan de ejercicios y actividades de prueba, tal como está definido en el plan de continuidad?		40%	0	100	100

			¿Se revisa el plan de continuidad regularmente teniendo en cuenta cambios nuevos en la entidad, ya sea en los procesos de negocio, tecnologías, infraestructura, sistemas operativos y sistemas de aplicaciones?		50%			
			¿Se comunican los cambios para la aprobación del Director o CEO?		50%			
	PROMEDIO EVALUACIÓN DE PROCESOS					**0**	**100**	**100**

Instrumento para evaluar nivel de capacidad de los procesos de un modelo de gobierno y gestión de TI para garantizar la continuidad en las Entidades Públicas tomando como Marco de Referencia de COBIT 5.

Planificación

En este componente se definen la estrategia metodológica para establecer las políticas, objetivos, procesos y procedimientos, pertinentes que le permitan a la Entidad, la preparación de las TIC para la continuidad del negocio alineado a los objetivos de gobierno. Se basó en el proceso de Cobit 5:
DSS04.01 Definir las políticas de continuidad de negocio, objetivos y alcance
DSS04.02 Mantener una estrategia de Continuidad.

Las principales actividades son:

1. Identificar los procesos de negocio internos y subcontratados y actividades de servicios que son críticos para las operaciones de la entidad o necesario para cumplir con las obligaciones legales y / o contractuales.
2. Identificar las partes interesadas y los roles y responsabilidades clave para definir y acordar la política de continuidad y alcance.
3. Definir y documentar los objetivos para la continuidad del negocio y la necesidad de integrar la planificación de la continuidad a la cultura empresarial.
4. Identificar posibles escenarios que puedan dar lugar a sucesos que podrían causar incidentes que afecten el normal funcionamiento de la entidad y por tanto la prestación de servicios al ciudadano.
5. Realizar un análisis de impacto de negocio (BIA) para evaluar el impacto en el tiempo de una interrupción de las funciones críticas o misionales de la entidad y el efecto que una interrupción podría tener en ellos.

El procedimiento para realizar el BIA es tomado de la Guía para realizar el Análisis de Impacto de Negocios:

Id	Fases	Descripción
1	Identificación de funciones y procesos	Identificar áreas y procesos apoyo a los procesos misionales de negocio y servicios de TI relacionados.
2	evaluación de impactos Operacionales	El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio. Se hacen tablas de impacto, con esquemas de valoración, referente a la interrupción de la operación en los procesos listados en la fase anterior.
3	Identificación de Procesos críticos	La identificación de los procesos críticos del negocio se da con base en la clasificación de los impactos operacionales de las organizaciones, según los valores de interpretación del proceso crítico: A - Crítico para el Negocio, la función del negocio no puede realizarse B - No es crítico para el negocio, pero la operación es una parte integral del mismo. C - La operación no es parte integral del negocio.
4	establecimiento de tiempos de recuperación	Se establecen los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios: RPO - Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio. RTO - Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración. WRT - Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados, es

		decir, Tiempo de Recuperación de Trabajo. MTD - Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.
5	Identificación de activos	Las diferentes actividades contempladas en la función crítica del negocio deben considerarse de vital importancia cuando apoyan los procesos críticos del negocio; por lo tanto, es clave en este punto, la identificación de activos críticos de Sistemas de Tecnología de Información que permitan tomar acciones para medir el impacto del negocio de las Entidades.
6	identificación de procesos alternos	La identificación de procesos alternos hace posible que los procesos del negocio puedan continuar operando en caso de presentarse una interrupción; para ello es oportuno que las Entidades tengan métodos alternativos de manera temporal que ayuden a superar la crisis que ha generado una interrupción.
7	Generación de Informe de Impacto del negocio	Listado de procesos críticos Listado de prioridades de sistemas y aplicaciones Listado de tiempos MTD, RTO y RPO Listado de procedimientos alternos

6. Evaluar la probabilidad de amenazas que podrían causar la pérdida de la continuidad del negocio y determinar las medidas que reduzcan la probabilidad y el impacto a través de una mejor prevención y una mayor capacidad de recuperación.

7. Identificar los requisitos de continuidad, analizar para identificar las posibles opciones estratégicas empresariales y técnicas.

8. Determinar las condiciones y los propietarios de las decisiones clave que hará que los planes de continuidad para ser invocados.

9. Obtener la aprobación del ejecutivo de negocios para las opciones estratégicas seleccionadas.

Implementación

Para la implementación del componente de planificación, se tiene en cuenta los aspectos más relevantes en los procesos de implementación de la estrategia del Plan de Continuidad, las cuales deberán ser implementadas después de la aprobación de la alta dirección.
La implementación se gestiona como un proyecto a través del proceso de control de cambios formales de la Entidad y de los controles de gestión del proyecto de la Gestión de Continuidad del Negocio con el fin de asegurar visibilidad completa de la gestión y del reporte.

Las actividades generales a desarrollar en este proceso son:

1. Definir las acciones de respuesta a incidentes y las comunicaciones que deben adoptarse en caso de perturbación. Definir las funciones y responsabilidades relacionadas, incluyendo la rendición de cuentas de las políticas y su implementación.
2. Desarrollar y mantener operativos los procedimientos que deben seguirse para permitir la operación continua de los procesos críticos de negocio y / o régimen de temporales, incluyendo enlaces a los planes de los proveedores de servicios externalizados.
3. Asegurar que los proveedores clave tienen planes de continuidad de efectivos. Obtener evidencia auditada según sea necesario.

4. Definir las condiciones y procedimientos de recuperación que permitan la reanudación del proceso de negocio, incluida la actualización y la recuperación de las bases de datos de información para preservar la integridad de la información.
5. Definir y documentar los recursos necesarios para apoyar los procedimientos de continuidad y recuperación, teniendo en cuenta las personas, las instalaciones y la infraestructura de TI.
6. Definir y documentar los requisitos para las copias de seguridad de información necesarias para apoyar los planes, incluyendo los planes y documentos en papel, así como archivos de datos, y considerar la necesidad de seguridad y almacenamiento externo.
7. Determinar las habilidades necesarias para las personas involucradas en la ejecución del plan y los procedimientos.
8. Distribuir los planes y la documentación de apoyo debidamente autorizada a las partes interesadas y asegurarse de que son accesibles en todos los escenarios de desastre.

Gestión

Para el desarrollo de este proceso se tuvo como referencia Cobit 5.0 en sus prácticas:

- DSS04.06 - Llevar a cabo la formación y capacitación del plan de continuidad.
- DSS05.07 - Supervisar la infraestructura para detectar eventos relacionados con la seguridad.
- DSS06.06 - Asegurar los activos de información.

En este proceso se determinan temas relacionados con la capacitación y sensibilización de todos los funcionarios de la entidad respecto a la continuidad del negocio, cuales son su roles y responsabilidades en caso de una emergencia.
En gestión también se definen cuáles son las habilidades y perfiles necesarios para restaurar las aplicaciones, sistemas y datos críticos de la organización en términos de conocimientos tecnológicos. Esto es en caso que sea necesario reemplazar en un momento dado a todos los miembros del equipo de TI, por ausencia o incapacidad.

Las principales actividades de esta práctica referentes a la práctica

DSS04.06 son:

1. Definir y mantener los requisitos de formación y planes para los que realizan la planificación de continuidad, las evaluaciones de impacto, evaluaciones de riesgo, medios de comunicación y respuesta a incidentes. Asegúrese de que los planes de formación consideran la frecuencia y los mecanismos de entrega de capacitación y formación.

2. Desarrollar Competencias basados en la Formación Práctica, Incluyendo la Participación en Ejercicios y Pruebas.

3. Habilidades y competencias del líder en función de los ejercicios y resultados de pruebas.

De igual forma se agregaron prácticas adicionales de seguridad y protección de los datos que se manejan en la entidad, que es donde entran a jugar su papel el DSS05 Gestionar servicios de seguridad y DSS06 Gestionar Controles de Proceso de Negocio. Las principales actividades son:

1. Aplicar las políticas de clasificación de datos y uso aceptable y seguridad y los procedimientos para proteger los activos de información bajo el control del negocio.
2. Restringir el uso, la distribución y el acceso físico a la información acorde a su clasificación.
3. Registrar los eventos relacionados con la seguridad reportada por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse con base a la consideración de riesgo. Se debe retener por un periodo apropiado para asistir en futuras investigaciones.

En este proceso también se ejecuta la actividad que tal vez es la más importante en la Gestión de la Continuidad de Negocio, que es la gestión de backups. Para esto nos basamos en el subproceso de Cobit DSS04.06 Gestionar Copias de Seguridad. Las actividades generales son:

1. Documentación procedimiento de backup. Tener en cuenta:
- Frecuencia (diario, semanal, mensual)

- Modo de backup (ejemplo: duplicación de copias de seguridad en tiempo real)
- Tipo de Backup (incremental, total)
- Tipo de medios (cintas, DVD, Nube)
- Tipos de datos
- Creación de registros
- Datos informáticos críticos de los usuarios (ejemplo: hojas de cálculo).
- Ubicación física y lógica de la fuente de datos.
- Seguridad y derechos de acceso
- Cifrado

2. Asegúrese de que los sistemas, las aplicaciones, los datos y la documentación que mantienen o son procesados por terceros están suficientemente apoyadas o aseguradas de otra manera. Considere la posibilidad de requerir devolución de las copias de seguridad de terceros. Considere la posibilidad de acuerdos de depósito en garantía o depósito.

3. Definir los requisitos para el almacenamiento en sitio y en custodia externa, de los datos de copia de seguridad que cumplen con los requerimientos del negocio. Tenga en cuenta la accesibilidad necesaria para realizar copias de seguridad de datos.

4. Formación y sensibilización. Establecer un control para asegurarse que el proceso se está llevando correctamente.

5. Realizar pruebas periódicas de recuperación de backup.

Mejora continua

Para definir el proceso de mejora continua, nos basamos en el numeral 10 de la norma ISO 22301:2012 y DSS04.4 probar y revisar el BCP; el DSS04.5 Revisar, mantener y mejorar el plan de continuidad y el DSS04.8 Revisión posterior a la reanudación.
La guía fundamenta la mejora continua en:

1. Administración del cambio de la organización. Cambios importantes

de los procesos, estrategia, cambio del sector, cambio de políticas externas e internas, nueva regulación, cambios importantes a la infraestructura de tecnología, entre otros.

2. Capacitación del personal. Identificar oportunidades de mejora del plan mediante la participación activa los funcionarios de la entidad.

3. Resultados de las pruebas del plan de continuidad. Una vez ejecutadas las pruebas se definen los ítems o actividades que no se ejecutaron de acuerdo a lo planeado y los factores que contribuyeron al no cumplimiento, para definir oportunidades de mejora.

ROLES Y RESPONSABILIDADES DEL GOBIERNO Y LA GESTIÓN DE TI PARA GARANTIZAR LA CONTINUIDAD EN LA INSTITUCIÓN

Existen varios tipos de roles en la entidad, los cuales pueden ser de TI o de las diferentes áreas o dependencias, los cuales, de acuerdo al nivel de jerarquía, tienen distintos niveles de responsabilidad:

- R (responsable): La persona que está ejecutando la tarea.
- A (responsable de que se haga): Es la persona que rinde cuentas sobre el éxito de la tarea, es decir es el encargado de la correcta asignación de la misma.
- C (consultado): Es la persona que proporciona las entradas de información para la ejecución de las tareas.
- I (informado): Es la persona que recibe la información, este rol es el que recibe los entregables y/o logros de las tareas asignadas.

Las prácticas de los procesos junto con las responsabilidades y roles se especifican con base a la matriz RACI del proceso de Gestión de la Continuidad y Aseguramiento del Establecimiento y Mantenimiento del Marco de Gobierno

Matriz RACI DSS04																										
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance.				A	C	R					C					C	C	R			R	C	R		R	
DSS04.02 Mantener una estrategia de continuidad.				A	C	R					I					C	C	R	R	C	R				R	
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.					I	R									I	C	C	R	C	C	R				A	
DSS04.04 Ejercitar, probar y revisar el plan de continuidad.					I	R									I		R	R		C	R				A	
DSS04.05 Revisar, mantener y mejorar el plan de continuidad.				A	I	R					I							R		C	R				R	
DSS04.06 Proporcionar formación en el plan de continuidad.					I	R												R		R	R	R			A	
DSS04.07 Gestionar acuerdos derespaldo.																				C	A				R	
DSS04.08 Ejecutar revisiones post-reanudación.					C	R					I							R	C	C	R	R			A	

Matriz de Responsabilidades Prácticas clave del Proceso DSS04 COBIT5. Tomado de (ISACA, 2012)

Métricas

Tomando como referencia la cascada de metas de Cobit 5 se definieron las métricas por proceso, por las metas de TI relacionadas a los procesos y por las metas Corporativas alineadas a las metas de TI.

Métricas de los procesos

ÁREA	PROCESO	META	Métricas
GESTIÓN	DSS04 Gestionar la Continuidad	1. La información crítica está disponible La institución en línea con los niveles de servicio mínimos requeridos.	% de restauraciones satisfactorias y en tiempo de copias alternativas o de respaldo
			% de medios de respaldo almacenados de forma segura.
		2. Los servicios críticos tienen resiliencia.	# de sistemas críticos para el negocio no cubiertos por el plan.
		3. Las pruebas de continuidad del servicio han sido efectivas de acuerdo al BCP.	# de pruebas que han conseguido los objetivos de recuperación.
			Frecuencia de las pruebas
		4. Un plan de continuidad actualizado refleja los requisitos de actuales.	% de mejoras acordadas que han sido reflejadas en el plan.
		5. Las partes interesadas internas y externas han sido formadas en el plan de continuidad.	% de interesados internos y externos que han recibido formación.
			% de asuntos identificados que se han tratado subsecuentemente en los materiales de formación

Métricas de los Procesos. Elaborado con base a Métricas de Cobit 5

Métricas de las metas de TI de los procesos

ÁREA	PROCESO	META DE TI	Métricas
GESTIÓN	DSS04 Gestionar la Continuidad	04 riesgos de negocio relacionados con las TI gestionados	% de servicios críticos de TI cubiertos por evaluaciones de riesgos.
		07 entrega de servicios TI de acuerdo a los requisitos del negocio	% de usuarios satisfechos con la calidad de los servicios de TI entregados
		14 disponibilidad de información útil y relevante para la toma de decisiones	Nivel de satisfacción de los usuarios del negocio y disponibilidad de la información de gestión.

Métricas de las metas de TI. Elaborado con base a Métricas de Cobit 5

Métricas de las metas Corporativas con las metas de TI de los procesos

Dimensión	Metas Corporativas relacionadas con las Metas de TI	Métricas
Financiera	1. Valor para las Partes Interesadas de las Inversiones de Negocio.	% de inversiones en las que la entrega cumple con las expectativas de los interesados
	2. Cartera de productos y servicios competitivos	% de productos y servicios que alcanzan o exceden los objetivos de satisfacción al cliente
	3. Riesgos de negocio gestionados (salvaguarda de activo)	% de objetivos de negocio críticos y servicios cubiertos por gestión del riesgo
Cliente	6. Cultura de servicio orientada al cliente	# de quejas de clientes debido a incidentes relacionados con el servicio TI
	7. Continuidad y disponibilidad del servicio de negocio	# de interrupciones de servicio al cliente
	8. Respuestas ágiles a un entorno de negocio cambiante	Nivel de satisfacción del Consejo de Administración con la capacidad de respuesta corporativa a nuevos requerimientos del Estado o entidades externas.
	9. Toma estratégica de Decisiones basadas en información	Tiempo requerido para ofrecer información de apoyo que permita decisiones de negocio efectivas.
	10. Optimización de costes de entrega del servicio	Frecuencia de las evaluaciones de optimización del coste de entrega del servicio
Interna	11. Optimización de la funcionalidad de los procesos de negocio	Frecuencia de las evaluaciones de madurez de la capacidad de los procesos
	13. Programas gestionados de cambio en el negocio	Número de programas cumplidos en tiempo y en presupuesto

Métricas de las metas Corporativas alineadas a las metas de TI. Elaborado con base a Cobit 5

Modelo de madurez

El cumplimiento de los atributos del proceso predetermina el nivel de capacidad, y de ahí el nivel de madurez viene determinado por los niveles de capacidad de todos los procesos asociados.

De acuerdo al nivel de capacidad definido en el componente de Diagnóstico (6.1), el modelo define las reglas de derivación para los Niveles de madurez, basados en el sistema de evaluación de la norma ISO/IEC 155045:

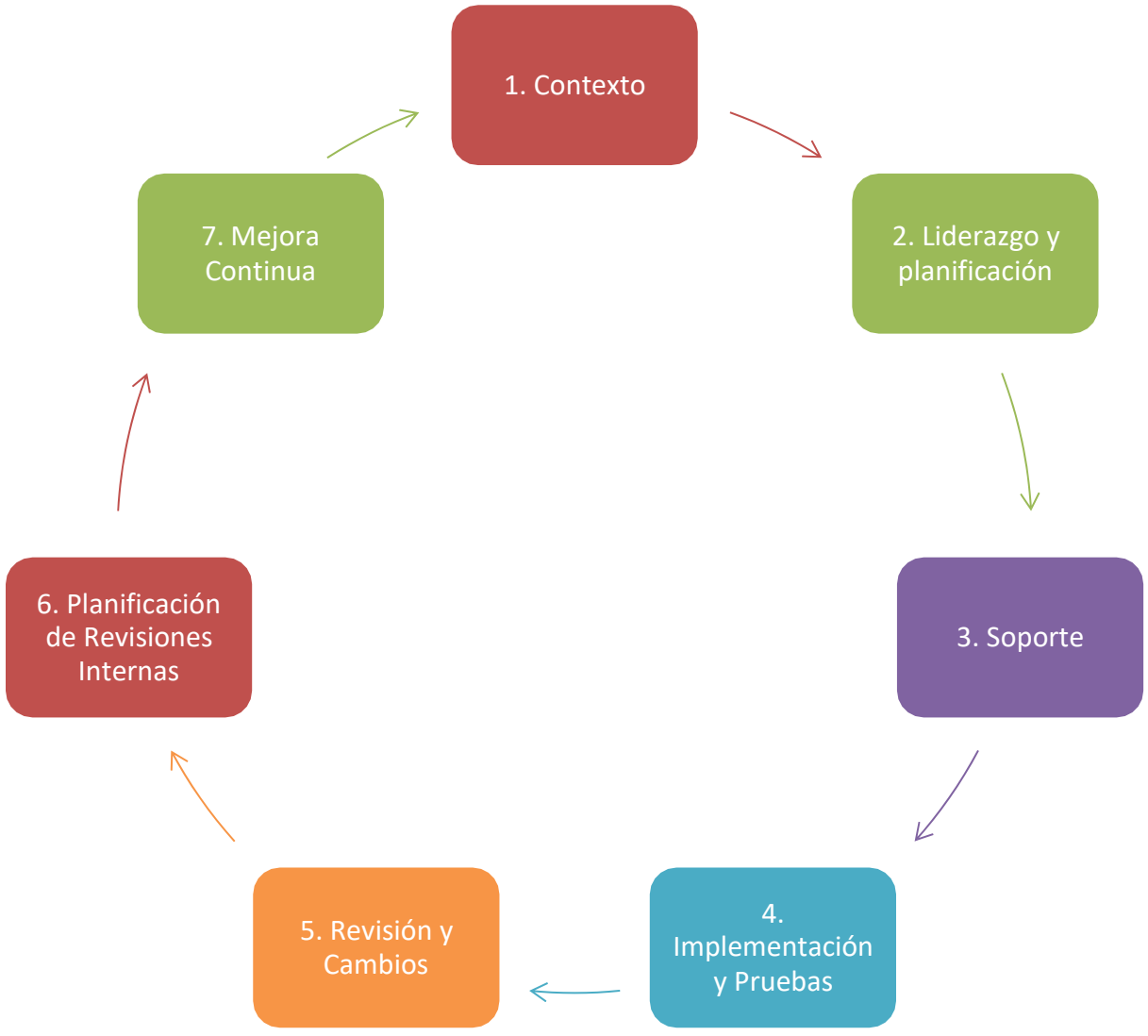
NIVEL DE MADUREZ	REGLA DE DERIVACIÓN	DESCRIPCION	CALIFICACIÓN DEL COMPONENTE (hasta)
0	La Entidad no tiene una implementación efectiva de los procesos.	**Organización inmadura.** En este nivel no se han implementado los procesos, por consiguiente, no se alcanza el propósito de la Entidad, ni se identifican productos o salidas de proceso. Por consiguiente, no hay atributos que evaluar en este nivel.	0
1	Los procesos objeto de evaluación alcanzan el nivel de capacidad 1, es decir, existen productos resultantes para los mismos y el proceso se puede identificar.	**Organización básica.** En este nivel la organización simplemente implementa y alcanza de manera básica los resultados del proceso y al alcanzar los resultados propuestos es posible identificar satisfactoriamente las salidas (resultados) del proceso evaluado.	20
2	Los procesos de nivel de	**Organización**	40

	madurez 2, tienen nivel de capacidad 2 o superior.	**gestionada**. La organización además de implementar los objetivos del proceso, demuestra una planificación, seguimiento y control tanto de los procesos, como de sus productos de trabajo asociados.	
3	Los procesos de nivel de madurez 2 y 3 tienen nivel de capacidad 3 o superior.	**Organización establecida.** En este nivel de madurez los procesos se estandarizan para toda la organización.	60
4	Uno o más de los procesos tienen nivel de capacidad 4 o superior.	**Organización predecible.** La organización gestiona cuantitativamente los procesos, es decir, se miden y se analiza el tiempo de su realización.	80
5	Uno o más procesos tienen nivel de capacidad 5.	**Organización optimizada.** Se lleva a cabo una monitorización continua de los procesos y se analizan los datos obtenidos.	100

Ilustración. Diagnóstico - Nivel de Madurez

9.1.8. Guía de implementación del modelo y caso de estudio

Teniendo en cuenta el mapeo de la norma ISO 22301 con Cobit 5, se define una guía de implantación del modelo propuesto.



Fases de la implementación del ciclo de vida. ISO 22301.

Fase	Entregables	Componente del Modelo
1. Contexto	Conocimiento de la organización ▪ Identificación de stakeholders o responsables ▪ Procesos misionales ▪ Elección del proceso crítico ▪ Estado actual y objetivo – Herramienta de Diagnóstico	0. DIAGNÓSTICO
2. Liderazgo y planificación	Política de Continuidad del Negocio ▪ Creación de equipos ▪ Propósito y Alcance ▪ Identificación de activos: Se hace valoración del activo de información y la clasificación (Componente de Gestión - Asegurar activo de información– Práctica Cobit DSS06) ▪ Identificación de Riesgos ▪ Análisis de impacto del negocio	1. PLANIFICACIÓN 4. GESTIÓN
3. Soporte	Formulación del Plan de Continuidad del Negocio Definición de fases para la activación del plan de emergencias	2. PLANIFICACIÓN
4. Implementación y pruebas	Escenarios de pruebas del Plan de Continuidad del Negocio Cronograma de pruebas Plan de capacitación	3. IMPLEMENTACIÓN 4. GESTIÓN
5. Revisión y cambios	Cambios al plan de continuidad	5. MEJORA CONTINUA

6. Planificación de revisiones internas	Cronograma de capacitación al personal Plan de respaldo o copias de seguridad	4. GESTIÓN
7. Mejora continua	Revisión del modelo y Mejora Continua	5. MEJORA CONTINUA

Contexto

Caso de estudio: instituto para la investigación y la preservación del patrimonio cultural y natural del valle del cauca (INCIVA)

INCIVA, es una entidad pública gubernamental no centralizada, que al igual que sus entidades homólogas, debe estar comprometida con la implementación de herramientas y mejores prácticas, como parte de la estrategia nacional de gobierno digital, para fortalecer su gestión administrativa y cumplimiento de los objetivos de gobierno, mediante la apropiación de las tecnologías para la seguridad y privacidad de la información en los procesos críticos, como es la gestión tributaria, la gestión financiera, presupuestal y contable y , cuyo objetivo es dotar a la entidad de recursos propios para el cumplimiento de sus metas.

Así, es preciso que se establezca un marco de gobierno que ayude a dar un enfoque a la continuidad en este proceso y se alinee con la estrategia de continuidad del negocio, aplicando guías prácticas que han sido bien aceptadas por la industria, como lo es el marco de referencia COBIT 5, que presenta y cubre aspectos fundamentales como lo es la gestión de la continuidad del negocio, cubriendo aspectos generales del Modelo de Seguridad y Privacidad de la Información del Marco de referencia de Arquitectura de TI propuesto por el Gobierno Nacional a través de la guía de preparación para la continuidad del negocio.
El marco de gobierno debe garantizar la restauración oportuna de las operaciones esenciales como son los, servicios de Portal web, Servidor de dominio, Servicio web de gestión documental, Paquete G-suite con correo institucional, servicio de espacio en la nube, administrativo y financiero SAP, Sistema para la gestión de rendición de cuentas e información contable FIRSTSOFT, Sistema de mesa de ayuda. Acceso a redes sociales para publicación, entre otros.

La falta de disponibilidad de estos servicios, causados por diferentes incidentes, y la posible pérdida de información tiene consecuencia directa en la prestación de servicios de información al usuario y entidades externas, afectando la toma de decisiones del direccionamiento estratégico y la gestión administrativa y financiera.

Información Institucional del instituto para la investigación y la preservación del patrimonio cultural y natural del valle del cauca.

Funciones

a) Promover la preservación y conservación del patrimonio histórico, natural y cultural del Departamento en colaboración con las autoridades competentes;
b) Incentivar, promover y fomentar la investigación científica del patrimonio histórico, natural, cultural y ambiental del Departamento.
c) Incentivar, promover, fomentar la investigación y el estudio para el desarrollo de la agricultura orgánica y agro biológica en el Departamento.
d) Contribuir al inventario de la biodiversidad y el patrimonio histórico y cultural existente en el Departamento y conservar, suministrar y divulgar

la información que resulte sobre ella.
e) Acopiar, suministrar y publicar información para fines del manejo, preservación, recuperación y aprovechamiento sostenible de los recursos naturales.
f) Acopiar, suministrar y publicar información sobre los recursos históricos y culturales.
g) Fomentar el desarrollo y difusión de los conocimientos y valores sobre el manejo ambiental de recursos naturales de las culturas indígenas y demás grupos étnicos.
h) Realizar estudios, investigaciones y proyectos sobre el desarrollo de tecnologías para el uso adecuado de los recursos naturales del Departamento;
i) Adelantar programas de ecoturismo que resalten los valores históricos, culturales y naturales del Departamento.
j) Fortalecer servicios de apoyo e intercambio de la investigación científica y tecnológica.
k) Celebrar convenios con Centros de Investigación, Universidades públicas y privadas, Organizaciones No Gubernamentales y Centros privados, sobre la base de formulación de programas y proyectos conjuntos relacionados con el patrimonio histórico, cultural y ambiental del Departamento.
l) Apoyar el desarrollo de tesis de grado y postgrado, pasantías e intercambios, así como la realización de cursos de educación permanente, extensión y capacitación sobre temas relacionados con sus objetivos.
m) Desarrollar investigaciones arqueológicas y etnográficas y promover la creación de museos arqueológicos y etnográficos sobre las culturas prehispánicas e indígenas que tuvieron como sede el territorio del Valle del Cauca;
n) Servir de órgano de consulta al Gobierno Departamental sobre el patrimonio cultural, histórico y natural del Valle del Cauca.
o) Servir de órgano de enlace con entidades nacionales, públicas y privadas o internacionales, que trabajen en el campo de la investigación científica de los recursos naturales y sociales y demás campos relacionados con los objetivos de la entidad.
p) Administrar y coordinar las actividades de los centros de investigación y divulgación del patrimonio cultural, histórico y natural del instituto a saber:

1. Museo de Ciencias Naturales “Federico Carlos Lehmann Valencia”, en Cali.
2. Estación Biológica “El Vínculo”, en Buga.

3. Jardín Botánico “Juan María Céspedes” en Tuluá.
4. Museo Arqueológico “Calima” en Calima Darién
5. Hacienda “El Paraíso” en El Cerrito.

Macroprocesos, principales procesos y funciones esenciales

- **Direccionamiento Estratégico:**

Macroproceso: Direccionamiento Estratégico -Crítico para la institución, la función del negocio no puede realizarse. Sus principales actividades son:

- La Dirección junto con los líderes de los procesos elaboran el Plan Estratégico de la Entidad articulado con el Plan de Desarrollo del Departamento.
- Elaborar el Plan Operativo Anual de Inversiones (POAI)
- Consolidar los planes de acción de los procesos para elaborar el informe de cumplimiento
- Dirigir y controlar los procesos administrativos junto con los líderes de proceso de investigación, mercadeo y divulgación, jurídico, Administración de recursos, Gestión Humana, Informática.
- Estudia el requerimiento para evaluar la viabilidad técnica, jurídica, financiera, social y ambiental

- **Investigación:**

Macroproceso Personal - No es crítico para la Institución, pero la operación es una parte integral del mismo. Principales actividades:

- Elaborar el Plan de Investigaciones.
- Ejecutar las fases de investigación (aplicación de método científico y protocolos)
- Analizar y procesar información primaria y secundaria.
- Escribir, evaluar artículos y remitirlos para su publicación
- Leer los artículos enviados, enviarlos a los pares para evaluación, recibir correcciones
- Elaborar guiones, reuniones técnicas, analizar la información, elaborar maquetas, simulacros.

- **Mercadeo y Divulgaciones**

Macroproceso: Personal - No es crítico para la Institución, pero la operación es una parte integral del mismo. Principales actividades:

- Elaborar Plan de Mercadeo y comunicaciones
- Gestionar, preparar y montar la exposición. Revisar y corregir contenidos.
- Realizar la asistencia Editorial: Armar la revista, hacer corrección de estilo y llevarla a imprenta para producción, y proceso de prueba y edición final y distribución por canje o donación.
- Recibir y trasladar, hacer seguimiento y dar respuesta a la PQRS.
- Producir contenido para material de divulgación.

- **Administración de recursos**

Macroproceso: Apoyo - No es crítico para la Institución, pero la operación es una parte integral del mismo. Principales actividades:

- Elaborar el proyecto de presupuesto y el PAC
- Elaborar Plan anual de Adquisiciones
- Procesar la información financiera y contable
- Hacer toma física de los bienes, elementos e insumos de la entidad en existencia
- Resumir lo que se hace durante el mes para depuración de la información contable, presentar proyecto de los ajustes contables para ser aprobados
- Rendir informes en el aplicativo RCL según calendario de la Contraloría Departamental

Elección de proceso crítico

Direccionamiento Estratégico: INCIVA es una institución Gubernamental descentralizada que interactúa de manera directa con la gobernación del valle del cauca y con el ciudadano en la prestación de servicios por medio de los centros turísticos y servicios arqueológicos, Para tal efecto requiere de ingresos

propios y envió de recursos de la gobernación por medio de convenios, para su funcionamiento, es por eso que el direccionamiento estratégico es el proceso critico en el cual se basa la relación y rendición de cuentas de la institución con la gobernación del valle y el ciudadano. Además de que los demás procesos deben dar cumplimiento de sus respectivos planes de acción por medio de indicadores de gestión al proceso de direccionamiento estratégico, que es el que elabora el Informe de cumplimiento anual.

Las aplicaciones y plataformas que apoyan El direccionamiento estratégico y los demás procesos de la Institución son:

- Portal web del INCIVA.
- Servidor de dominio para la interconectividad de los equipos de cómputo utilizados por todos los procesos de la institución
- Servicio web de gestión documental.
- Paquete G-suite con correo institucional, servicio de espacio en la nube entre otras herramientas
- Convenio de acceso con la gobernación del valle para el uso del sistema administrativo y financiero SAP
- Sistema para la gestión de rendición de cuentas e información contable FIRSTSOFT
- Sistema de mesa de ayuda para el uso de los funcionarios para el reporte y solicitudes de soporte técnico.
- Acceso a redes sociales para publicación.

Estado actual

De acuerdo a la fase preliminar del modelo, Diagnóstico, se realiza la evaluación del estado actual, con el instrumento diseñado, teniendo en cuenta el proceso crítico elegido de Direccionamiento estratégico.

Instrumento para evaluar nivel de capacidad de los procesos de un modelo de gobierno y gestión de TI para garantizar la continuidad en las Entidades Públicas tomando como Marco de Referencia de COBIT 5

			Diagnóstico Situación Actual Gobierno y Gestión de la Continuidad							
	Práctica	Descripción	Actividades	Calificación Actual	Peso Actividad	Valor Práctica	Calificación Objetivo	GAP	Nivel de Madurez del Componente	NIVEL DE MADUREZ
PLANIFICACIÓN	DSS04.01	**Definir la política de continuidad del negocio, objetivos y alcance.**	¿Se encuentran identificados los procesos de negocio internos y subcontratados y actividades de servicios que son críticos para la institución?	50	30%	21	100	79	22	GESTIONADA
			¿Están identificados los roles y responsabilidades para definir la política de continuidad?	20	30%					
			¿La política de continuidad del negocio se encuentra definida y documentada?	0	40%					

	DSS04.02	**Mantener una estrategia de continuidad.**	¿Se realiza un análisis de impacto en el negocio para evaluar el impacto en tiempo de una disrupción en funciones críticas de la institución y su efecto?	10	50%	23	100	78		
			¿Se hace algún análisis de la probabilidad de amenazas que pueden causar pérdidas de continuidad de negocio y se identifican las medidas para reducir la probabilidad y el impacto?	10	25%					
			¿Se tiene aprobación del del director o CEO para implementar las estrategias identificadas?	60	25%					
IMPLEMENTACIÓ	**DSS04.03**	**Desarrollar e implementar una respuesta a la continuidad del**	¿Se encuentran definidas las condiciones y procedimientos de recuperación que permitan la	20	50%	26	100	74	26	GESTIONADA

		negocio.	reanudación de los procesos							

			críticos de la institución?							
			¿Los proveedores clave tienen implantados planes de continuidad efectivos?	70	20%					
			¿Están definidos y documentados los recursos necesarios para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI?	10	20%					

GESTIÓN	**DSS04.06**	**Proporcionar formación en el plan de continuidad.**	¿Existen planes de formación para quienes realicen de manera continuada planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes?	20	100%	20	100	80	45	ESTABLECIDO

	DSS04.07	**Gestionar acuerdos de respaldo**	¿Se realizan copias de seguridad de los sistemas?	80	40%	59	100	41		
			¿Las aplicaciones, sistemas o datos mantenidos por terceras personas se encuentran respaldadas?	70	30%					
			¿Se realizan pruebas periódicamente de las copias de seguridad?	20	30%					
	DSS05.07	**Supervisar la infraestructura TI para detectar eventos de seguridad.**	¿Se registro de los eventos relacionados con la seguridad reportados por las herramientas de monitorización de la seguridad de la infraestructura?	50	100%	50	100	50		
	DSS06.06	**Asegurar los activos de información.**	¿Se aplican las políticas de clasificación de datos y seguridad y los procedimientos para proteger los activos de información bajo	50	100%	50	100	50		

			el control interno de la entidad?					

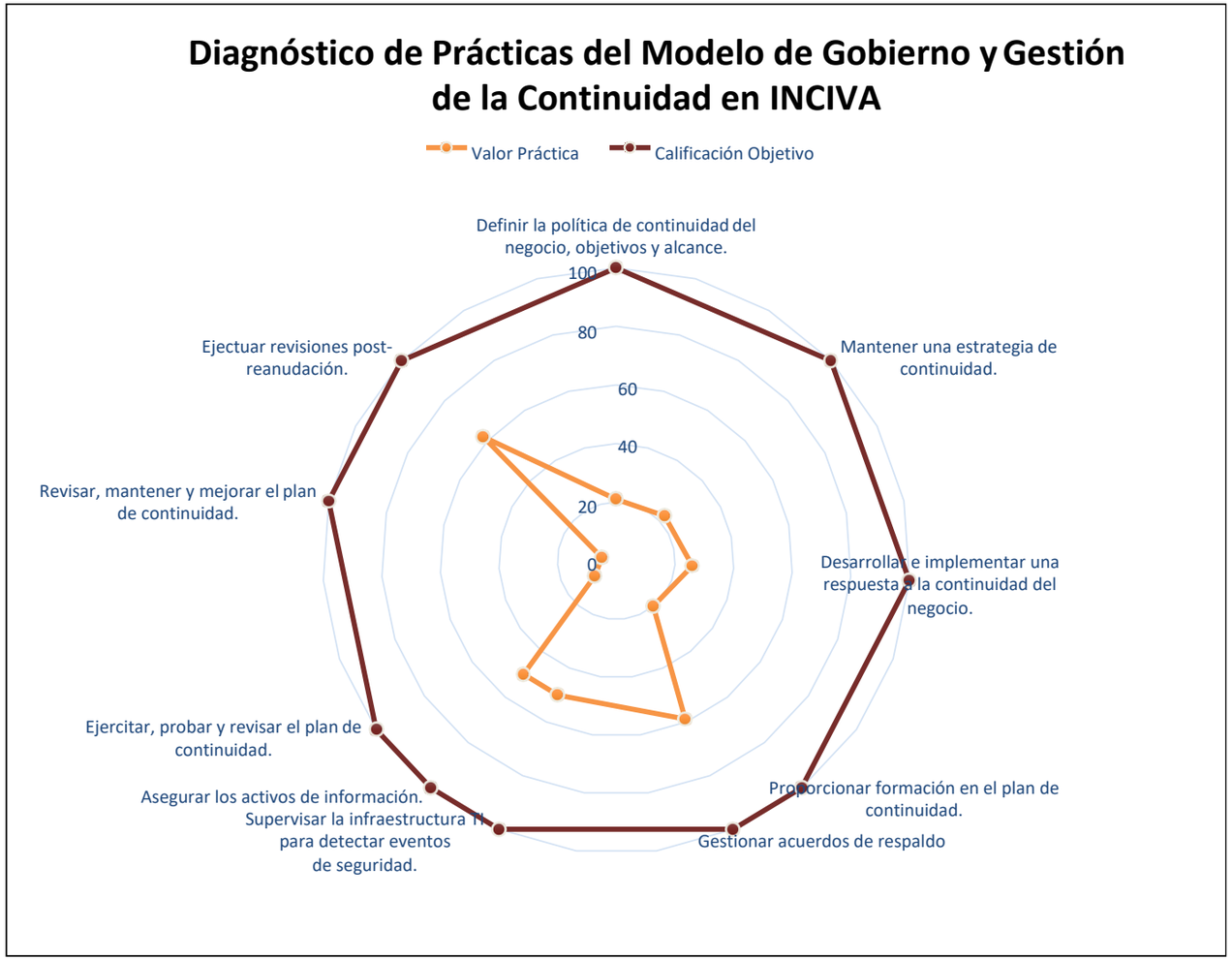
MEJORA CONTÍNUA	**DSS04.04**	**Ejercitar, probar y revisar el plan de continuidad.**	¿Se encuentran definidos los objetivos para probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio.?	10	30%	9	100	91	25	GESTIONADA
			¿Existe un procedimiento de asignación de roles y responsabilidades para realizar ejercicios y pruebas del plan de continuidad?	20	30%					
			¿Existe un plan de ejercicios y actividades de prueba, tal como está definido en el plan de continuidad?	0	40%					

	DSS04.05	**Revisar, mantener y mejorar el plan de continuidad.**	¿Se revisa el plan de continuidad regularmente teniendo en	10	50%	5	100	95		

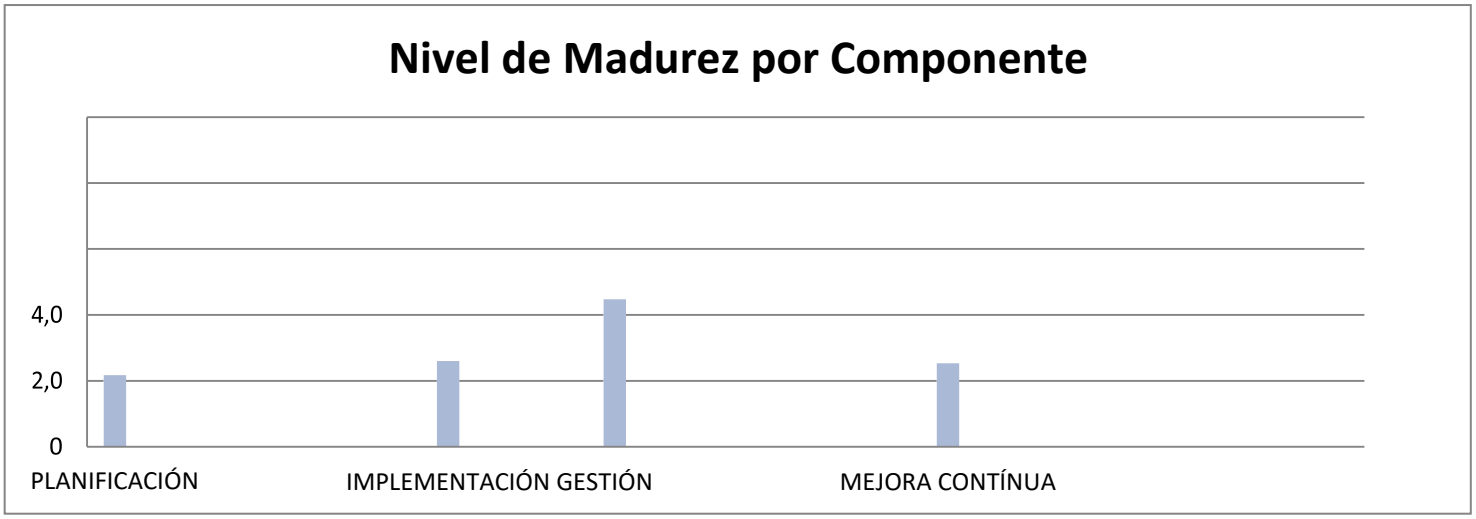
			cuenta cambios nuevos en la secretaría de hacienda, ya sea en los procesos de negocio, tecnologías, infraestructura, sistemas operativos y sistemas de aplicaciones?						
			¿Se comunican los cambios para la aprobación del Secretario de ¿Hacienda?	0	50%				
	DSS04.08	**Ejecutar revisiones post-reanudación.**	¿Existe un plan de ejercicios y actividades de prueba, tal como está definido en el plan de continuidad?	30	40%	62	100	38	
			¿Se revisa el plan de continuidad regularmente teniendo en cuenta cambios nuevos en la secretaría de hacienda, ya sea en los procesos de negocio, tecnologías,	20	50%				

			infraestructura, sistemas operativos y sistemas de							

			aplicaciones?						
			¿Se comunican los cambios para la aprobación del Director y CEO?	80	50%				
	PROMEDIO EVALUACIÓN DE PROCESOS					**32**	**100**	**68**	**29**



Diagnóstico Gestión de la Continuidad de los procesos de INCIVA.



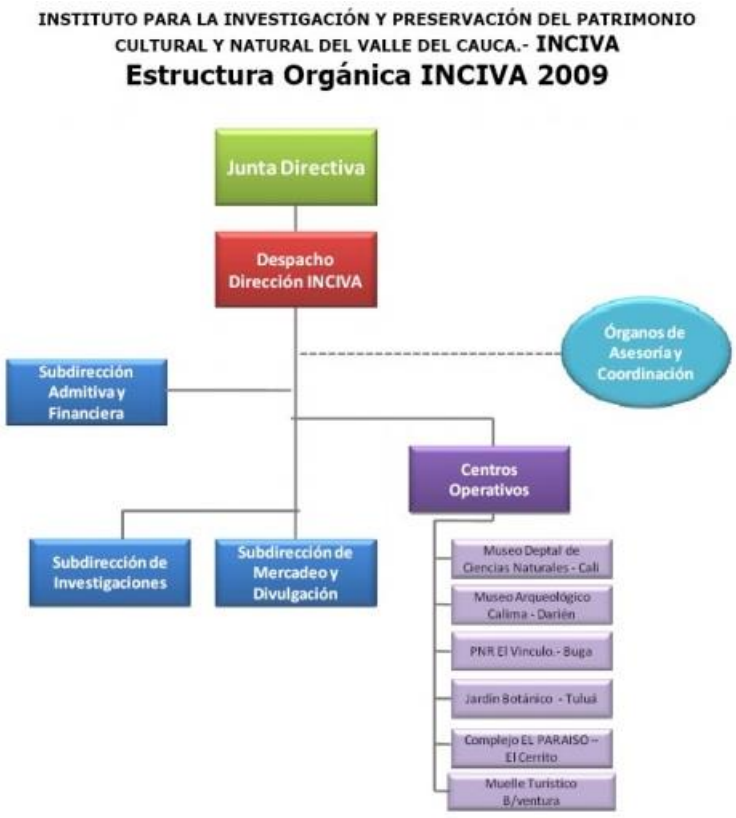
Diagnóstico por componente del modelo de Gobierno y Gestión

Para el desarrollo del componente de Seguridad y Privacidad de la Información, el Ministerio de Tecnologías de la Información y las Comunicaciones, MinTIC, ha definido la política general de seguridad y privacidad de la información y seguridad digital y continuidad de los servicios del ministerio/fondo de tecnologías de la información y las comunicaciones. (Adoptada mediante Resolución 512 de 2019).

LIDERAZGO Y PLANIFICACIÓN

Responsables de mayor nivel de la continuidad del negocio.

Organigrama INCIVA



La oficina de Apoyo de informática no se encuentra visible sin embargo maneja una labor importante con respecto a la gestión TI, donde algunas sus funciones enfocadas en la institución son:

a. Elaborar cronograma para realizar mantenimiento anual de equipos

b. Asesorar en los temas relacionados con las Tecnologías de la Información y las Comunicaciones.

c. Analizar la factibilidad y aplicabilidad de requerimientos

d. Elaborar requerimiento y estudios previos para evaluar necesidades

e. Recopilar información y compilarla para protegerla

f. Atender el llamado para corregir a la mayor brevedad el caso

g. Dar soporte para el envío de la información requerida de ley

h. Verificar si se ha materializado algún riesgo y si los controles están siendo efectivos

La oficina de Asesora de informática cuenta con el rol cuyas funciones alineadas a la institución son:

Asesor de informática
• Mantener actualizado los componentes de infraestructura y comunicaciones de la institución y coordinar su ejecución. • Establecer y verificar el cumplimiento de políticas de servicios informáticos de conectividad y seguridad para el transporte de la información • Cumplir las políticas y estándares de control de seguridad de infraestructura de comunicaciones y de acceso a datos y aplicaciones de la institución • Administrar la infraestructura tecnológica que se le asigne para garantizar la operación de los servicios de la institución. • Asesorar en la elaboración y ejecución del Plan de acción de la Dirección de Informática y Tecnología • Proponer la metodología de mantenimiento de software y hardware • Coordinar la adquisición del software que hace parte de los Sistemas de Información de la institución. • Mantener actualizado el catálogo de Servicios de Informática y Tecnología dispuestos tanto para los usuarios internos y externos
• Realizar la gestión y administración de las garantías del inventario de los equipos de escritorio, portátiles, impresoras y otros equipos informáticos a nivel de cliente y su correspondiente software • Resolver incidentes de tecnología reportados por funcionarios o usuarios externos. • Se encarga del crecimiento de la infraestructura de tecnología de información en lo que corresponde a la instalación de software, hardware, redes y seguridad informática. • recolecta información para la actualización del plan de contingencia de la entidad y hojas de vida de los equipos de cómputo y periféricos.

- **Esquema organizacional para la continuidad**

Se crea un esquema organizacional de manera que incluya los roles determinantes que intervienen en la planeación, el manejo de crisis, la respuesta, la recuperación y la logística.

- Comité de gobierno digital:

Es el comité de mayor nivel de la continuidad del negocio TI, que administra y verifica los recursos necesarios para recuperar las operaciones críticas de la institución con respecto a TI en caso de ocurrencia de una contingencia y/o emergencia, cuyo orden jerárquico es:

- Asesor de informática como representante de la alta dirección y líder de gobierno digital
- Asesor de Planeación
- Subdirector de mercadeo y divulgaciones
- Funcionario encargado de las comunicaciones, manejo de contenidos y atención a la ciudadanía
- Funcionario a cargo de archivo central
- Asesor jurídico
- Asesor de control interno como invitado permanente con voz, pero sin voto.
- Subdirector administrativo y financiero
- Subdirector de investigaciones

✓ Cuando se presente una contingencia y/o emergencia se deberá contar como mínimo, con el líder del comité o suplente y con dos integrantes.

- El Asesor de Informática es el responsable tanto de la notificación de la contingencia y/o emergencia a los medios externos e internos.

Política de continuidad

Alcance

La presente Política de Continuidad de Negocio es provisional hasta que se redacte y se apruebe una nueva política de continuidad del negocio por el comité de gobierno digital, con cumplimiento obligatorio de los procesos involucrados.

Objetivos

Mediante esta política se establece el marco para el desarrollo, implantación, revisión y mejora del plan de Continuidad del negocio en el proceso de Direccionamiento estratégico y los demás procesos de la institución, de manera que:

- Faciliten una respuesta apropiada y oportuna ante la materialización de un riesgo de seguridad o del entorno con características catastróficas, que provoquen un escenario de falta de disponibilidad de alguno de los componentes básicos de la actividad de la institución: personas, infraestructura, tecnología, información y procesos.

- Disminuir el impacto de las posibles catástrofes sobre las actividades de negocio, garantizando que se preservan las funciones esenciales y si no es el caso, que las funciones se recuperen paulatinamente.

Responsabilidades:

El Comité de gobierno digital es el responsable de impulsar el desarrollo e implantación de los Planes de Continuidad de Negocio en la institución, decidir y coordinar las actividades de continuidad de negocio, así como la revisión de esta Política. Igualmente, asume la dirección ejecutiva y la gestión de aquellas situaciones de crisis derivadas de un desastre que tengan repercusiones en toda la entidad.

Identificación de Activos

		Atributos del activo				Ubicación en	Valoración del Activo de Información				Clasificación de la Información		
Tipo	Nombre Activo	¿El activo contiene y datos personales?	¿El activo es susceptible de fraude o corrupción?	¿El activo es vital para la operación del proceso?	¿El activo es vital para la operación del INCIVA?		Confidencialidad	Integridad	Disponibilidad	Criticidad	Confidencialidad	Integridad	Disponibilidad
Datos / Información	Actas, Resoluciones y circulares y demás documentación de gestión administrativa de la institución	Si	Si	Si	Si	Gestión Documental	Alto	Alto	Alto	Crítico	Pública Reservada	Crítica	Crítica
Software	Servicio web de gestión documental	Si	Si	Si	Si	Oficina de apoyo de informática	Alto	Alto	Medio	Crítico	Pública Reservada	No Crítica	Crítica
Datos / Información	Contratos de servicios y proveedores	Si	No	Si	No	Jurídica, gestión documental	Bajo	Bajo	Bajo	No Crítico	Pública	No Crítica	No Crítica

Datos / Información	Informes de investigación, investigaciones científicas, estudios y planes arqueológicos	Si	No	Si	Si	Gestión Documental. investigación	Alto	Alto	Alto	Crítico	Pública Reservada	Crítica	Crítica

Datos / Información	Información Financiera	Si	No	Si	Si	Contabilidad, tesorería	Alto	Alto	Alto	Crítico	Pública Reservada	Crítica	Crítica
Hardware	Servidores	Si	Si	Si	Si	Oficina de apoyo de informática	Alto	Alto	Medio	Crítico	Pública Reservada	No Crítica	Crítica
Hardware	Equipos de escritorio	Si	Si	Si	Si	Oficina de apoyo de informática	Alto	Alto	Medio	Crítico	Pública Reservada	No Crítica	Crítica
Hardware	Redes de comunicación y conectividad	Si	Si	Si	Si	Oficina de apoyo de informática	Alto	Alto	Medio	Crítico	Pública Reservada	No Crítica	Crítica
Datos / Información	Base de datos de funcionarios y contratistas	Si	No	Si	Si	Gestión Humana	Bajo	Bajo	Bajo	No Crítico	Pública	No Crítica	No Crítica
Software	sistema administrativo y financiero	Si	No	Si	Si	Oficina de apoyo de informática, Admin	Alto	Alto	Medio	Crítico	Pública Reservada	No Crítica	Crítica

						recursos							

Equipos de continuidad

Equipos de emergencia:

Aun no se ha establecido equipos de continuidad, por lo tanto, la responsabilidad recae en el comité de gobierno digital para establecer equipos de continuidad, a continuación, se describirá las funciones principales de estos Equipos

Comité de gobierno Digital:

Es el comité de mayor nivel de la continuidad del negocio con respeto a TI, que administra y verifica los recursos necesarios para recuperar las operaciones críticas de la Institución en caso de que ocurrencia una contingencia y/o emergencia. Está conformado por:

- Asesor de informática como representante de la alta dirección y líder de gobierno digital
- Asesor de Planeación
- Subdirector de mercadeo y divulgaciones
- Funcionario encargado de las comunicaciones, manejo de contenidos y atención a la ciudadanía
- Funcionario a cargo de archivo central
- Asesor jurídico
- Asesor de control interno como invitado permanente con voz, pero sin voto.
- Subdirector administrativo y financiero
- Subdirector de investigaciones

Equipo de Planeación:

Equipo responsable de elaborar el plan para la recuperación de desastres (DRP), el cual define las actividades de respuesta y el uso de los recursos durante una emergencia. Los miembros que conforman el equipo de planeación son: Un funcionario delegado de las subdirecciones y funcionario de la oficina de planeación. El equipo se complementa con la Oficina de Control Interno.

Equipo de Respuesta:

Equipo responsable de dar respuesta, evaluar los daños y estabilizar la situación después de un escenario de contingencia y/o emergencia en la institución. Los miembros que conforman el equipo de Respuesta son:

- Funcionario, responsable de la vigilancia
- Funcionario de la Oficina de apoyo de informática, responsable del mantenimiento de planta y equipo y la gestión de la conectividad
- Brigada de emergencia, para primeros auxilios, incendio, evacuación y apoyo externo, conformado por funcionarios estratégicamente seleccionados por la ubicación de sus oficinas.

Equipo de Recuperación y Operación:

Equipo responsable de restablecer los procesos u operaciones críticas de la institución, teniendo en cuenta los tiempos de recuperación objetivo, la secuencia de recuperación y la información requerida por cada proceso para garantizar la continuidad.

Los miembros que conforman el equipo de Recuperación y Operación son:

- ✓ Funcionario de dirección estratégica
- ✓ Subdirector de administración de recursos
- ✓ Funcionario de Presupuesto
- ✓ Funcionario de Contabilidad
- ✓ Funcionario de Tesorería.

Equipo Logístico y de Soporte:

Equipo responsable de dar soporte administrativo y tecnológico al equipo de la Sección de Recuperación, de manera que se faciliten las labores de planeación, recuperación y retorno a la operación normal. Igualmente es responsable de facilitar la comunicación con el personal.

Los miembros que conforman el equipo logístico son:

- o Funcionarios de la oficina de Apoyo de informática para la gestión de la infraestructura tecnológica, la gestión de la conectividad y la gestión de soporte
- o Funcionario encargado de las comunicaciones, manejo de contenidos y atención a la ciudadanía
- o Funcionarios responsables de archivo físico y administración de bienes.

Identificación de riesgos

Es importante identificar escenarios de riesgos de la continuidad del negocio para hacer un análisis de impacto.

Escenarios

Algunos escenarios que pueden presentarse en la institución,

impactando en la continuidad son:

Id	Escenario	Descripción
E1	Fallo de Infraestructura de red	Fallo o daño en cualquier dispositivo de infraestructura de red (Routers, Switch) debido a: 1. Cruce entre hilos (mala conexión) 2. Ruptura de los cables 3. Ruido o estática
E2	Fallo de servidores	Fallo o daño en los servidores tanto de dominio, como de gestión documental. Puede ser causado por intervención humana o falla del dispositivo.
E3	Interrupción del fluido eléctrico	Fallas eléctricas debido a tormenta eléctrica que puede producir un corto circuito originando un apagón o un incendio
E4	Denegación del servicio o falla del sistema administrativo y financiero.	Falla de acceso de servicio del sistema administrativo y financiero puede darse por caída el mismo sistema o por falla de los equipos de cómputo o servidores ya que el sistema se trabaja de manera local.

Procedimiento de identificación de riesgos

Identificación de Riesgos	
R1	Impacto en la integridad de las personas debido a incendio en las instalaciones.
R2	Impacto en la continuidad de los servicios debido a fallas por falta de disponibilidad y contingencia de la infraestructura tecnológica
R3	Impacto en la confidencialidad debido a las vulnerabilidades detectadas en la infraestructura tecnológica
R4	Impacto en la imagen debido a fuga de información confidencial por parte del personal
R5	Impacto en la imagen debido a la no detección oportuna de errores contables o financieros
R6	Impacto financiero debido a la vulnerabilidad de la infraestructura de TI

Controles Existentes	
C1	Plan de evacuación y Sistema contra incendios instalado.
C2	Diseño de esquema de equipos auxiliares e información en la nube
C3	Tercerización de la fuerza de trabajo de TI
C4	Implementación de prácticas de desarrollo en tiempo real
C5	Protocolos y mecanismo de análisis de irregularidades contables o financieras
C6	Centralización de la información generada por los diferentes centros

Análisis de Impacto del Negocio.

Se definen las tablas de impacto y se aplican a los riesgos identificados para hacer el cálculo del Riesgo de exposición y residual en la institución

Definición de impactos:

Tabla de impacto Rangos acumulados de pérdidas en Millones de pesos (Tangible):

Determinada por un valor promedio de la infraestructura actual de la institución, que si se deja de percibir tendría consecuencias financieras para la misma.

Score	Rango de pérdida financiera
0	Ninguna
1	< $10
2	≥ $10 < $40
3	≥ $41< $60
4	≥ $61< $80
5	≥ $81

Impacto acumulado por días usando la tabla de pérdida financiera:						
Categoría	1	3	5	10	20	30
Pérdida Financiera	1	2	3	3	4	5

Tabla de impacto en la Continuidad de los servicios:

La oficina de informática salvaguarda la información diariamente.
La máxima cantidad de tiempo tolerable requerido para verificar integridad de los datos y los sistemas es de 12 horas.

Tiempo máximo tolerable (MTD): 4 días = 96 horas
Tiempo de recuperación objetivo (RTO): 1 día = 24 horas
Tiempo de trabajo de recuperación (WRT): ½ día = 12 horas
Punto de recuperación objetivo (RPO): 1 día = 24 horas

Impacto en la continuidad de los servicios de TI

5 48 a 96 horas

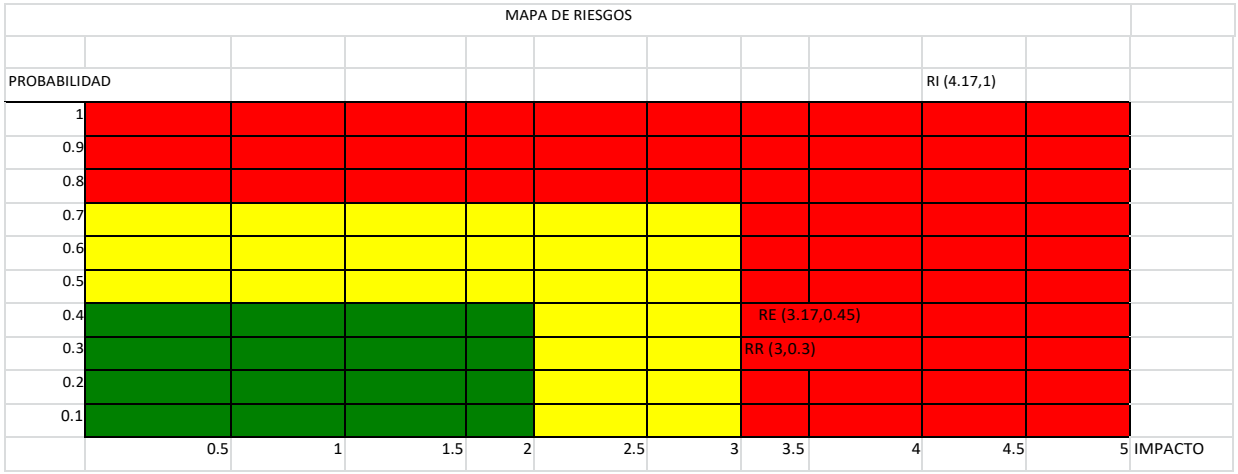
	RIESGO INHERENTE		CONTROLES EXISTENTES	RIESGO DE EXPOSICIÓN		CONTROLES PROPUESTOS	RIESGO RESIDUAL	
RIESGO	IMPACTO	PROBABILIDAD		IMPACTO	PROBABILIDAD		IMPACTO	PROBABILIDAD
R1	5	1	C1	3	0.5		3	0.5
R2	4	1	C2	2	0.3	CP2	1	0.2
R3	5	1	C3, C4	3	0.8	CP3	3	0.5
R4	5	1	C1, C5	5	0.5	CP1	5	0.2
R5	3	1	C5, C6, C7, C8	3	0.2		3	0.2
R6	3	1	C3, C4	3	0.4	CP2	3	0.2
TOTAL	4.17			1.47			0.90	
PROMEDIO	4.17	1.00		3.17	0.45		3.00	0.30

4 24 a 48 horas
3 12 a 24 horas
2 1 a 12 horas
1 menos de 1 hora

Tablas finales de valoración de impactos

Impacto Pérdida Financiera en Millones de pesos		Impacto en la continuidad de los servicios de TI		Impacto en la integridad de las personas	
5	>=81	5	48 a 96 horas	5	Crítico
4	>=61 < 80	4	24 a 48 horas	4	Importante
3	>=41 < 60	3	12 a 24 horas	3	Moderado
2	>=11 < 40	2	1 a 12 horas	2	Tolerable
1	< 10	1	Menos de 1 hora	1	Leve

Controles Propuestos	
CP1	Acuerdos de confidencialidad con pólizas de cumplimiento
CP2	Implementación de una infraestructura de alta disponibilidad y contingencia
CP3	Implementación de mejores prácticas de COBIT



Soporte

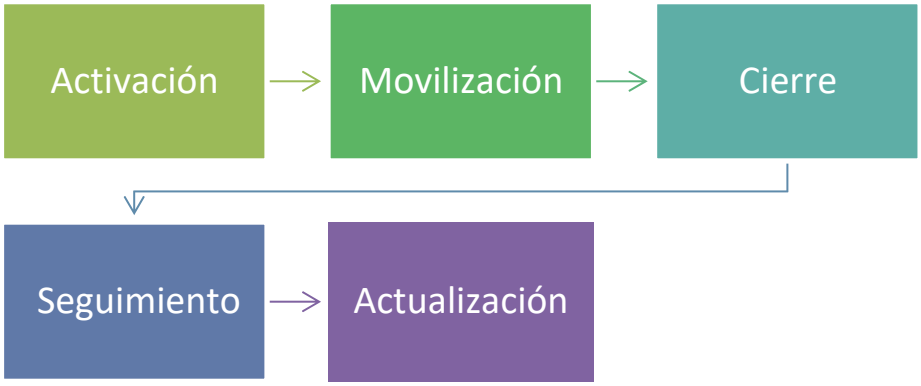
Se formula el plan de continuidad cuyo objetivo es Salvaguardar la información financiera, administrativa y de gestión para garantizar la disponibilidad de la misma.

A continuación de define la matriz RACI en donde se definan las actividades y equipos de continuidad que deberá intervenir, así como el rol (intercepción fila-columna) de cada área en la prevención, respuesta y recuperación ante la materialización del riesgo crítico con mayor impacto y probabilidad:

Denegación del servicio administrativo y financiero, información crítica, servicios en la nube, gestión documental y equipos de cómputo.		Roles / Responsabilidades						
ID	Actividad	comité de gobierno digital	Equipo logístico	Equipo Respuesta	Equipo de recuperación	Oficina de Apoyo de informática	Sub Dirección Admin. de recursos	Equipo de Planeación
1	Aviso desde área administrativa para indicar la interrupción del servicio	A	I	I	I	I	R	I
2	Monitoreo del tráfico de red y revisión de estado de servidor	I	I	I	I	R	I	I
3	Reportar diagnóstico de Denegación del Servicio	A	I	I	I	R	R	I
4	Evaluar el diagnóstico y activar Plan de continuidad	A	I	I	I	R	C	I
5	Notificar al personal de Sistemas de activar plan de recuperación de acuerdo al escenario de Denegación de servicio	RA	I	R	R	I	I	I
6	Iniciar Plan local	C	I	I	A	R	I	I
7	Iniciar el Plan de recuperación del servicio (Servidor de respaldo)	A	I	I	R	R	I	I
8	Levantar el servicio - Mitigar el riesgo de denegación del servicio en el sistema	C	I	I	RA	R	I	I

10	Documentar incidente y actualizar el Plan de continuidad	A	I	I	C	C	I	R

Fases para la operación del plan de continuidad



Se define las fases para ejecutar plan de continuidad:

Activación

Con el fin de establecer los lineamientos para gestionar una comunicación efectiva y controlada para la activación de una emergencia de impacto al interior de la institución se define un protocolo de Comunicación.

Movilización

Con el objetivo de minimizar el impacto de las operaciones, se toma como instalación las zonas y oficinas del primer y segundo piso que poseen cierta infraestructura suficiente y presentan menor riesgo de incendio y remoción dado el caso que esta zona está cerca de las salidas de emergencia llegado a necesitarse evacuación

Operación

Con el propósito de responder exitosa y oportunamente ante eventos de interrupción de los servicios la institución de identificar sus operaciones críticas.

Desmovilización

la institución una vez concluya la operación, cuya notificación la hará el equipo logístico, realizará un análisis y evaluación del resultado del desempeño de las labores ejecutadas, basados en la documentación generada. Una vez se confirma el cierre del plan alterno, un representante de cada Subdirección hace entrega de los elementos y recursos asignados durante la emergencia.

Cierre

Finalizada la emergencia, se activa una nueva cadena de comunicación, siguiendo esquemas de comunicación, para informar la situación y las acciones a seguir para retornar a la normalidad, adicionalmente los miembros del Equipo de Recuperación deben generar un informe de trabajo en Contingencia, donde se citen los resultados obtenidos y los problemas presentados, para retroalimentar a los directivos de la institución.

Seguimiento

El plan de continuidad será monitoreado mediante un proceso sistemático, independiente y documentado por medio de una auditoría interna, cuya finalidad es realizar un examen objetivo e independiente de los procesos, procedimientos, actividades y operaciones que lo soportan, para formular recomendaciones. La coordinación para la ejecución de la auditoría está a cargo la Oficina de Control Interno.

Actualización

El documento del plan de continuidad será revisado como mínimo 1 vez al año con los responsables y participantes de las diferentes dependencias, para identificar y realizar los ajustes.

Implementación y pruebas

Se define el plan de pruebas del Plan de Continuidad (roles, tareas, etc). En el cual se indica una actividad de pruebas simulada donde se propone un plan óptimo para realizar dicha simulación

Procedimiento de plan de prueba. TIPO SIMULACIÓN.

- ✓ Proceso: Administración de Recursos
- ✓ Escenario: *Denegación del servicio administrativo y financiero*.
- ✓ Activos involucrados:
  - 1 servidor de pruebas con *el sistema administrativo y financiero*
  - 3 equipos clientes
  - Equipos de conectividad de la red de la entidad
  - Back up restaurado del *sistema administrativo y financiero*
- ✓ Periodicidad: Una vez al año
- ✓ Participantes:
  - Líder del comité de gobierno digital
  - Equipo de la oficina de informática
  - Representante de dirección estratégica
  - Funcionarios y usuarios que usan el *sistema administrativo y financiero*
  - Sub director de Administración de recursos

Id	Descripción de la actividad
1	EL Asesor de informática quien es el líder del comité de gobierno se debe reunir con el Director, el área de administración de recursos y sus respectivos miembros. Una vez reunidos se les entrega copia de los procedimientos pertinentes a cada miembro y se le instruye sobre el alcance y los objetivos de la prueba a realizar.
2	El Asesor de informática da inicio de la prueba.
3	Se inicia la prestación del servicio.
4	El equipo de informática monitorea el tráfico de red y mediante herramienta de software

	simula un ataque de Denegación de servicio sobre la plataforma donde se aloja el *Sistema administrativo y financiero*
5	Después de 5 minutos de interrupción, los usuarios del sistema, reportan al área de informática de la situación.
6	El equipo de informática realiza medición del tráfico de red y revisión de estado de servidor. Reporta el diagnóstico de Denegación del Servicio al Asesor de informática.
7	El Asesor de informática evalúa el diagnóstico y toma decisión de notificar al comité, Líderes de equipo del área y activar plan de continuidad de acuerdo al escenario de Denegación de servicio. Por parte de informática restablecer la información de un backup previamente respaldado y ejecutándolo sobre el servidor para garantizar que la información consultada una vez superada la falla es la más actualizada posible. Por parte del personal del área de Admin recursos, activan el Plan papel que consiste en usar formatos manuales donde se registra la información necesaria para ser luego registrada en el sistema una vez superada la falla, por medio de notas de calidad donde se especifique la extemporaneidad de la información.
8	El Asesor de informática inicia el Plan de recuperación restaurando la información del servidor
9	Al mismo tiempo se el equipo de la oficina de informática realiza medición de los tiempos de detección y respuesta.
10	El Asesor de informática da por terminada la prueba y debe generar un informe de lo relevante encontrado en esta prueba y debe anexar este documento al Al plan de continuidad del negocio (BCP) y proceder a su actualización.

Revisión y cambios

En esta fase se debe evaluar si el plan de continuidad es efectivo cuando se realizan las pruebas. En caso de que no se cumpla con el procedimiento o se altere, se debe actualizar el plan.

Para el caso de estudio se debe tener especial cuidado en la actualización del procedimiento de Análisis de Impacto del Negocio de acuerdo a la identificación de nuevos riesgos y amenazas ya que es fundamental para el desarrollo y procedimiento de la gestión de la continuidad.

La prueba es liderada por la oficina de Apoyo de informática y debe contar con aprobación del comité de gobierno digital.

Planificación de revisiones internas

Se identifican y describen el plan de entrenamiento para el personal involucrado (frecuencia y mecanismo utilizado)

Entrenamiento	Frecuencia
Capacitaciones de tipo recorrido del Plan de Continuidad con el fin de comprobar la efectividad del plan y revisar roles y responsabilidades	Una vez al año
Simulacro de escenarios	Una vez al año
Campañas con slogans y emails para concientizar al personal de los posibles escenarios de riesgo	Cada 2 meses

Para lograr retroalimentación, se debe habilitar una dirección de correo electrónico, donde se consiga dirigir las sugerencias, en cuanto a las gestiones realizadas que vayan surgiendo por parte de los usuarios críticos.	Permanente

Igualmente se define el plan de copias de respaldo de la información del proceso seleccionado (tipo, periodicidad, medio, tiempo de retención, custodia).

Tipo	Método	Periodicidad	Medio	Tiempo retención	Custodia
Completo	Automático	Semanal	Disco/Nube	1 año	Oficina de informática/Proveedor
Incremental	Automático	Diario	Disco	1 año	Oficina de informática

✓ Se tienen datos personales de nivel medio-alto y de acuerdo a política de seguridad, se debe tener respaldos en la nube.

✓ Se las pruebas de respaldo deben hacerse cada 2 meses.

Revisión del modelo y mejora continua

Se debe seguir el procedimiento:

- Aplicar los controles propuestos en la identificación de riesgos.
- Análisis de la brecha del estado actual con respecto al anterior análisis con la herramienta del componente de Diagnóstico.
- De acuerdo a la evaluación resultante, hacer revisión y actualización del modelo de gobierno si se requiere.
- Se elige el proceso crítico a evaluar para implementar el modelo.
- Revisar el presupuesto de continuidad.

Fase	Observaciones	Oportunidades de Mejora
1. Contexto	No Existe un Plan estratégico de TI aparte del plan estratégico de la institución.	El plan estratégico de TI está enfocado a mantenimiento y soporte y debe ser alineado a la estrategia del negocio.
	Existe un presupuesto aprobado de TI en el rubro Fortalecimiento Institucional.	
	Se tienen definidos roles del personal de la oficina de Apoyo de informática.	Diseñar, aplicar y mantener actualizado el plan de continuidad para procesos críticos como es la gestión tributaria
	Existen políticas de seguridad documentados y política de privacidad y protección de datos dentro de la ejecución actual de implementación del sistema de gestión de seguridad informática de acuerdo a los lineamientos del Modelo de Seguridad y Privacidad de MinTIC.	Hacer plan de pruebas del respaldo de información.
		Los procesos evaluados en la institución obtuvieron como resultados un nivel de madurez del 29% en su estado inicial, un nivel Gestionado que implica que las actividades se están monitoreando. Sin embargo, es necesario que se documente toda la gestión.
	No Existen manuales de entrenamiento de los sistemas de información.	
	Existen acuerdos de niveles de servicio	
	Se realiza mantenimiento preventivo de la infraestructura de TI	
	Los procesos cuentan con sistemas de información estables. Cuentan con un sistema Administrativo y Financiero que integra todos los módulos de gestión. Además, de una res de dominio que intercomunica todas las áreas y con web services de soporte y gestión documental	

	Los procesos no están identificados según su nivel de criticidad

2. Liderazgo y planificación	Se tienen identificados riesgos de TI	Dentro de la política de seguridad que están desarrollando se debe incluir los controles de continuidad del negocio de cada proceso de la institución incluyendo cada área.
	Los equipos de emergencia y continuidad son escasos y no están asignados oficialmente	Gestionar los riesgos.
	Se tienen identificado activos tecnológicos	Se debe actualizar la identificación de nuevas amenazas y vulnerabilidades dentro del análisis de impacto del negocio
	Existe una valoración y clasificación del activo de información.	
3. Soporte	No existe un procedimiento para la activación de un plan de continuidad.	Desarrollar e implementar la gestión de la continuidad que contemple el plan con roles y responsabilidades que involucre a la dirección estratégica de la institución
	No existe un documento formal de gestión de la continuidad	
4. Implementación y pruebas	No se realizan pruebas de incidentes que puedan provocar una interrupción de los servicios de TI dentro de la institución.	Incluir dentro de la gestión de la continuidad de los servicios TI dentro de la institución, el escenario de pruebas, y teniendo en cuenta la necesidad de capacitaciones para el personal encargado de ejecutarlas
	El personal es capacitado periódicamente en temas de seguridad informática.	

5. Revisión y cambios	Es necesario un plan estratégico meramente orientado a TI de acuerdo a los nuevos requerimientos de operación y mantenimiento actuales.	Incluir dentro del plan estratégico de la institución la implementación del modelo de gobierno y gestión de TI para garantizar la continuidad de los servicios de TI.

6. Planificación de revisiones internas	El personal es capacitado en lineamientos de la estrategia Gobierno digital, que incluye Modelo de Seguridad y Privacidad	Diseñar un cronograma de capacitación enfocado a la Guía de elaboración de Continuidad del Negocio de MinTIC.
	Se realizan copias de respaldo de las bases de datos con periodicidad, aunque no se realizan copias del funcionamiento del respaldo	Diseñar cronograma de pruebas del respaldo dentro del modelo de gobierno y gestión, componente de Gestión.
		Desarrollar e implementar Programa de concientización y entrenamiento del Plan de Continuidad.
7. Mejora continua		Coordinar y aprobar la definición de requerimientos, para los procesos tendientes a la adquisición o contratación de recursos técnicos y tecnológicos de las TIC.
	Existe compromiso y disposición de la institución para mantener dentro de su estrategia el componente tecnológico para lograr las metas de gobierno.	Crear comité de continuidad involucrando a la alta dirección y oficializarla por medio de Resolución o documento administrativo el responsable de la entidad, en este caso el director de la institución. El modelo es flexible y puede replicarse

Conclusiones

La gestión de la continuidad es la herramienta que las organizaciones deben implementar, para mantener sus operaciones y desarrollar la resiliencia frente a eventos disruptivos. Esta gestión debe estar alineada a los objetivos del negocio para que efectivamente se haga la entrega de los beneficios a los stakeholders, en el caso de las Entidades públicas, principalmente a los ciudadanos.

La aplicación de frameworks que involucran gobierno y gestión de TI, como lo es Cobit 5, hace que se mire la organización desde la perspectiva de la cascada de metas lo que facilita la identificación y alineación de los objetivos de TI con los objetivos del negocio y por ende se pueden implementar procesos y gestionar proyectos de manera efectiva apuntando siempre a las necesidades de la alta dirección.

Las políticas con respecto a la recuperación después de una emergencia deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y cumplimiento. El hecho de gestionar un plan de continuidad del negocio en entidades territoriales no implica un reconocimiento de la ineficiencia en la gestión de la empresa, sino todo lo contrario, supone un importante avance a la hora de superar todas aquellas situaciones descritas y que pueden provocar grandes pérdidas, no solo materiales si no aquellas derivadas de la paralización del negocio durante un período más o menos largo. Además, el modelo cubre una práctica importante dentro del Modelo de Seguridad y Privacidad de la Información – MSPI - del Marco de Referencia Arquitectura Ti de MinTIC, el cual debe estar con el máximo cumplimiento dentro de tres años.

El modelo propuesto se alinea al MSPI en todos sus componentes por lo que las entidades pueden contar con algo más que la guía de elaboración del Plan de continuidad de manera que la gestión sea controlada y comprometida por la alta dirección. Esto es lo que realmente hace efectivo una gestión de continuidad en las entidades públicas.

El modelo de gobierno y gestión propuesto tiene diferentes niveles de complejidad y flexibilidad según las necesidades y características de la Institución. Igualmente, no contempla todos los escenarios y los recursos suficientes para estar totalmente preparados, por tal razón es de vital importancia que el proceso deba ser paulatino e ir evolucionando según el contexto, resaltando la fase preliminar de Diagnóstico y la Fase de Mejora Continua para la actualización del modelo de gobierno y gestión de la continuidad. El monitoreo y revisiones de las acciones es esencial para asegurar se estén llevando a cabo eficazmente. Además, permite evidenciar los factores que pueden estar afectando negativamente la aplicación de controles.

La probabilidad que las amenazas externas, como efectos climáticos, se materialicen se minimizará diseñando y aplicando planes de emergencias de acuerdo a las fases especificadas en la guía de implementación.

La aplicación del modelo de gobierno y gestión de TI para garantizar la continuidad de la institución permitirá a la entidad estar preparados para identificar las posibles situaciones de disrupción y emergencia, los procedimientos para hacerles frente, las actualizaciones de dichos procedimientos y las alternativas disponibles.

Lineamientos para el buen uso de las tecnologías de la información y la comunicación

Objetivo

Estructurar la base de los lineamientos básicos de la distribución, funcionamiento y uso de las tecnologías de la información y la comunicación-TIC, para el instituto para la Investigación y la Preservación Del Patrimonio Cultural y Natural del Valle del Cauca INCIVA, y alinear el uso eficiente y eficaz de las herramientas asignadas a los integrantes de la red y funcionarios de la institución.

Alcance

Los presentes lineamientos son aplicables a todos los integrantes de la red institucional y funcionarios de la entidad, responsables de cada uno de los recursos TIC que se le asigne o que le sean asignados, de acuerdo a la disponibilidad de equipos que tenga la institución, como herramienta para comunicación interna, el trabajo ofimático, gestión de recursos entre otras ocupaciones exclusivas de la institución.

Definiciones

Computador portátil: "Una computadora portátil, ordenador portátil o computador portátil, es un dispositivo informático que se puede mover o transportar con relativa facilidad. Los ordenadores portátiles son capaces de realizar la mayor parte de las tareas que realizan los ordenadores de escritorio, también llamados «de torre», o simplemente PC, con similares capacidades y con la ventaja de su peso y tamaño reducidos; ello sumado también a que tienen la capacidad de operar por un período determinado sin estar conectadas a una red eléctrica por medio de baterías recargables".

Disponibilidad: Se refiere a la presencia de una persona, durante el horario de oficina de lunes a viernes, para gestionar y comunicar oportunamente, un requerimiento o una incidencia a los actores de la oficina de informática. También hace referencia a la existencia de herramientas TIC libres para uso de necesidad o contingencia.

Dispositivo móvil: Un dispositivo móvil es un aparato de tamaño pequeño, que posee algunas capacidades de procesamiento, conexión a una red, memoria limitada, dentro de los cuales se encuentran los teléfonos inteligentes, las tabletas, entre otros.

Herramientas Tic: Son herramientas de las tecnologías de la información y de comunicaciones, que consta de equipos de programas informáticos y medios de comunicación para medir, reunir, almacenar, procesar, transmitir y presentar información en cualquier formato, es decir voz, datos, texto o imágenes.

Mesa De ayuda: es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados con las Tecnologías de la Información y la Comunicación (TIC)

Actores de los sistemas de información e integrantes de la red institucional.

Son todos aquellos profesionales funcionarios y/o contratistas a quienes se les asignan herramientas TIC y/o hacen parte de la institución que laboran en las siguientes áreas o cargos:

- Dirección
- Sub Dirección Administrativa y Financiera
- Sub Dirección de Investigaciones
- Sub Dirección de mercadeo y divulgaciones
- Secretaría
- Planeación
- Banco de Proyectos
- Jurídica
- Tesorería
- Gestión humana
- Contabilidad
- Almacén
- Control Interno
- Ventanilla Única

- Gestión Documental
- Botánica
- Arqueología
- Zoología
- Taxidermia
- Informática
- Coordinación Museo de Museo de ciencias Naturales
- Coordinación Parque regional El Vinculo
- Coordinación Museo Arqueológico Calima
- Coordinación Jardín Botánico Juan María Céspedes
- Coordinación Hacienda El Paraíso.

Lineamientos generales

Medios de contacto con la mesa de ayuda

La comunicación con la mesa de ayuda del INCIVA se realiza a través de las siguientes opciones;

- Web services de mesa de ayuda: por medio de la dirección web, http://helpdesk.INCIVA.gov.co:81/ , se puede realizar el reporte de una incidencia o requerimiento técnico o de soporte con solicitud descrita y opcionalmente, fotos o capturas de pantalla. El cual será revisado y atendido por el personal de la oficina de informática.

- Correo electrónico sistemas@INCIVA.gov.co, de igual manera como se reporta incidencias o requerimientos al webservices, también se puede hacer de manera escrita al correo electrónico, también se puede usar en el momento que requiera reportar un daño técnico, robo, pérdida, hurto que le ocurra a cualquiera de las herramientas TIC proporcionadas por la institución.

- Teléfono 5146848 Ext 128, las peticiones, incidencias y requerimientos pueden ser atendidos de manera verbal en línea telefónica, solo cuando previamente también se ha reportado en el web services, para su posterior registro y seguimiento, la línea telefónica se puede usar para dar explicaciones más detalladas y de pronto seguimiento.

Asignación de herramienta TIC (dispositivos móviles, computadores portátiles, correo institucional, etc.).

La Asignación para las nuevas herramientas TIC, serán responsabilidad de la Dirección de INCIVA o a quien esta delegue, atendiendo a las necesidades de los funcionarios o aquellos que la soliciten por medio de un requerimiento, del cual primero se someterá a un análisis presupuestal antes de ser aprobado.

La responsabilidad de la asignación de herramientas TIC ya disponibles, en la institución, estará a cargo del asesor de informática el cual decidirá dependiendo de las necesidades de la red a la disponibilidad de equipos con que se cuente, (computadores de escritorio, portátiles, routers, etc) autorizado previamente por el director o a quien se delegue.

Directorio de funcionarios

Los integrantes de la red del INCIVA, deben mantener actualizada su información como servidores públicos ya que ellos son los que administran y operan los equipos mencionados, informando las novedades que se presenten, a través del correo electrónico sistemas@INCIVA.gov.co, en caso de contingencia, al correo: Divulgacion@INCIVA.gov.co

La información de los integrantes de la red, se actualizará el listado en la página web:
https://www.INCIVA.gov.co/institucion/directorio-funcionarios

Tenencia e inventario

Todos los integrantes de la red, deben garantizar la tenencia, administración y buen uso de los equipos asignados por la institución,

hasta el momento en que el usuario ya no pertenezca a la institución y se le solicite su devolución.

El servidor público, debe mantener en óptimas condiciones técnicas y de uso los dispositivos que le sean asignados, destinando su servicio exclusivamente para las actividades que son propias de la institución

Los dispositivos deben estar siempre disponibles, en caso de que los servidores públicos se ausenten de la institución por cualquier motivo (vacaciones, licencias, entre otros), deben asignar el equipo a la persona que queda a cargo del área o puesto de trabajo, y de todas las actividades inherentes a la red de la institución.

La oficina de informática deberá ser informada y preverá cuando un funcionario responsable de un equipo se desvincule de la entidad, también velará de que devuelva el equipo en las condiciones en que se le entregó, el cual podrá ser reasignado a otra persona que realizará la misma actividad que se venía desempeñando.

Daño de equipo

Daño de equipo por defectos de fábrica, fallas técnicas u otras no atribuibles al usuario:

En este caso, los usuarios de la institución deberán hacer directamente el reporte a la mesa de ayuda por medio del web services o directamente al correo electrónico de la oficina de informática. Por otra parte, los usuarios de los centros turísticos, deberán reportarlo a través del correo electrónico institucional dirigido a la oficina de informática para tal fin, solicitando el soporte técnico. Si el daño es tal que el dispositivo es inoperable, el personal de la oficina de sistemas deberá suministrar un equipo provisional de los disponibles, hasta tanto se determine la anomalía del equipo y se dé respuesta al caso.

Daño ocasionado por el usuario:

El usuario responsable del equipo de la red local de la institución, debe realizar un reporte y garantizar su reparación o sustitución y si no se puede

recuperar el equipo, deberá reemplazarlo con otro de iguales o mejores características del que tenía asignado, se le asignara un tiempo determinado dependiendo de la eventualidad (coste de reparación o reemplazo de equipo y necesidad laboral), para la reparación o sustitución del equipo dañado; el reporte debe contener factura, y en caso de sustitución del equipo los datos del nuevo equipo como marca, modelo y características.

Robo o hurto de equipo

En caso de robo o hurto de alguna de las TIC asignadas (dispositivos móviles, computadores portátiles): el servidor público de la institución deberá informar de manera inmediata a la oficina de informática por medio de llamada telefónica y/o correo electrónico. Por otra parte, los usuarios de los centros turísticos, deberán reportarlo a través de la persona responsable del equipo asignado a la oficina de informática, utilizando el correo electrónico institucional y/o llamada telefónica. Adicionalmente, deberá adjuntar la denuncia instaurada ante la Fiscalía General de la Nación o a la Unidad de Respuesta Inmediata URI respectiva, dentro de las 24 horas siguientes al suceso; la cual debe incluir además de los datos personales, los datos del equipo.

Extravío de equipo

En caso de extravío o pérdida de la herramienta TIC designada, el servidor público de la institución, deberá informar de manera inmediata a la oficina de informática, los usuarios de los centros, deberán reportarlo a través de la persona responsable del equipo asignado a la oficina de informática, utilizando el correo electrónico institucional y/o llamada telefónica.

Lineamientos específicos

Del buen uso de equipo de cómputo de escritorio y portátil.

Los funcionarios usuarios de la red empresarial de INCIVA deben garantizar que no se cambiarán los parámetros de configuración del equipo, dado que estos son integrados a la red de monitoreo desde el servidor del dominio por la oficina de informática
Los funcionarios de los centros operativos y los que usan equipos portátiles de la institución deben garantizar que el uso extramural es exclusivamente para actividades propias de la operación de la institución, por lo tanto, el trato y la devolución de los equipos debe ser en óptimas condiciones de funcionamiento.

Del buen uso de los dispositivos móviles y de datos

Los funcionarios usuarios de la institución que tienen asignados dispositivos móviles u otros como GPS deben garantizar el uso de exclusivo de los dispositivos para actividades propias de la institución

Del buen uso del correo institucional y almacenamiento en la nube.

Los funcionarios usuarios de la institución que tienen asignados cuentas de correo institucional deben garantizar el uso exclusivo del servicio de correo electrónico institucional para actividades y labores propias de la institución, así como para la comunicación interna entre funcionarios y notificaciones.

Los funcionarios usuarios de la institución que tienen asignados cuentas de correo institucional deben garantizar el uso exclusivo del almacenamiento en la nube para la realización de backup y compartir información propia de la institución.

Informe de disponibilidad

Los funcionarios de la institución deberán reportar de acuerdo con sus competencias, todo evento, situación o amenaza identificada con la información disponible o su herramienta TIC, directamente al correo

institucional de la oficina de informática de INCIVA: sistemas@INCIVA.gov.co así como al número de teléfono de contacto 5146848 ext. 128.

La oficina de informática de INCIVA, hará monitoreo de la red y realizará las acciones que se consideren pertinentes para garantizar la disponibilidad de la información, así como de las herramientas TIC. Para cualquier caso, además de estos lineamientos, se deben tener en cuenta las instrucciones dispuestas por los fabricantes de los dispositivos móviles, computadores de escritorio y computadores portátiles.

Definición sistemas de información y servicios tecnológicos

Catálogo de sistemas de información del INCIVA

Introducción

El área de informática del INCIVA, crea este catálogo de servicios de información TI con el objetivo de dar a conocer a los funcionarios, las herramientas tecnológicas con las que cuentan, para el desarrollo de sus actividades.

Alcance

El Catálogo de Servicios de TI, se realizó en colaboración del Grupo de Plataforma Tecnológica y la Subdirección de Operaciones, áreas adscritas a la Dirección de Tecnología, utilizando las siguientes fuentes de información.

1. Marco de Referencia de Arquitectura Empresarial.
2. Mejores prácticas de ITIL v3.

¿Qué es un catálogo de servicios de información?

Un servicio es un medio de entrega de valor a los clientes facilitando los resultados que los clientes desean lograr sin la responsabilidad sobre los costos y riesgos específicos. Los resultados se obtienen a través del desempeño de tareas y se ven limitados por la presencia de ciertas restricciones. En líneas generales, los servicios proporcionan resultados mediante la mejora del rendimiento y la reducción de las limitaciones.
Aunque algunos servicios mejorar el desempeño de la tarea otros presentan un efecto más directo, realizan la propia tarea.
Es importante a la hora de determinar que si efectivamente lo que se ha identificado es un servicio de TI, para ello se debe verificar las siguientes características:
Utilidad: ¿El servicio es de valor o agrega valor a las actividades del usuario?
Garantía: ¿El servicio brinda la funcionalidad requerida?
Disponibilidad: ¿Efectivamente este servicio es solicitado por los usuarios?
¿El servicio se encontrará a disposición de los usuarios cuando este lo requiera?

Fiabilidad: ¿El usuario podrá confiar en la información que se le suministre?
Capacidad: ¿Se dispone de la capacidad operativa para prestar el servicio?
Seguridad: ¿Se puede garantizar el resguardo de la información que se maneje a través del servicio?

sistemas de información en el INCIVA

first soft

ATRIBUTO	DESCRIPCIÓN
Proceso	Subdirección Administrativa y Financiera
Dependencia	Tesorería, Contabilidad, Presupuesto, Gestión Humana y Almacén.
Nombre del sistema	First Soft
Tipo de sistema de información	Visual FoxPro
Dirección o URL	Servidor de Dominio
Descripción del sistema de información	Sistema de información Financiera
Objetivo	Tiene como objetivo ser un instrumento para la rendición de cuentas, viabilizar la gestión contable y generar condiciones de transparencia sobre el uso, gestión y conservación de los recursos y su patrimonio. permite la administración y seguimiento de los diferentes tipos de ingresos o egresos que posee la entidad. Se lleva el registro de todos los datos básicos como características tributarias de los funcionarios y proveedores de la entidad además permite mediante el programa de facturación el registro y cuentas por pagar a los mismos. Genera los correspondientes registros contables y presupuestales.
Estado	Activo
Proveedor o desarrollador	Best Service International - BSI
Tipo	Cliente - Servidor
Mantenimiento	No

Proceso que soporta	Subdirección Administrativa y Financiera
Responsable	Subdirector Administrativo y Financiero
Módulos	Presupuesto, Contabilidad, Tesorería, Inventario, Nomina
Entradas	Requerimientos, Recaudos, Cuentas por pagar, Servicios
Salidas	Reportes, CDP, CRP, Facturas.
Fortalezas	Se cuenta con el software desde hace 10 años.
Debilidades	No se tiene póliza de soporte
Líder Funcional	Subdirector Administrativo y Financiero
Plataforma	Visual FoxPro, Mysql
Iniciativas	Mantenimiento y soporte
Sistema con el que se integra	No
Información que se intercambia	Pagos, recaudos, proveedores,
Tipo de integración	Web services
Estado de la interfaz	En operación
Tipo de Intervención	Actualización del aplicativo
Usuarios	Funcionarios de la Subdirección Administrativa y financiera

Sistema financiero SAP

ATRIBUTO	DESCRIPCIÓN
Proceso	Subdirección Administrativa y Financiera
Dependencia	Tesorería, Contabilidad, Presupuesto, Gestión Humana y Almacén.
Nombre del sistema	SAP
Tipo de sistema de información	ABAP
Dirección o URL	192.168.200.73
Descripción del sistema de información	ERP – Planificación de recursos empresariales
Objetivo	Integrar todos los módulos de la entidad para dar mayor agilidad en el procesamiento de la información financiera
Estado	Activo
Proveedor o desarrollador	Gobernación del Valle
Tipo	Cliente - Servidor
Mantenimiento	Área de tecnología de la Gobernación del Valle.

Proceso que soporta	Subdirección Administrativa y Financiera
Responsable	Subdirector Administrativo y Financiero
Módulos	Presupuesto, Contabilidad, Tesorería, Inventario, Nomina
Entradas	Requerimientos, Recaudos, Cuentas por pagar, Servicios
Salidas	Reportes, CDP, CRP, Facturas.
Fortalezas	Reportes e informes en el menor tiempo, mayor seguridad, se integra con otros sistemas.
Debilidades	Migración de la información del anterior sistema.
Líder Funcional	Subdirector Administrativo y Financiero
Plataforma	SAP ABAP
Iniciativas	Integrar módulo de gestión humana y tesorería
Sistema con el que se integra	Excel
Información que se intercambia	Financiera, activos, proveedores
Tipo de integración	Web services
Estado de la interfaz	En operación
Tipo de Intervención	Actualización del aplicativo
Usuarios	Funcionarios de la Subdirección Administrativa y financiera

Software de gestión documental SIGECEM

ATRIBUTO	DESCRIPCIÓN
Proceso	Subdirección Administrativa y Financiera
Dependencia	Gestión Documental
Nombre del sistema	SIGECEM
Tipo de sistema de información	PHP
Dirección o URL	www.gestiondocumental.INCIVA.gov.co:81
Descripción del sistema de información	Software de ventanilla única web
Objetivo	Radicación de documentos internos y externos que ingresan y salen de la entidad.
Estado	Activo
Proveedor o desarrollador	Vennex Group
Tipo	Web cliente - servidor
Mantenimiento	Vennex Group
Proceso que soporta	Gestión documental
Responsable	Técnico operativo Gestión Documental.

Módulos	Radicación interna – radicación externa-TRD – Usuarios, bandeja, informes
Entradas	Documento
Salidas	Radiación interna o externa
Fortalezas	Es un Software web donde se puede radicar un documento interno desde cualquier parte, se pueden hacer seguimiento en la página web y notificación por el correo electrónico
Debilidades	Software en servidor ubicado en la sede central del INCIVA.
Líder Funcional	Técnico Operativo Centro de Documentación
Plataforma	PHP, Visual FoxPro, Mysql
Iniciativas	Gestión documental, política Cero papeles
Sistema con el que se integra	Navegador web Google Chrome, Correo Electrónico Institucional.
Información que se intercambia	Correspondencia Interna y externa, Documentos internos
Tipo de integración	Web Services
Estado de la interfaz	En operación
Tipo de Intervención	Mantener, Mejorar
Usuarios	Funcionarios del INCIVA

Sistema de incidencias GLPI

ATRIBUTO	DESCRIPCIÓN
Proceso	Informática
Dependencia	Sistemas
Nombre del sistema	GLPI
Tipo de sistema de información	PHP
Dirección o URL	http://helpdesk.INCIVA.gov.co:81
Descripción del sistema de información	Software de Mesa de ayuda virtual
Objetivo	Registrar solicitudes y requerimientos de soporte al área de sistemas en tiempo real.
Estado	Activo.
Proveedor o desarrollador	Software libre
Tipo	Web cliente - servidor
Mantenimiento	Sistemas
Proceso que soporta	Informática
Responsable	Asesor de informática
Módulos	Incidencias- crear incidencia- problemas- cambios- planificación- estadísticas- usuarios – inventario.

Entradas	solicitudes de requerimiento o incidencias
Salidas	Respuesta de solicitudes, estadísticas de incidencias.
Fortalezas	Gracias a este software se tiene un canal de comunicación con los usuarios con respecto al soporte. Permitiendo así dejar evidencia de las solicitudes de requerimientos o incidencias que se presentan.
Debilidades	Él envió de Solicitudes depende completamente del usuario.
Líder Funcional	Asesor de Informática
Plataforma	Apache, PHP, MySQL
Iniciativas	Mesa de Ayuda
Sistema con el que se integra	Navegador web Google Chrome
Información que se intercambia	Solicitudes de Soporte
Tipo de integración	Web Services
Estado de la interfaz	En operación
Tipo de Intervención	Mantener, Mejorar
Usuarios	Funcionarios del INCIVA

Página web

ATRIBUTO	DESCRIPCIÓN
Proceso	Informática, mercadeo y divulgación
Dependencia	Sistemas, Mercadeo y divulgación
Nombre del sistema	Portal web INCIVA
Tipo de sistema de información	PHP
Dirección o URL	www.INCIVA.gov.co
Descripción del sistema de información	Medio electrónico que almacena y divulga información sobre la gestión del INCIVA, informes de ley, alineada a la metodología de gobierno digital
Objetivo	Promover y divulgar la visión y la misión del INCIVA, a través de una herramienta tecnológica, el cual permita realizar interacción con las partes interesadas.
Estado	Activo.
Proveedor o desarrollador	Vennex Group
Tipo	Web cliente - servidor

Mantenimiento	Vennex Group
Proceso que soporta	informática
Responsable	Asesor de informática
Módulos	La institución, Transparencia y acceso a la información pública, patrimonios turísticos, servicios, publicaciones, redes sociales, Colecciones, Investigaciones, Cespedecia.
Entradas	PQRS
Salidas	Información y documentación referente a Trasparencia y acceso a la información pública, publicaciones de interés.
Fortalezas	Fortalece la trasparencia del estado y la participación ciudadana de la entidad. Es un medio por el cual facilita la divulgación de información y la interacción con las partes interesadas.
Debilidades	
Líder Funcional	Asesor de informática
Plataforma	PHP, MYSQL
Iniciativas	Gobierno Digital
Sistema con el que se integra	Navegador web Google Chrome, Correo Electrónico Institucional
Información que se intercambia	Documentación e información Pública
Tipo de integración	Web cliente - servidor
Estado de la interfaz	En operación
Tipo de Intervención	Mantener, Mejorar
Usuarios	Funcionarios del INCIVA, de otras entidades y público en general

Google apps

ATRIBUTO	DESCRIPCIÓN
Proceso	Informática
Dependencia	Sistemas
Nombre del sistema	GOOGLE APPS FOR WORK
Tipo de sistema de información	G SUITE -GOOGLE APPS
Dirección o URL	https://accounts.google.com
Descripción del sistema de información	Servicio de red que permite el intercambio de mensajes mediante sistemas de comunicación electrónica, y almacenamiento en la nube a través de una cuenta institucional tipo

	"cargo@INCIVA.gov.co", que lo identifica como funcionario del INCIVA, incluyendo funcionalidades como: • Google Drive. • Calendario. • Ofimática. • Chat. • Video llamada.
Objetivo	Permitir a los funcionarios del INCIVA, el intercambio de mensajes con las partes interesadas, a través de un correo electrónico institucional garantizado, que facilite el desarrollo de sus funciones. Además de permitir almacenamiento en la nube para la realización de Backup de la información institucional.
Estado	Activo.
Proveedor o desarrollador	Vennex Group
Tipo	Web cliente
Mantenimiento	Vennex Group,
Proceso que soporta	informática
Responsable	Asesor de informática
Módulos	Gmail, Drive, Calendario, Documentos (ofimática), Hangouts (chat), Duo (video llamada), Administración de usuarios
Entradas	Mensajes, notificaciones, documentos Institucionales. Backup de información institucional.
Salidas	Descarga de documentos e información institucional.
Fortalezas	envío y recepción de información a través de navegadores web ingresando a https://mail.google.com. además de realización de backup de la información institucional, que maneja los funcionarios en https://drive.google.com sin necesidad de instalación de programas en el equipo del funcionario.
Debilidades	La realización del backup y el uso del mail es completamente manejado por el usuario.

Líder Funcional	Asesor de informática
Plataforma	G SUITE -GOOGLE APPS
Iniciativas	Correo Institucional. Backup de la información.
Sistema con el que se integra	Navegador web Google Chrome
Información que se intercambia	Mensajes, notificaciones, documentos Institucionales
Tipo de integración	Web cliente - servidor
Estado de la interfaz	En operación
Tipo de Intervención	Mantener, Mejorar
Usuarios	Funcionarios del INCIVA.

Catálogo de servicios tecnológicos del INCIVA.

Descripción de los servicios

Internet

Objetivo: Brindar un medio de comunicación ágil, seguro y eficaz, en el cual se pueda hacer el envío y recepción de información (voz, datos, imágenes, etc.) con el exterior.

Descripción: El servicio de internet facilita al usuario, a través de la red del INCIVA, el envío y recepción de información a través de un navegador web.

Necesidades que satisface.

- envío y recepción de información a través de navegadores web para suplir las necesidades laborales del INCIVA
- Comunicación entre los usuarios de la sede central del INCIVA y sus centros operativos.

Responsable del servicio: Oficina asesora de informática, sistemas@INCIVA.gov.co, teléfono: (2) 5146848 ext. 128.

Prerrequisitos para recibir el servicio: El usuario debe cumplir los siguientes prerrequisitos:

- Ser funcionario de planta o contratista del INCIVA.

- Tener a cargo un equipo de cómputo (escritorio o portátil) asignado por el INCIVA o autorizado para la conexión a la red del INCIVA, por parte de la oficina asesora de informática.
- Tener un usuario y contraseña para ingresar al dominio del INCIVA (personal de planta)
- Solicitar a la oficina asesora de informática las credenciales para ingresar a la red del INCIVA, a través de conexión Wifi (Personal de planta y contratistas).

Políticas: Para el manejo del servicio, se establecen las siguientes políticas en el INCIVA.

- Los usuarios son los únicos responsables del buen uso y supervisión de la información de la entidad que adquieren en el ejercicio de sus actividades.
- Cumplir con el capítulo 5 de la resolución reglamentaria de informática del INCIVA # 010.16.01.15.319 del 14 de septiembre de 2015.

Seguridad:

- Horario permitido de acceso: Horario Laboral establecido por la Dirección del INCIVA.
- Nivel de acceso al servicio: El servicio de internet está restringido para el ingreso a páginas de sexualidad, juegos, streaming, entre otras.

Niveles de servicio:

- **En donde se entrega:** En la sede principal del INCIVA y sus centros operativos.
- **Soporte:** Oficina asesora de informática y proveedor externo.
- **Horario de soporte:** lunes a jueves, de 7:30 a.m. a 5 y 30 p.m. y el día viernes de 7:30 a.m. a 4:30 p.m.

Intranet

Objetivo: Brindar un sistema de comunicación interna, en el cual se pueda hacer transferencia de archivos entre los funcionarios de la sede central del INCIVA.

Descripción: El servicio de intranet facilita al usuario, a través de la red del INCIVA, el envío y recepción de información a través de los recursos informáticos del INCIVA (carpetas compartidas, impresoras)

Necesidades que satisface.

- envío y recepción de información a través de los recursos informáticos ubicados en la sede central del INCIVA.
- Comunicación entre los usuarios de la sede central del INCIVA.

Responsable del servicio: Oficina asesora de informática, sistemas@INCIVA.gov.co, teléfono: (2) 5146848 ext. 128.

Prerrequisitos para recibir el servicio: El usuario debe cumplir los siguientes prerrequisitos:

- Ser funcionario de planta o contratista del INCIVA.
- Tener a cargo un equipo de cómputo (escritorio o portátil) asignado por el INCIVA o autorizado para la conexión a la red del INCIVA, por parte de la oficina asesora de informática.
- Tener un usuario y contraseña para ingresar al dominio del INCIVA (personal de planta)
- Solicitar a la oficina asesora de informática las credenciales para ingresar a la red del INCIVA, a través de conexión Wifi (Personal de planta y contratistas).

Políticas: Para el manejo del servicio, se establecen las siguientes políticas en el INCIVA.

- Los usuarios son los únicos responsables del buen uso y supervisión de la información de la entidad que adquieren en el ejercicio de sus actividades.
- Cumplir con el capítulo 5 de la resolución reglamentaria de informática del INCIVA # 010.16.01.15.319 del 14 de septiembre de 2015.

Seguridad:

- Horario permitido de acceso: Horario Laboral establecido por la Dirección del INCIVA.

- Nivel de acceso al servicio: El servicio de intranet está restringido para el uso personal.

Niveles de servicio:

- **En donde se entrega:** En la sede principal del INCIVA.
- **Soporte:** Oficina asesora de informática y proveedor externo.
- **Horario de soporte:** lunes a jueves, de 7:30 a.m. a 5 y 30 p.m. y el día viernes de 7:30 a.m. a 4:30 p.m.

Correo electrónico

Objetivo: Permitir a los funcionarios del INCIVA, el intercambio de mensajes con las partes interesadas, a través de un correo electrónico institucional garantizado, que facilite el desarrollo de sus funciones.

Descripción: Servicio de re que permite el intercambio de mensajes mediante sistemas de comunicación electrónica, a través de una cuenta institucional tipo cargo@INCIVA.gov.co, que lo identifica como funcionario del INCIVA, incluyendo funcionalidades como:

- Google Drive.
- Calendario.
- Ofimática.
- Chat.
- Video llamada.

Necesidades que satisface.

- envío y recepción de información a través de navegadores web ingresando a https://mail.google.com.
- oportunidad en el acceso de la información.

Responsable del servicio: Oficina asesora de informática, sistemas@INCIVA.gov.co, teléfono: (2) 5146848 ext. 128.

Prerrequisitos para recibir el servicio: El usuario debe cumplir los siguientes prerrequisitos:

- Ser funcionario de planta del INCIVA.
- Tener a cargo un equipo de cómputo (escritorio o portátil) asignado por el INCIVA
- Solicitar a la oficina asesora de informática las credenciales para ingresar al correo electrónico institucional.
- Contar con servicio de internet.

Políticas: Para el manejo del servicio, se establecen las siguientes políticas en el INCIVA.

- Los usuarios son los únicos responsables del buen uso y supervisión de la información de la entidad que adquieren en el ejercicio de sus actividades.
- Cumplir con la resolución # 010.16.02.16.279 del 14 de julio del 2016, por medio del cual se fijan las políticas y medidas institucionales para reglamentar la administración, el uso del correo electrónico y el acceso a internet en la entidad.

Seguridad:

- Horario permitido de acceso: las 24 horas del día, los 7 días de la semana.
- Nivel de acceso al servicio: El servicio de correo electrónico es exclusivo para uso de funciones institucionales.

Niveles de servicio:

- **En donde se entrega:** En la sede principal del INCIVA y sus centros operativos.
- **Soporte:** Oficina asesora de informática y proveedor externo.
- **Horario de soporte:** lunes a jueves, de 7:30 a.m. a 5 y 30 p.m. y el día viernes de 7:30 a.m. a 4:30 p.m.

Página web

Objetivo: Promover y divulgar la visión y la misión del INCIVA, a través de una herramienta tecnológica, el cual permita realizar interacción con las partes interesadas.

Descripción: Medio electrónico que almacena y divulga información sobre la gestión del INCIVA, informes de ley, alineada a la metodología de gobierno digital.

Necesidades que satisface

- Divulgación de información.
- Interacción con las partes interesadas.
- Fortalece la transparencia del estado y la participación ciudadana.

Responsable del servicio: Oficina asesora de informática, sistemas@INCIVA.gov.co, teléfono: (2) 5146848 ext. 128, Oficina de mercadeo y divulgación, mercadeo@INCIVA.gov.co, divulgación@INCIVA.gov.co, teléfono: 5146848 ext. 105 – 106. Proveedor externo: Vennex Group. soporte@vennexgroup.com, teléfono: 57 318 532 6001.

Prerrequisitos para recibir el servicio: El usuario debe cumplir los siguientes prerrequisitos:

- Ser funcionario de planta del INCIVA.
- Contar con un hosting y dominio.
- Contar con servicio de internet.
- Recibir información solicitada a los procesos del INCIVA, para subir a página web.

Políticas: Para el manejo del servicio, se establecen las siguientes políticas en el INCIVA.

- Solo los funcionarios de Informática y de Mercadeo y Divulgación, pueden subir información a la página web del INCIVA.
- Toda información que se requiera subir a la página web del INCIVA, tiene que ser enviada a los correos electrónicos: mercadeo@INCIVA.gov.co y divulgación@INCIVA.gov.co, para verificar su contenido institucional.
- Es obligatorio que todo funcionario público del INCIVA, abra la página web del INCIVA, al inicio de sus labores.

Niveles de servicio:

- **En donde se entrega:** En la sede principal del INCIVA.
- **Soporte:** Oficina asesora de informática, Mercadeo y divulgación y proveedor externo.

- **Horario de soporte:** lunes a jueves, de 7:30 a.m. a 5 y 30 p.m. y el día viernes de 7:30 a.m. a 4:30 p.m. Proveedor externo: las 24 horas del día, siete días de la semana.

Software de gestión documental

Objetivo: Proporcional al INCIVA, un software de gestión documental web integral, que cumpla con el proceso de gestión documental, de archivo y política de cero papeles.

Descripción: Con el software de gestión documental se centraliza el proceso de gestión documental y archivística a través de un sistema de gestión de contenidos y documentación que ayuda en la normalización del flujo de información que recibe o emite la entidad. El software de gestión documental se gestiona a través de roles y permite las siguientes soluciones:

- Radicación de correspondencia interna: Permite gestionar la correspondencia interna radicada por funcionarios del INCIVA, mediante el módulo de radicación, submenú: radicación interna – interna.
- Radicación de correspondencia externa: Permite gestionar la correspondencia interna –externa o externa – interna, radicada por funcionarios del INCIVA, y terceros que tienen alguna relación con la entidad, este proceso se realiza solo en la ventanilla única del INCIVA.
- Gestión de correspondencia o radicado: Todo documento radicado que automáticamente guardado en formato PFD con su respectivo número de radicado.

Necesidades que satisface:

- Gestión de radicación de documentos en la ventanilla única del INCIVA, para documentación externa – interna e interna – externa.
- Gestión de radicación de documentos internos en los equipos de cómputo asignados a los funcionarios de planta del INCIVA.
- Notificación de radicación a través del correo electrónico.
- Digitalización de la correspondencia.

Responsable del servicio: Oficina asesora de informática, sistemas@INCIVA.gov.co, teléfono: (2) 5146848 ext. 128, Proveedor

externo: Vennex Group. soporte@vennexgroup.com, teléfono: 57 318 532 6001.

Prerrequisitos para recibir el servicio: El usuario debe cumplir los siguientes prerrequisitos:

- Servicio de internet.
- Servidor web.
- Servidor local, ubicado en la sede central del INCIVA.

Políticas: Para el manejo del servicio, se establecen las siguientes políticas en el INCIVA.

- El horario de atención para la radicación de correspondencia interna – externa y externa – interna, es de lunes a jueves, de 8:00 a.m. a 12:30 p.m. y de 1:30 p.m. hasta 5:00 p.m. y los viernes de 8:00 a.m. a 12:30 p.m. y de 1:30 p.m. hasta 4:30 p.m.
- El horario para la radicación de correspondencia interna, corresponde al horario laboral del INCIVA.
- Un contratista no puede radicar un documento interno.
- Todo oficio que se va a radicar, debe tener en perfecto cumplimiento las normas archivísticas (T.R.D) establecidas por el INCIVA.

Seguridad:

- Horario permitido de acceso: las 24 horas del día, los 7 días de la semana para radicación interna, no se puede radicar fuera del horario laboral. De lunes a jueves, de 8:00 a.m. a 12:30 p.m. y de 1:30 p.m. hasta 5:00 p.m. y los viernes de 8:00 a.m. a 12:30 p.m. y de 1:30 p.m. hasta 4:30 p.m. para correspondencia externa.

Niveles de servicio:

- **En donde se entrega:** En la sede principal del INCIVA, centros operativos y ventanilla única.
- **Soporte:** Oficina asesora de informática, y proveedor externo.

- **Horario de soporte:** lunes a jueves, de 7:30 a.m. a 5 y 30 p.m. y el día viernes de 7:30 a.m. a 4:30 p.m. Proveedor externo: las 24 horas del día, siete días de la semana.

Software ERP First Soft

Objetivo: Proporcionar de una manera eficiente y eficaz la gestión de activos que componen los módulos de planeación, contabilidad, presupuesto, tesorería, gestión humana e inventarios, en el INCIVA.

Descripción: First Soft es un sistema de información que permite realizar la planificación, la gestión contable, presupuestal, control de inventarios, de tesorería y nomina; a través de los siguientes módulos:

- Seguridad: Permite crear usuarios, controlar el nivel de acceso y las acciones que los usuarios puedan ejecutar en los distintos formularios.
- Mantenimiento: Permite crear nuevas empresas, restaurar copias de seguridad, hacer regeneraciones de archivos.
- Financiero: Es el operador del sistema, donde se estructuran los parámetros y maestros, a este llega toda la información ingresada desde los otros módulos del sistema, permite generar diferentes tipos de informes.
- Facturación: permite realizar las facturas por concepto de forma masiva o individual por los servicios prestados.
- Propiedad plata y equipo: se crean los activos de la empresa, además puede asociar la depreciación acumulada a dichos activos de manera automática.
- Control presupuestal: Permite planear, coordinar y controlar todos los gastos, ingresos e inversiones de la operación.
- Gestión fiscal: en este módulo se generan informes para liquidar impuestos, generar datos para medios magnéticos y expedir certificados de retención en la fuente, IVA e ICA.
- Comercial: en él se gestiona el control de inventario.
- Talento Humano: En este módulo se gestiona todo lo relacionado con el proceso de nómina.

Necesidades que satisface:

- Gestión de movimientos presupuestables y contables.
- Gestión de activos.

- Gestión del recurso humano.
- Gestión de cartera.
- Gestión de facturación.
- Gestión de informes a entes de control.

Responsable del servicio: Oficina asesora de informática, sistemas@INCIVA.gov.co, teléfono: (2) 5146848 ext. 128, Proveedor externo: soporte@grupobsi.com.

Prerrequisitos para recibir el servicio: El usuario debe cumplir los siguientes prerrequisitos:

- Servidor local.
- Licencia cliente y servidor.
- Equipo de cómputo ingresado en el dominio del INCIVA.
- Credenciales para ingresar al aplicativo First Soft.

Políticas: Para el manejo del servicio, se establecen las siguientes políticas en el INCIVA.

- Pertenecer al área financiera y de planeación de la entidad.
- Solo se puede ingresar al software en horario laboral.
- No se puede ingresar al aplicativo remotamente por un usuario sin privilegios.
- No se pueden compartir las credenciales para ingresar al aplicativo.
- No puede dejar el aplicativo abierto al cierre o pausas de sus actividades.
- Se deben realizar copias de seguridad de la base de datos del aplicativo.

Seguridad:

- Horario permitido de acceso: Horario laboral, de lunes a jueves, de 7:30 a.m. hasta las 5:30 p.m. y los viernes de 7:30 a.m. hasta las 4:30 p.m.

Marco normativo del gobierno nacional y territorial en relación a ti para cumplimiento en la institución

- Decreto 1008 de 2018, se define la política de Gobierno Digital, por el cual se establecen los lineamientos generales de la política de Gobierno Digital, la cual tiene por objeto promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.
- Decreto N°415 de 7 de marzo 2016, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones
- Ley 1341 de 2009, en el Parágrafo de su artículo 38 establece que: “Las autoridades territoriales implementarán los mecanismos a su alcance para gestionar recursos a nivel nacional e internacional, para apoyar la masificación de las TIC, en sus respectivas jurisdicciones”.
- Ley 1474 de 2011, Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública, hace referencia al uso obligatorio de los sitios web de las entidades públicas como mecanismo para la divulgación de información pública.
- Artículo 232 de la Ley 1450 de 2011 prevé, sobre la Racionalización de trámites y procedimientos al interior de las entidades públicas. Que: los organismos y entidades de la Rama Ejecutiva del Orden Nacional y Territorial procederán a identificar, racionalizar y simplificar los procesos, procedimientos, trámites y servicios internos, con el propósito de eliminar duplicidad de funciones y barreras que impidan la oportuna, eficiente y eficaz prestación del servicio en la gestión de las organizaciones.
- Decreto – Ley 019 de 2012, por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública, estableció en su artículo 4, en relación con la celeridad en las actuaciones administrativas, que: “Las autoridades tienen el impulso oficioso de los procesos administrativos; deben utilizar: formularios gratuitos para actuaciones en serie, cuando la naturaleza de ellas lo haga posible y cuando sea asunto de su competencia, suprimir los trámites innecesarios, sin que ello las releve de la obligación de considerar y valorar todos los argumentos de los interesados y los medios de pruebas decretados y practicados; deben incentivar el uso de las tecnologías de la información y las comunicaciones a efectos de que los procesos administrativos se adelanten con diligencia, dentro de los términos legales y sin dilaciones injustificadas; y deben adoptar las decisiones administrativas en el menor tiempo posible”.
- Artículo 63 del Decreto 067 del 31 de Julio de 2009, mediante el cual se creó el estatuto básico de la Administración Municipal, consagra que con

el fin de mejorar la atención de los servicios y cumplir con eficacia y eficiencia los objetivos, políticas y programas de las dependencias centrales, el alcalde, previo estudio de viabilidad y conveniencia emitido por el DAFP, podrá organizar con carácter permanente o transitorio, grupos internos de trabajo que sean necesarios. También podrá con el mismo procedimiento, fusionar o suprimir los que hayan creado, cuando el desarrollo de los procesos, competencias y funciones de las dependencias así lo exija.

- Decreto No 2573 de 2014, se reglamenta parcialmente la Ley 1341 de 2009 y que en el mismo decreto se define el componente de Privacidad y Seguridad de la información que incluye el modelo de seguridad y privacidad de la información (MSPI), y para ello cuenta con una serie de guías anexas que ayudan a las entidades a cumplir con lo solicitado permitiendo abordar de manera detallada cada una de las fases del modelo, buscando a su vez comprender cuales son los resultados a obtener y como desarrollarlos.
- CONPES - Política Nacional de Seguridad Digital, se tiene como objetivo: “Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país”.
- Resolución No 0002710 del 3 de octubre de 2017, “Por la cual se establecen lineamientos para la adopción del protocolo IPv6”
- Decreto 415 de 2016, se adiciona al decreto único reglamentario de la función pública la definición de lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
- Decreto 1499 de 2017, se modifica el decreto 1083 de 2015 y se definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública.
- Decreto 1078 de 2015 - Por medio del cual se expide el decreto único reglamentario del sector de tecnologías de la información y las comunicaciones.

Definición del plan de capacitaciones de TI del INCIVA

Justificación

El recurso más importante en cualquier organización lo forma el personal

implicado en las actividades laborales. Esto es de especial importancia en una organización, en la cual la conducta y rendimiento de los individuos influye directamente en la calidad y optimización se brindan.

Un personal motivado y trabajando en equipo, son los pilares fundamentales en los que las organizaciones exitosas sustentan sus logros. Estos aspectos, además de constituir dos fuerzas internas de gran importancia para que una organización alcance elevados niveles de competitividad, son parte esencial de los fundamentos en que se basan los nuevos enfoques administrativos o gerenciales.

Sin embargo, en la mayoría de organizaciones de nuestro País, ni la motivación, ni el trabajo aprovechar significativos aportes de la fuerza laboral y por consiguiente el de obtener mayores ganancias y posiciones más competitivas en el mercado.
Tales premisas conducen automáticamente a enfocar inevitablemente el tema de la capacitación como uno de los elementos vertebrales para mantener, modificar o cambiar las actitudes y comportamientos de las personas dentro de las organizaciones, direccionado a la optimización de los servicios de asesoría y consultoría empresarial.
En tal sentido se plantea el presente Plan de Capacitación Anual Del Área de informática.

Alcance

El presente plan de capacitación se aplicará a todo el personal del Instituto para la Investigación y la Preservación Del Patrimonio Cultural y Natural del Valle del Cauca - INCIVA.

Objetivos del plan de capacitación

Objetivo General:

Preparar al personal para la ejecución eficiente de sus responsabilidades que asuman en sus cargos, Brindando oportunidades de desarrollo personal en los cargos actuales y para otros puestos para los que el colaborador puede ser considerado.

Objetivos Específicos

- Proporcionar orientación e información relativa a los objetivos de los sistemas de información y servicios tecnológicos como funcionamiento, normas y políticas.
- Proveer conocimientos y desarrollar habilidades que cubran la totalidad de requerimientos para el desempleo de sus cargos específicos.
- Actualizar y ampliar los conocimientos requeridos en áreas especializadas de actividad.
- Contribuir a elevar y mantener un buen nivel de eficiencia individual y rendimiento colectivo.
- Ayudar en la preparación de personal calificado, acorde con los planes, objetivos y requerimientos de la Institución.
- Apoyar la continuidad y desarrollo institucional.

Meta

Capacitar al 100% jefes de Área, asesores, profesionales universitarios, técnicos administrativos y contratistas que desempeñen cargos y actividades correspondientes al uso de sistemas de información y recursos tecnológicos en la institución

Estrategias

Las estrategias a emplear son:
– Desarrollo de trabajos prácticos que se vienen realizando cotidianamente.
– Presentación de casos casuísticos de su área.
– Metodología de exposición – diálogo

Tipos de capacitación

Capacitación Inductiva: Es aquella que se orienta a facilitar la integración de un nuevo colaborador. Normalmente se realiza al ingresar nuevo personal a un determinado cargo.

Capacitación Preventiva: Es aquella orientada a prever los cambios que se producen en el personal, toda vez que su desempeño puede variar con los años, sus destrezas pueden deteriorarse y la tecnología hacer obsoletos sus conocimientos. Esta tiene por objeto la preparación del personal para enfrentar con éxito la adopción de nuevas metodologías

de trabajo, nueva tecnología o la utilización de nuevos equipos, llevándose a cabo en estrecha relación al proceso de desarrollo empresarial.

Capacitación Correctiva: Como su nombre lo indica, está orientada a solucionar "problemas de desempeño". En tal sentido, su fuente original de información es la Evaluación de Desempeño realizada normal mente en la empresa, pero también los estudios de diagnóstico de necesidades dirigidos a identificarlos y determinar cuáles son factibles de solución a través de acciones de capacitación.

Modalidades de Capacitación

Los tipos de capacitación enunciados pueden desarrollarse a través de las siguientes modalidades:

Formación: Su propósito es impartir conocimientos básicos orientados a proporcionar una visión general y amplia con relación al contexto de desenvolvimiento.

Actualización: Se orienta a proporcionar conocimientos y experiencias derivados de recientes avances científico – tecnológicos en una determinada actividad.

Especialización: Se orienta a la profundización y dominio de conocimientos y experiencias o al desarrollo de habilidades, respecto a un área determinada de actividad.

Perfeccionamiento: Se propone completar, ampliar o desarrollar el nivel de conocimientos y experiencias, a fin de potenciar el desempeño de funciones técnicas, profesionales, directivas o de gestión.

Complementación: Su propósito es reforzar la formación de un colaborador que maneja solo parte de los conocimientos o habilidades demandados por su puesto y requiere alcanzar el nivel que este exige.

Recursos

Humanos: Lo conforman los participantes, facilitadores y expositores especializados en la materia, como: licenciados en administración, contadores, Psicólogos, etc.

Materiales: Infraestructura. - Las actividades de capacitación se desarrollarán en ambientes adecuados proporcionados por la gerencia de la institución.

Mobiliario, equipo y otros: Está conformado por carpetas y mesas de trabajo, pizarra, plumones, total folio, equipo multimedia, video Beam, y ventilación adecuada.

Cronograma

Cronograma Plan de capacitaciones de recursos tecnológicos y sistemas de información de INCIVA

Actividades a desarrollar	Mes												Intensidad
	1	2	3	4	5	6	7	8	9	10	11	12	
Cursillo: Correcto uso de almacenamiento en dispositivos USB y uso de antivirus.		x											1 hora
Cursillo: Uso de mesa de ayuda, incidencias y requerimientos.				x									1 hora
Cursillo: Navegación segura y políticas de navegación en sitios web						x							1 hora
Cursillo: Manejo del sistema de Gestión Documental								x					1 hora
Cursillo: Realización de Backup y correcto uso del correo institucional									x				1 hora
Cursillo: políticas de uso y correcto manejo de equipos de computo											x		1 hora

Alineación de la estrategia de ti con la estrategia de la institución pública: disposición de residuos tecnológicos.

Objetivo general

El INCIVA, en asesoramiento de la oficina de informática y almacén, en contexto con las políticas departamentales y nacionales ambientales para la gestión integral de residuos y los lineamientos técnicos para el manejo de residuos de aparatos eléctricos y electrónicos del Ministerio de Ambiente y Desarrollo Sostenible; pone a disposición el siguiente procedimiento para el manejo de residuos eléctricos y electrónicos RAEE.

Este documento tiene el objetivo de establecer los procesos mínimos a seguir para un correcto manejo de residuos de aparatos RAEE, este se basa en las actividades a llevar a cabo para cada proceso. Teniendo en cuenta que los aparatos electrónicos y electrónicos, son una mezcla de muchos materiales, que comprende tanto materias primas escasas, como elementos o compuestos peligrosos, las operaciones de almacenamiento, tratamiento, aprovechamiento y disposición final de residuos de aparatos eléctricos y electrónicos (RAEE) se deben seguir bajo los lineamientos establecidos para tal fin.

Objetivos específicos

- Definir una política en el INCIVA para el manejo de los Residuos de Aparatos Eléctricos y Electrónicos (RAEE).
- Establecer un protocolo de obligatorio cumplimiento para la recolección, manejo, almacenamiento y disposición final de los RAEE en el INCIVA
- Capacitar al personal del INCIVA en la correcta aplicación del Programa de disposición final de residuos tecnológicos.
- Establecer un lugar adecuado para el almacenamiento de los RAEE en el INCIVA que permita cumplir la cadena de custodia y seguridad.
- Identificar la extracción de elementos y partes que tengan posibilidad de reusó, reutilizables o reciclables.
- Monitorear, evaluar y retroalimentar anualmente los procesos de recolección, manejo, almacenamiento y disposición final de los RAEE en el INCIVA.

Alcance

Este programa de disposición final de residuos tecnológicos se aplicará en la sede central del INCIVA y sus 5 centros operativos.

Responsables

- **Oficina asesora de informática:** Es el encargado de diseñar el programa, monitorearlo y retroalimentarlo; además emite conceptos de técnicos por el daño u obsolescencia de los equipos.

- **Almacén General:** contribuye al diseño del plan, recepción y viabiliza los conceptos técnicos de la oficina de sistemas, autoriza el desplazamiento de los RAEE hasta su lugar de almacenamiento y realiza las labores administrativas legales para excluir el bien del inventario de la institución y entregarlo al aliado estratégico en la disposición final.

- **Comité Directivo:** Es quien aprueba el plan para su publicación y divulgación.

Términos y definiciones

- **Aparatos eléctricos y electrónicos (AEE):** Todos los aparatos que para funcionar necesitan corriente eléctrica o campos electromagnéticos, así como los aparatos necesarios para generar, transmitir y medir tales corrientes.

- **Baja de bienes:** La baja de bienes, es un proceso que consiste en retirar del patrimonio de la entidad, aquellos bienes que han perdido la posibilidad de ser utilizados, por haber sido expuestos a acciones de diferente naturaleza, como las siguientes: Daño y/o deterioro Desgaste o afectación de los bienes debido al uso continuo.

- **Bienes de consumo:** Los bienes de consumo son los bienes finales en el proceso de producción de una economía. Satisfacen necesidades de las personas de una manera directa y se consume en su primer uso o en un período razonable de tiempo.
- **Bienes inservibles:** Son bienes que, por su desgaste, deterioro u obsolescencia, material o tecnología, no son útiles para el servicio al cual

se encuentran destinados y no ofrecen posibilidad alguna de uso o aprovechamiento de su parte.

- **Bienes no utilizables:** Son bienes que no obstante de estar en buen estado, la entidad no los requiere para el normal desarrollo de sus actividades, por caer en desuso.

- **Bienes servibles:** Son aquellos bienes muebles que se encuentren en buenas condiciones.

- **Destrucción de bienes:** Reducir a pedazos o a cenizas los bienes muebles objeto de la baja.

- **Disposición final:** Es el proceso de aislar y confinar los residuos sólidos en especial los no aprovechables, en forma definitiva, en lugares especialmente seleccionados y diseñados para evitar la contaminación, y los daños o riesgos a la salud humana y al ambiente.

- **Donación de bienes:** Es la autonomía de la entidad para transferir gratuita e irrevocablemente un bien mueble de su propiedad a otra persona jurídica de derecho público que lo acepta.

- **Gestor de RAEE:** Persona que presta de forma total o parcial los servicios de recolección, transporte, almacenamiento, tratamiento, aprovechamiento o disposición final de los residuos de aparatos eléctricos y electrónicos (RAEE) dentro del marco de la gestión integral y cumpliendo con los requerimientos de la normativa ambiental vigente.

- **Gestión integral:** Conjunto articulado e interrelacionado de acciones políticas, normativas, operativas, financieras, de planeación, administrativas, sociales, educativas, de evaluación, seguimiento y monitoreo desde la prevención de la generación hasta la disposición final de los residuos de aparatos eléctricos y electrónicos, a fin de lograr beneficios ambientales, la optimización económica de su manejo y su aceptación social, respondiendo a las necesidades y circunstancias de cada localidad o región.
- **RAEE:** Residuos de Aparatos Eléctricos y Electrónicos que funcionan

con corriente eléctrica o un campo electromagnético y han dejado de ser efectivos.

- **Reacondicionamiento:** Procedimiento técnico de renovación, en el cual se restablecen las condiciones funcionales y estéticas de un aparato eléctrico y electrónico con el fin de ser usado en un nuevo ciclo de vida. Puede implicar además reparación, en caso de que el equipo posea algún daño.

- **Reciclaje:** Son los procesos mediante los cuales se aprovechan y transforman los residuos recuperados y se devuelven a los materiales su potencialidad de reincorporación como materia prima para la fabricación de nuevos productos.

- **Residuo o desecho peligroso:** Es aquel residuo o desecho que en función de sus características corrosivas, reactivas, radioactivas, explosivas, tóxicas, inflamables, biológicas e infecciosas puede causar riesgo para la salud humana y/o deteriorar el ambiente.

- **Residuos de aparatos eléctricos y electrónicos (RAEE):** Se refiere a aparatos dañados, descartados u obsoletos que consumen electricidad. Incluye una amplia gama de aparatos como computadores, equipos electrónicos de consumo, celulares y electrodomésticos que ya no son utilizados o deseados por sus usuarios.

- **Reusó:** el reusó de un equipo eléctrico o electrónico se refiere a cualquier utilización de un aparato o sus partes, después del primer usuario, en la misma función para la que el aparato o parte fueron diseñados.

- **Sistemas de recolección y gestión de los RAEE:** instrumento de control y manejo ambiental que contiene el conjunto de actividades desarrolladas por el productor de aparatos eléctricos y electrónicos para garantizar la recolección y gestión integral y ambientalmente segura de los RAEE, con el fin de prevenir y controlar los impactos a la salud y el ambiente.

- **Venta de bienes muebles:** Es la operación mercantil mediante la cual se transfiere a dominio ajeno un bien mueble dado de baja a cambio de dinero en el precio convenido.

- **Usuario o consumidor:** toda persona natural o jurídica que contrate la adquisición, utilización o disfrute de un bien o la prestación de un servicio determinado

Identificación de fuentes

A continuación, se relacionan todas las oficinas generadoras de residuos tecnológicos en el INCIVA y sus centros operativos:

A. Sede Central

- Oficina de Taxidermia.
- Oficina de Zoología.
- Oficina de Arqueológica.
- Oficina de Botánica.
- Oficina de Gestión Documental.
- Ventanilla Única.
- Oficina de Museo de Ciencias Naturales y Recepción.
- Oficina de Investigaciones.
- Cocineta 1 piso.
- Oficina de Control Interno.
- Oficina de Almacén General.
- Oficina de Informática.
- Museo de ciencias naturales
- Auditorio.
- Oficina Jurídica.
- Oficina de Mercadeo y Divulgación.
- Dirección General.
- Oficina de secretaria General.
- Oficina de planeación y banco de proyectos.
- Oficina de administración de recursos.
- Oficina de Tesorería.
- Oficina de contabilidad.
- Oficina de presupuesto.
- Oficina de Gestión Humana.

- Cocineta 4 piso.

B. Museo Arqueológico Calima

- Oficina de administración.
- Laboratorio de arqueología.

C. Jardín Botánico Juan María Cespedes

- Oficina de administración.
- Laboratorio Etnobotánico.

D. Hacienda El Paraíso

- Oficina de administración.

E. Parque Natural Regional El Vinculo

- Oficina de administración.

Marco legal

- **Decreto 1076 de 2015**: Por medio del cual se expide el Decreto Único Reglamentario del Sector Ambiente y Desarrollo Sostenible.

- **Ley 1672 de 2013**: Por la cual se establecen los lineamientos para la adopción de una política pública de gestión integral de residuos de aparatos eléctricos y electrónicos (RAEE), y se dictan otras disposiciones.

- **Resolución 1512 de 2010 (Ministerio de Ambiente, Vivienda y Desarrollo Territorial, 2010)**: por la cual se establecen los sistemas de recolección selectiva y gestión ambiental de residuos de computadores y periféricos y se adoptan otras disposiciones.

- **Resolución 1297 de 2010 (Ministerio de Medio Ambiente, Vivienda y Desarrollo Territorial, 2010):** por la cual se establecen los sistemas de recolección selectiva y gestión ambiental de residuos de pilas y acumuladores y se adoptan otras disposiciones. Decreto 2041 de 2014 por el cual se reglamenta el Título VIII de la Ley 99 de 1993 sobre licencias ambientales.

Políticas de operación

Categoría del RAEE:

Según la Directiva de la Unión Europea sobre RAEE, 2002, los productos o aparatos que al final de su vida útil pueden constituir residuos de aparatos eléctricos y electrónicos (RAEE), se clasifican en 10 categorías, la clasificación y rotulación de los RAEE debe corresponder a estas categorías:

Recolección y almacenamiento del RAEE:

El MinTic a través de la guía práctica de disposición de residuos tecnológicos, define cuales son los requisitos mínimos que debe tener el sitio donde se almacenaran de manera temporal los residuos tecnológicos del INCIVA.

Los requisitos que se deben tener en cuenta son los siguientes:

- Protección contra la intemperie: El almacenamiento debe realizarse a temperatura ambiente y protegido de la intemperie, con el objetivo de evitar que agentes contaminantes puedan lixiviar al ambiente debido a los efectos del tiempo y para permitir el posterior reacondicionamiento o reutilización de los equipos.

- Pisos: Impermeables para evitar infiltraciones y contaminación de los suelos.

- Capacidad: Adecuada para el manejo de todo el inventario.

- Protección contra acceso no autorizado: El desecho se debe almacenar en un lugar donde no se permita el ingreso de personas no autorizadas.

- Registros: Deben mantener registros de inventarios, tanto de equipos en de uso enteros, como piezas recuperadas en caso de cada aplique.

- Procedimientos**:** Se deben documentar los procedimientos que se llevan a cabo en el sitio de almacenamiento.

- Personal: El personal debe estar capacitado para cumplir con los procedimientos del almacenamiento.

- Almacenamiento y empaque: Los RAEE se deben almacenar sobre estibas, o en cajas de rejas o de madera, facilitando su almacenamiento, carga y transporte hacia procesos posteriores.

- Rotulado: Con el propósito de identificar los residuos que se encuentran almacenados, se debe utilizar un rotulo para marcar los bienes o elementos

Situación actual del RAEE en el INCIVA

En el INCIVA se están utilizando 2 bodegas para el almacenamiento de los residuos tecnológicos de la entidad; la primera bodega tiene un espacio de 5 metros de ancho por 5 metros de largo con una altura de 2.75 metros, la segunda bodega tiene un espacio de 3.02 metros de ancho por 4.65 metros de largo con una altura de 2.75 metros.
Estas bodegas se encuentran a temperatura ambiente, no cuentan con pisos impermeables y maneja una capacidad para el manejo del inventario del INCIVA.
El área de almacén cuenta con un técnico administrativo para el manejo del RAEE, y 3 contratistas como soporte.
La Bodega no cuenta con cajas de maderas o estibas para almacenar los residuos tecnológicos y transportarlos fácilmente, estos residuos tecnológicos están acaparados unos sobre otros dificultando su ubicación y transporte.
Se debe realizar un rotulado para identificar cada residuo tecnológico en la entidad.

Transporte y logística

Para la ejecución del transporte de RAEE a su disposición final, el INCIVA realizara los procedimientos contractuales necesarios. El contratista que sea seleccionado para el transporte y logística de RAEE debe dar cumplimiento a los siguientes requisitos técnicos, teniendo en cuenta los lineamientos establecido por el Ministerio de Ambiente y Desarrollo sostenible.

Requisitos técnicos:

- Se debe garantizar siempre la protección contra la intemperie

- Durante el transporte se debe evitar que las personas no autorizadas tengan acceso a la carga, con el fin de evitar la adición o pérdida de partes o piezas de equipos sin supervisión.

- La carga en el vehículo debe estar debidamente empacada, acomodada, estibada, apilada, sujeta y cubierta de tal forma que no presente peligro para la vida de las personas y el medio ambiente.

- Para este fin se recomienda que todo transporte de residuos de aparatos eléctricos y electrónicos de tamaño mediano o pequeño se realice en cajas de madera, de cartón grueso o de rejas metálicas.

- En caso de transportar los residuos de aparatos eléctricos y electrónicos en estibas, se debe envolver toda la estiba con una película plástica cuando esté cargada.

- Es recomendable no poner más de tres capas de residuos de aparatos eléctricos y electrónicos en las estibas y asegurar que la carga no sobresalga de las cajas.

- Por lo general no se requieren cartones o espumas entre las capas. Sin embargo, para algunas excepciones se recomienda colocarlos, por ejemplo, para el transporte de monitores en desuso.

- En caso de ofrecer los servicios de recolección y transporte de equipos de impresión y fotocopia en desuso, tener un sistema de recolección de derrames de tinta para evitar contaminación del medio ambiente y de los demás componentes conjuntamente transportados.

- Portar como mínimo dos (2) extintores tipo multipropósito, uno en la cabina y los demás cerca de la carga, en sitio de fácil acceso para que se pueda disponer de él rápidamente en caso de emergencia, y contar con personal preparado para su utilización.

Disposición final

El INCIVA realizara un contrato de prestación de servicios y/o un convenio interadministrativo con alguna autoridad ambiental facultada para el manejo de los residuos tecnológicos en el Valle del Cauca. La empresa Ambiental entregara al INCIVA un certificado de disposición final, garantizando el buen manejo de los RAEE por parte de la entidad, protegiendo el medio ambiente a través del cumplimiento de la reglamentación del Ministerio de Ambiente y Desarrollo Sostenible.

Seguimiento y evaluación del programa

Este programa debe ser auditado cada año con el fin de garantizar su funcionalidad, efectividad e impacto ambiental.

Comunicación y divulgación

El programa de disposición final de residuos tecnológicos será divulgado a través de la subdirección de mercadeo y divulgación del INCIVA, con el objetivo de sensibilizar al personal la importancia del manejo de los residuos tecnológicos.

REFERENCIAS

[1] Hitt, Ireland y Hoskisson. (2009). *Strategy Management*. USA: South-Western Cengage Learning.

[2] Hitt, Ireland y Hoskisson. (2009). *Strategy Management*. USA: South-Western Cengage Learning.

[3] Selig, G. (2008). *Implementing IT Governance - A Practical Guide to Global Best Practices in IT Management* (1St ed.). Zaltbommel: Van Haren Publising.

[4] Ministerio de Tecnologías de la Información y las Comunicaciones, Gobierno de Colombia. (2017). *Conoce la estrategia de gobierno en línea*. Recuperado de http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html

[5] ISACA. (2012). *COBIT5: Procesos catalizadores*. ISBN 978-1-60420-285-4.

USA.

[6] AXELOS. (2017). *What is ITIL® Best Practice.* Recuperado de https://www.axelos.com/best-practice-solutions/itil/what-is-itil

[7] ISACA. (2012). *COBIT5: Un marco de negocio para el gobierno y la gestión de las TI de la empresa*. USA.

[8] Ministerio de Tecnologías de la Información y las Comunicaciones, Gobierno de Colombia. (2017). *Arquitectura TI Colombia*. ISBN: 978-958-58786-6-2. Recuperado de http://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8114.html

[9] Instituto para el Desarrollo de Antioquia. (2015). *Gestión tributaria para municipios*. Recuperado de http://www.idea.gov.co/es-co/SalaDePrensa/Publicaciones/Gesti%C3%B3n%20tributaria%20para%20municipios.pdf

[10] Ministerio de la Tecnologías y las Comunicaciones. (2010) *Guía No. 10. Marco para la preparación de las TIC para la Continuidad del negocio*. Colombia.

[11] Kulkarni, G. (2012). *Adaptación COBIT 5 e ITIL en un municipio saudí*. Recuperado de http://www.isaca.org/COBIT/focus/Pages/cobit-5-and-itil-adaptation-at-a-saudi- municipality-spanish.aspx.

[12] Ferrer V., R. (2015). *Metodología para la Gestión de la Continuidad del Negocio*. *Cintel Proyectos TIC innovadores*. http://cintel.org.co/wp-content/uploads/2013/05/Metodolog%23U00eda-para-la-Gesti%23U00f3n-de-la-Continuidad-del-Negocio.pdf

[13] Secretaría de Hacienda. Alcaldía Mayor de Bogotá D.C. (2013). Plan institucional de respuesta a emergencias “PIRE”. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/adminverblobawa?tabla=T_NORMA_ARCHIVO&p_NORMFIL_ID=3495&f_NORMFIL_FILE=X&inputfileext=NORMFIL_FILENAME

[14] Arquitectura de TI de MINTIC: https://www.mintic.gov.co/arquitecturati/630/w3-channel.html

[15] Wikipedia Information Technology Infraestructure Library: https://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

[16] Contenido de la Norma ISO 22301 [en línea]. Disponible en internet: http://normaiso22301.com/contenido-de-la-norma-iso-22301/