



PLAN DE CONTINUIDAD DE SERVICIOS DE TI

PROCESO DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN

2021

TABLA DE CONTENIDO

Glosario	4
Presentación	6
Normograma	7
1. Política de Continuidad y Recuperación de Servicios de TI	8
1.1 Introducción	8
1.2 Documentos Relacionados.....	8
1.3 Objetivo	8
1.4 Alcance	9
1.5 Enunciado.....	9
1.6 Roles y Responsabilidades	9
1.7 Estrategias.....	10
2. Contexto Institucional.....	11
2.1 Misión	11
2.2 Visión.....	11
2.3 Estructura Organizacional	11
2.4 Análisis De Procesos.....	12
3. Marco Conceptual del Proceso de TSI	15
3.1 Misión de TSI.....	15
3.2 Visión de TSI	15
3.3 Objetivos Estratégicos de TSI	15
3.4 Políticas de TSI	16
3.5 Organigrama del Procesos de Tecnologías y Sistemas de Información de ITSa	16
4. Análisis de Impacto.....	17
4.1 Descripción	17
4.2 Actividades	17
4.2.1 Identificación de procesos	17
4.2.1.1 Procesos Críticos.....	17
4.2.2 Identificación de aplicaciones	18
4.2.2.1 Relación de aplicaciones	18
5. Responsables de la Continuidad de los Servicios de TI en la Institución.....	28
6. Identificación de Activos	29

7. Definición de Impactos	32
7.1 Pérdida de la Continuidad	33
8. Riesgos Asociados	35
9. Línea de Madurez ITIL	41
10. Equipos de Emergencia para Activación del Plan de Continuidad	43
11. Procedimientos para ejecución del Plan de Continuidad	46

Glosario

Análisis del impacto al negocio (BIA por sus siglas en inglés): Proceso del análisis de actividades, las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas [Fuente: ISO 22300].

Continuidad del Negocio: Capacidad de la organización para continuar con la entrega de productos o servicios a los niveles predefinidos aceptables después de un evento perjudicial.

Disparador o detonante: Evento que hace que el Sistema inicie una respuesta. También es conocido como evento activador.

DRP: (Por sus siglas en inglés, Disaster Recovery Plan - Plan de Recuperación de Desastres), es la estrategia que se sigue para restablecer los servicios de tecnología (red, servidores, hardware y software) después de haber sufrido una afectación por un incidente o catástrofe de cualquier tipo, el cual atente contra la continuidad del negocio.

Evento de interrupción mayor: Evento con afectación considerable de la disponibilidad y operatividad de los servicios de la organización.

Gestión de la Continuidad: Proceso general de gestión holístico que identifica amenazas potenciales a una organización y el impacto que se podría causar a la operación del negocio en caso de materializarse. Provee un marco de trabajo para la construcción de la resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarde los intereses de las partes interesadas claves, reputación, marca y actividades de creación de valor.

Incidente: Situación que sería o podría llevar a una interrupción, pérdida, emergencia o crisis.

Infraestructura TI: Sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de una organización.

Interrupción: Incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. Fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden afectar el normal curso de las operaciones en alguna de las ubicaciones de la organización.

Mejoramiento continuo: Actividad periódica para mejorar el desempeño de las actividades y procesos.

Plan de Continuidad del Negocio - PCN: Procedimientos documentados que guían y orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel pre-definido de operación debido una vez presentada / tras la interrupción.

Típicamente, esto incluye los recursos, servicios y actividades necesarios para garantizar la continuidad de las funciones críticas del negocio Fuente: ISO 22301].

Plan de Prevención, Preparación y Respuesta ante Emergencias: Documento que contempla las acciones e instrucciones que se deben seguir para responder rápida, eficaz y con el menor traumatismo posible ante una emergencia.

Prueba: Procedimiento para determinar la presencia, cualidad o veracidad de algo.

Procesos críticos: Procesos de negocio relevantes para la viabilidad y operación de la organización. La no disponibilidad de éstos puede afectar gravemente los intereses tanto reputacionales como de cumplimiento normativo.

Tiempo objetivo de recuperación (RTO): Periodo de tiempo en el cual los mínimos niveles de productos y/o servicios y los sistemas, aplicaciones, o funciones que los soportan deben ser recuperados después de que una interrupción ocurra.

Recurso: Todos los activos, recursos humanos, conocimientos, información, tecnología, locales y suministros e información que una organización tiene que tener disponibles para su uso, cuando sea necesario, con el fin de operar y cumplir con su objetivo.

Resiliencia: Habilidad Capacidad para que una organización para resistir cuando es afectada al ser afectada por una interrupción.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

RPO: Punto más reciente en el tiempo en el que los sistemas pueden ser recuperados, reflejando por tanto cuánta es la cantidad de información que una organización puede permitirse perder sin que le afecte negativamente. Por tanto, el RPO determina la periodicidad con la que deben salvaguardarse los datos para todos aquellos procesos de negocio.

RTO: Urgencia que las diferentes unidades de negocio precisan para volver a su funcionamiento habitual.

Presentación

La Gestión de la Continuidad del Servicio se encarga de impedir que una interrupción de los servicios que se presente de manera imprevista genere grandes consecuencias para el negocio; éstas interrupciones podrían derivarse no solo de fallos en la infraestructura tecnológica o TI (ataques de denegación de servicio, virus, entre otros) sino también de desastres naturales (incendios, inundaciones, terremotos, entre otros). Hoy en día el tema cobra vital trascendencia ya que ante la emergencia sanitaria ocasionada por el COVID-19, las tecnologías desempeñan un papel importante como elemento fundamental para la continuidad de muchos negocios, permitiendo que las actividades que antes se hacían de manera presencial se puedan realizar de manera remota.

En el caso de las entidades educativas, la continuidad de los servicios de TI es fundamental dado que es transversal a todos los procesos de las mismas, tanto para las actividades administrativas como para las actividades misionales, donde, ahora más que nunca la virtualidad desempeña un rol esencial.

Para una entidad como la Institución Universitaria ITSA, es fundamental disminuir la posibilidad de ocurrencia de incidentes, sobre todo en la actualidad, donde la Institución ha procurado por el establecimiento de estrategias que permitan dar continuidad a la prestación del servicio y el desarrollo de sus actividades misionales, ante la situación generada por la pandemia del COVID-19.

En este orden de ideas, el presente documento es construido teniendo en cuenta la “*Guía Número 10: Preparación de las TIC para la Continuidad del Negocio*” (Mintic, 2010), el cual es un referente para las entidades públicas en materia de Continuidad del Negocio, posibilitando además que la Institución cumpla con los lineamientos de la Política de Gobierno Digital.

Para la Institución Universitaria ITSA contar con un Plan de Continuidad de los Servicios de TI, le permite la identificación clara de los mecanismos, procesos, procedimientos, actividades y los recursos humanos, financieros y activos que deben tenerse en cuenta ante una posible interrupción o desastre. El Plan Continuidad de los Servicios de TI, se presenta a la comunidad educativa y la sociedad en general como un libro abierto, que requiere de la revisión y actualización periódica, con el objeto de reflejar siempre la realidad del entorno y de la Institución.

Normograma

- 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 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.
- Decreto N° 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, que 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”.
- 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.

1. Política de Continuidad y Recuperación de Servicios de TI

1.1 Introducción

La Política de Continuidad y Recuperación de Servicios de TI de la Institución Universitaria ITSA permite identificar los impactos potenciales que amenazan la continuidad de los servicios de Tecnologías de la Información y las estrategias para la recuperación ante la materialización de alguna amenaza, y se realiza con el fin de:

- Identificar y gestionar amenazas actuales y futuras para la Institución.
- Adoptar un método proactivo para minimizar el impacto de los incidentes y construir resiliencia.
- Identificar al personal clave requerido para la operación del proceso desde los Servicios de TI el cual es crítico para el negocio.
- Desarrollar capacidades para brindar respuestas efectivas para proteger los intereses de la Institución.
- Mantener operativas y actualizadas las funciones críticas durante los momentos de crisis.
- Minimizar los tiempos muertos durante los incidentes.
- Mejorar los tiempos de recuperación.
- Impartir capacitaciones iniciales para el correcto funcionamiento del plan.
- Establecer un plan de prueba, gestión y mantenimiento para garantizar los objetivos del plan.
- Preservar la buena reputación de la Institución.

1.2 Documentos Relacionados

- ITIL V3
- Requisitos definidos en la Norma ISO/IEC 27001: 2013, punto A.14.1.3
- Requisitos definidos en la Norma ISO 22301: 2012, punto 8.4
- Norma BS 25999: 2007, punto 4.3
- Cobit 5.0
- Manual de políticas de seguridad de la Información GN-M-01

1.3 Objetivo

Asegurar la continuidad del negocio a través de la definición de lineamientos a seguir antes, durante y después de eventos que puedan producir una interrupción en las operaciones de los Servicios de TI de la Institución Universitaria ITSA. Lo anterior, con el fin de reducir los

riesgos, asegurar la restauración inmediata y la gestión de la continuidad buscando el mínimo impacto en las operaciones.

1.4 Alcance

Esta política es aplicable para todos los funcionarios administrativos, docentes y contratistas de la Institución Universitaria ITSA. Es su deber, *i)* notificar ante cualquier situación que pueda suponer un riesgo para la Institución y/o las personas que en ellas laboran y *ii)* aplicar con diligencia las medidas que se establezcan en este documento.

1.5 Enunciado

“Debido a que la Institución no está exenta de la ocurrencia de incidentes disruptivos (desastres, fallas de seguridad, pérdida y disponibilidad del servicio) que puedan afectar su operación, es responsabilidad del Comité de Gestión y Desempeño Institucional aprobar un plan de continuidad para los Servicios de TI, que permita que la Institución Universitaria ITSA se encuentre preparada para responder de forma adecuada y oportuna ante cualquier daño potencial ocasionado por dicho incidente”.

1.6 Roles y Responsabilidades

- El Proceso de Tecnologías y Sistemas de Información es el responsable de establecer y mantener las estrategias de la Política de Continuidad y Recuperación de Servicios de TI, identificando estándares, normas, y documentación necesaria en la materia, como lineamiento transversal para todos los procesos de la Institución.
- El Proceso de Tecnologías y Sistemas de Información es el encargado de gestionar los riesgos de Tecnologías de la Información.
- El Comité de Gestión y Desempeño Institucional es el responsable de hacer seguimiento en el cumplimiento de la Política de Continuidad y Recuperación de Servicios de TI.
- El Proceso de Tecnologías y Sistemas de Información es responsable de realizar las mejoras a la Política de Continuidad y Recuperación de Servicios de TI, así como de su actualización de acuerdo a los cambios en los lineamientos de la Política de Gobierno Digital.
- El Comité de Gestión y Desempeño Institucional es responsable de aprobar la Política de Continuidad y Recuperación de Servicios de TI.

1.7 Estrategias

- Se debe elaborar y aprobar un plan de Continuidad de Servicios de TI, que incorpore la Política de Continuidad y Recuperación, de acuerdo a los lineamientos y actualizaciones propuestas desde el gobierno nacional a través de la Política de Gobierno Digital.
- Los propietarios y administradores de la información en cada uno de los procesos de la Institución deben identificar, clasificar y priorizar la información crítica de sus procesos.
- Se deben establecer actividades de prevención y de recuperación que ofrezcan las garantías necesarias para el restablecimiento de las operaciones de la Institución posterior a un desastre.
- Se debe establecer el tiempo aceptable para recuperar los datos que tiene la Institución en caso de una interrupción o desastre (RPO), y garantizar una recuperación eficaz.
- Se debe establecer el tiempo para retornar a las actividades normales después de la interrupción o desastre (RTO), y garantizar que los procesos críticos son recuperados dentro de los márgenes de tiempo requeridos en el Plan de Continuidad.
- Se debe contar con equipos servidores alternos que permitan tener disponible versiones de sistema operativo, plataformas de base de datos, de servicios Web y configuraciones necesarias que estén compatibles y sincronizadas con los servidores principales.
- Se debe disponer de energía eléctrica a través de sistemas de alimentación ininterrumpida y plantas eléctricas para suministrar energía a los equipos de cómputo, principalmente a equipos servidores.
- Se debe garantizar la divulgación y concientización de la Política y del Plan de Continuidad de Servicios de TI dentro de la cultura de la Institución.

2. Contexto Institucional

2.1 Misión

La Institución Universitaria ITSA, es un Establecimiento Público de Educación Superior, comprometido con la formación de personas autónomas, creativas, emprendedoras, éticas, responsables y con una visión sustentable, en un modelo de formación basado en competencias que responde a las necesidades del entorno en un contexto globalizado.

2.2 Visión

En el 2023, la Institución Universitaria ITSA, será reconocida como una Institución de Educación Superior de alta calidad con acreditación institucional e internacional de sus programas académicos; caracterizados por el uso y fomento de las TIC, el compromiso con el desarrollo sostenible, un sistema de internacionalización fortalecido y el mantenimiento de alianzas estratégicas con el sector productivo, estatal y social, contribuyendo al desarrollo de la región Caribe y a la transformación y mejora de la sociedad.

2.3 Estructura Organizacional

La Institución Universitaria ITSA cuenta con una estructura plana y flexible, que tiene distribuida las responsabilidades a través de la especialización del trabajo por áreas similares, desarrollando un modelo de administración y gestión que tiene su más grande fortaleza en la cultura de la participación.

En este orden de ideas, en la Figura 1 se presenta la estructura organizacional de la Institución, aprobada mediante Acuerdo de Consejo Directivo 008 de 2016, y la cual está constituida por un Consejo Directivo, un Consejo Académico, Rectoría, Oficina de Control Interno, Secretaría General, Vicerrectoría Académica, Vicerrectoría de Extensión e Investigación, Vicerrectoría Administrativa y Financiera y los Órganos de Asesoría y Coordinación, fortaleciendo así los procesos de docencia, investigación, extensión y proyección social como funciones sustantivas de la educación superior.

A su vez, los Órganos de Dirección y Administración de la Institución Universitaria ITSA son: el Consejo Directivo, el Consejo Académico y la Rectoría, siendo el Consejo Directivo el máximo órgano de dirección y administración, el Consejo Académico la máxima autoridad académica de la Institución, y el Rector el representante legal, ordenador del gasto y la primera autoridad ejecutiva de la Institución.



Figura 1. Estructura Organizacional Institución Universitaria ITSa

Con esta estructura la Institución ha venido atendiendo todas las apuestas y retos propuestos en el marco del Plan de Desarrollo Institucional, tales como la apertura a nuevas áreas de saber, la creación de nuevos programas académicos a nivel de pregrado y posgrado con pertinencia y calidad, el fortalecimiento de la internacionalización, y la investigación, el bienestar, y la gestión sostenible, entre otros.

2.4 Análisis De Procesos

Con el objetivo de prestar servicios de calidad, ITSa cuenta con un Sistema de Gestión de Calidad bajo las normas NTC ISO 9001:2015 y NTC 5580:2011, siendo la cuarta Institución Pública de Educación Superior que obtuvo esta certificación a nivel nacional. Por otra parte, en el 2017 dio inicio a la implementación del Modelo Integrado de Planeación y Gestión – MIPG-, a partir de los lineamientos del Decreto 1499 de 2017, y actualmente se encuentra en proceso de implementación de los sistemas de Seguridad y Salud en el Trabajo y de conservación del Medio Ambiente bajo los estándares de las normas OHSAS 18001:2007, resolución 1111 de 2017 e ISO 14001:2015. Asimismo, la Institución ha venido implementando los controles requeridos para la seguridad y privacidad de la información conforme la norma ISO 27001:2013.

En contraste con lo anterior, la Institución fundamenta el desarrollo de su gestión y la adecuada prestación del servicio a través de cuatro (04) grandes macro procesos que se articulan propiciando y contribuyendo al cumplimiento de la misión institucional, los cuales se conforman de la siguiente manera:

- **Estratégicos:** Incluye aquellos procesos que soportan la estrategia institucional y provisión de comunicación dando respuesta a la visión Institucional. Además, orientan, evalúan y hacen seguimiento a la gestión Institucional.
- **Misionales:** Contribuyen directamente al cumplimiento de los objetivos y a la Misión de la Institución, actuando como sistema productivo para la prestación del servicio que el usuario requiere para satisfacer sus necesidades.
- **Apoyo:** Son los procesos que se conciben como soporte para el buen funcionamiento y operación de los procesos estratégicos y misionales.
- **Evaluación:** Son aquellos procesos responsables de verificar la adecuación, pertinencia, y cumplimiento de acciones previstas y resultados obtenidos de conformidad con lo planeado.

Tomando como punto de partida la declaración de la misión institucional, se han establecido objetivos y metas institucionales cuyo cumplimiento impacta en la eficiencia y eficacia de la prestación del servicio. Para hacer frente a esto, la Institución cuenta con un Mapa de Procesos basado en la metodología del ciclo de Deming (Planear-Hacer-Verificar-Actuar), mediante el cual se puede evidenciar la interacción existente entre los procesos para el desarrollo de la gestión y el cumplimiento de objetivos y metas trazadas.

De este modo, actualmente la Institución define diecisiete (17) procesos claves, los cuales se conciben como una serie de actividades que desarrolladas lógicamente y secuencialmente producen un producto o servicio que satisface las necesidades, expectativas y requisitos de las partes interesadas. Estos procesos, su interrelación y clasificación se aprecian en la siguiente figura:

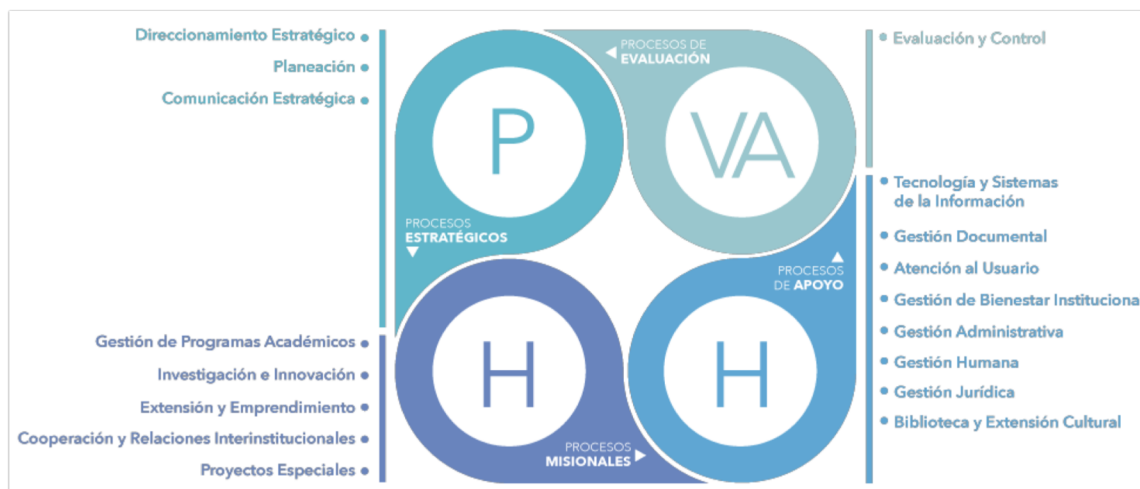


Figura 2. Mapa de Procesos Institución Universitaria ITSA

El proceso de Tecnología y Sistemas de Información -TSI- se encuentra dentro de los procesos de apoyo de la Institución, convirtiéndolo en un proceso de vital importancia para la continuidad del negocio por su transversalidad con todas las áreas. En este orden de ideas, el Proceso de Tecnologías y Sistemas de Información, se encarga de apoyar los procesos académicos y administrativos de la Institución, suministrando servicios tecnológicos y recursos informáticos de hardware, software, equipos de comunicación y medios audiovisuales, adecuados para el fortalecimiento de la misión institucional mediante procesos de adquisición administración, mantenimiento y/o desarrollo de los mismos, los cuales se ajustan a las necesidades de los diferentes procesos de la Institución (PETI, 2020).

Para conocer más acerca del mismo, se describe a continuación los principales aspectos del área de TSI de la Institución Universitaria ITSa.

3. Marco Conceptual del Proceso de TSI

3.1 Misión de TSI

Contribuir activamente a que la Institución Universitaria ITSA, logre sus objetivos estratégicos enmarcados en su PDI mediante el uso de Tecnologías de la Información apropiadas, eficaces y eficientes que satisfagan las necesidades de todos los procesos académicos y administrativos de la Institución.

3.2 Visión de TSI

En el 2023, el Proceso de Tecnologías y Sistemas de Información de la Institución Universitaria ITSA, será reconocido como un proceso estratégico de la misma, que apoye en la contribución al desarrollo de la región Caribe y a la transformación y mejora de la sociedad, a través del fortalecimiento del uso y fomento de las Tecnologías de la Información.

3.3 Objetivos Estratégicos de TSI

- Fortalecer los Sistemas de Información institucionales para la toma de decisiones en tiempo real (y el buen Gobierno Universitario) por medio del desarrollo de requerimientos que permitan que los Sistemas de Información se ajusten a las necesidades institucionales y del entorno.
- Liderar y elaborar los procesos de adquisición para la dotación de elementos tecnológicos que propendan por la innovación de los espacios de aprendizaje y creatividad, la interdisciplinariedad, y el fortalecimiento de los procesos institucionales.
- Fortalecer la infraestructura tecnológica en todo el quehacer universitario.
- Fortalecer y promover el uso y apropiación de las Tecnologías de la Información al interior de la Institución a través de estrategias, campañas, capacitaciones, elaboración e implementación de procedimientos y políticas que se potencialicen con los recursos tecnológicos adquiridos.
- Garantizar la correcta prestación de los servicios tecnológicos y sistemas de información a través de una infraestructura tecnológica apropiada, segura y eficiente.

3.4 Políticas de TSI

Se cuenta con distintas políticas, descritas en el Plan Estratégico de TI (PETI, 2020). Dentro de las más importantes se destacan:

- Política de Derecho de Autor
- Política de control de software y datos
- Política de adquisición y control de hardware
- Política para la adquisición de software
- Política para el uso de software
- Política para retirar de su uso hardware
- Política de seguridad de la Información
- Políticas del directorio activo para el dominio itsa.edu.local

3.5 Organigrama del Procesos de Tecnologías y Sistemas de Información de ITSa

A continuación, se presenta el organigrama del Proceso de Tecnologías y Sistemas de Información, el cual está constituido por un Líder de Proceso y tres subprocesos que corresponden a: Administración de Infraestructura Tecnológica, Administración de Sistemas de Información y Desarrollo de software; y Soporte Microinformático.

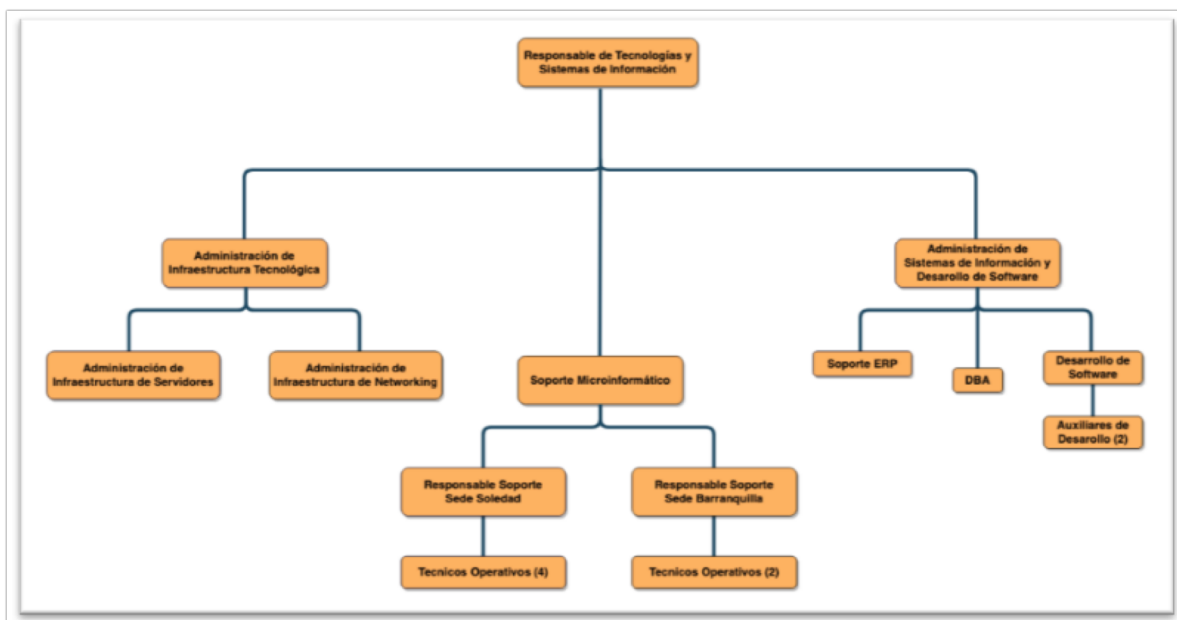


Figura 3. Organigrama Proceso de Tecnologías y Sistemas de Información

4. Análisis de Impacto

4.1 Descripción

Este tipo de análisis indica las vulnerabilidades de una organización, identifica los procesos de negocios más críticos, en este caso en el proceso de TSI, y describe el impacto potencial que tendría una interrupción de dichos procesos. Esta información permitirá seleccionar cual es la estrategia de recuperación más adecuada en caso de que se presente un desastre para así cumplir con los requerimientos del negocio.

4.2 Actividades

4.2.1 Identificación de procesos

En esta actividad se debe obtener una relación de los subprocesos que se llevan a cabo en el área de TSI y que se consideran necesarios para dar continuidad en caso de interrupción.

4.2.1.1 Procesos Críticos

Tabla1. Subprocesos de Tecnologías y Sistemas de Información

RELACIÓN DE PROCESOS	
Nombre del Proceso:	Tecnologías y Sistemas de Información
Descripción:	Coordinar, gestionar, asesorar, evaluar y controlar las herramientas, infraestructura tecnológica y Sistemas de Información, para la automatización, el soporte y el desarrollo de los procesos académicos y administrativos de la Institución, el desarrollo de Ciencia y Tecnología, de acuerdo con las metas y objetivos institucionales.
Nombre de Subproceso:	Administración de Infraestructura Tecnológica
Identificación:	SPR-TSI 01
Descripción:	Este subproceso es el encargado de gestionar los activos tecnológicos Core (Servidores y Networking),
Responsable:	Líder de Administración de Infraestructura
Nombre de Subproceso:	Soporte Microinformático
Identificación:	SPR-TSI 02
Descripción:	Este subproceso es el encargado se encarga de gestionar y administrar los activos microinformáticos y aplicaciones instalados en cada uno de estos, al igual que la conservación del buen estado de los dispositivos audiovisuales de la Institución, cubriendo las necesidades académicas, investigativas y administrativas de la Institución.
Nombre de Subproceso:	Administración de Sistemas de Información y Desarrollo de Software
Identificación:	SPR-TSI 03
Descripción:	Este subproceso es el encargado de gestionar y administrar los Sistemas de Información que apoyan los procesos académicos y administrativos de la Institución Universitaria ITSA. Además gestiona los desarrollos propios de la Institución. De igual manera. se encarga de investigar las nuevas tendencias tecnológicas en el mercado de las TIC y como resultado de esto, se desarrollan estrategias para la implementación y/o mejoras de los Sistemas de Información, brindando así innovación a los procesos de gestión de la Institución.
Responsable:	Líder de Administración de Sistemas de Información

4.2.2 Identificación de aplicaciones

En esta actividad se recogen datos de los recursos tecnológicos (Hardware, Software, Infraestructura) que soportan los procesos, con el fin de establecer cuales son los que le dan soporte directo a los servicios críticos. Así mismo se establecen unos rangos de criticidad para cada recurso:

Tabla 2. Rangos de Criticidad en aplicaciones de ITSA

RANGOS DE CRITICIDAD	
NIVEL	DESCRIPCIÓN
1	El proceso de Tecnologías y Sistemas de Información (TSI) no puede funcionar sin el sistema
2	El proceso de Tecnologías y Sistemas de Información (TSI) puede funcionar parcialmente sin el sistema
3	El proceso de Tecnologías y Sistemas de Información (TSI) puede funcionar sin el sistema

4.2.2.1 Relación de aplicaciones

Tabla 3. Relación de aplicaciones ITSA

Nombre:	Servicios adicionales Office 365
Código:	SSIS001
Descripción:	Acceso a servicio de almacenamiento en la nube de One Drive, Sistema de mensajería instantánea y video llamada a través de Sky Empresarial, Microsoft Teams, trabajo colaborativo con Office 365, entre otros
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Comunidad Universitaria
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	1

Nombre:	Página web institucional
Código:	SSIS002
Descripción:	Sitio web institucional que integra información sobre noticias, eventos de interés, políticas, normatividad y acceso unificado a servicios como correo electrónico, sistemas de información, herramientas de apoyo a la gestión académica y administrativa
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Comunidad Universitaria
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	1

Nombre:	Sistema administrativo y financiero GESTASOFT
Código:	SSIS003
Descripción:	Sistema de apoyo a la gestión administrativa y financiera de la Institución
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Comunidad Universitaria
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	1

Nombre:	Sistema académico ACADEMUSOFT
Código:	SSIS004
Descripción:	Sistema de apoyo a la administración de los procesos académicos como admisiones, matrículas, calificaciones, certificaciones, etc.
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Comunidad Universitaria
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	1

Nombre:	Aula Virtual MOODLE
Código:	SSIS005
Descripción:	Sistema de apoyo a los docentes a través del cual se crea un ambiente virtual que permite la publicación de contenidos, actividades, evaluaciones, foros, etc. Todos estos recursos en línea están soportados bajo la plataforma Moodle
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Comunidad Universitaria
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	2

Nombre:	Directorio Activo Institucional
----------------	--

Código:	SSIS006
Descripción:	Sistema de administración y gestión centralizada de las cuentas de usuarios, utilizadas para el acceso unificado a los distintos servicios y sistemas de información institucionales
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Comunidad Universitaria
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	1

Nombre:	Soporte Técnico Informático STI
Código:	SSIS007
Descripción:	Sistema para registro de solicitudes de soporte técnico al grupo de Tecnologías y Sistemas de Información. Funciona sobre plataforma GLPI
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Funcionarios y Contratistas
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	1

Nombre:	Sistema de solicitudes de Infraestructura física SIFIS
Código:	SSIS008
Descripción:	Sistema para reporte de fallas y solicitudes de mantenimiento al grupo de Infraestructura y Planta Física. Funciona sobre plataforma GLPI
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Responsable Planta Física Funcionarios y Contratistas
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	3

Nombre:	Sistema GLPI solicitudes de apertura de sistema
Código:	SSIS009

Descripción:	Sistema para solicitudes de apertura de sistema para ingreso de notas extemporáneas por parte de los docentes
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Decanaturas, Docentes
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	3

Nombre:	GLPI Calidad
Código:	SSIS010
Descripción:	Sistema de apoyo al Sistema de Gestión de la Calidad para el registro de planes de acción correctivos, preventivos, de mejora y tratamiento de servicios no conformes
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Responsable Sistema de Gestión de la Calidad Funcionarios y Contratistas
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	3

Nombre:	Sistema de apoyo al préstamo de recursos SISPEF
Código:	SSIS011
Descripción:	Sistema de apoyo al servicio de préstamo de recursos físicos y equipos de laboratorios mediante el registro a través de la captura de la huella digital
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Funcionarios, Contratistas y Docentes
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	2

Nombre:	Sistema de apoyo para Registro de Activos SIRA
Código:	SSIS012

Descripción:	Sistema de apoyo al módulo administrativo de almacén para el registro de las asignaciones de activos a los diferentes funcionarios y espacios físicos de la Institución, tanto en el campus Soledad como en el campus Barranquilla
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Funcionarios de Almacén
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	3

Nombre:	Sistema para publicación de revistas científicas OJS
Código:	SSIS013
Descripción:	Sistema de apoyo al grupo de investigación sobre la plataforma OPEN JOURNAL SYSTEM, diseñado para la publicación de artículos y revistas científicas de la Institución
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Grupos de Investigación Comunidad Universitaria
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	3

Nombre:	Sistema Bibliográfico SIABUC
Código:	SSIS014
Descripción:	Software de gestión bibliográfica que permite la categorización del material bibliográfico, la circulación y el préstamo a toda la comunidad universitaria
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Proceso de Biblioteca y Extensión Cultural Comunidad Universitaria
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	3

Nombre:	Sistema para Reporte de horas cátedra
Código:	SSIS015

Descripción:	Sistema de Información de apoyo al proceso de Gestión Humana para el registro de las horas dictadas por los docentes catedráticos durante el día
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Funcionarios de Gestión Humana Docentes
Contacto de Soporte:	Soporte al servicio: Oficina de Talento Humano. Ext. 118 Email: talentohumano@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. 12:00 m y 2:00 p.m. – 6:00 p.m. Soporte a infraestructura: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	3

Nombre:	Sistema SINEVO
Código:	SSIS016
Descripción:	Sistema de Información de apoyo al Grupo de Investigación, destinado al registro en línea de los proyectos de investigación realizados por los estudiantes de la Institución
Responsable:	Vicerrectoría de Extensión e Investigación
Usuario Objetivo:	Grupos de Investigación Estudiantes Docentes
Contacto de Soporte:	Soporte al servicio: Oficina de Acreditación. Ext. 113 Email: djruiz@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. 12:00 m y 2:00 p.m. – 6:00 p.m. Soporte a infraestructura: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	3

Nombre:	Sistema para aplicación de encuestas en línea Limesurvey
Código:	SSIS017
Descripción:	Sistema para aplicación de encuestas de satisfacción en línea a través de la plataforma libre Limesurvey
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Comunidad Universitaria
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	2

Nombre:	Sistema Integrado de Autoevaluación, Acreditación y Aseguramiento de la Calidad AAA
Código:	SSIS018

Descripción:	Sistema integrado de gestión institucional como apoyo a la toma de decisiones a través del análisis y control de indicadores claves que propenden con la prestación de un servicio de calidad
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Funcionarios Contratistas Docentes
Contacto de Soporte:	Soporte al servicio: Acreditación y Aseguramiento de la Calidad. Ext. 113 Email: marias@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. 12:00 m y 2:00 p.m. – 6:00 p.m. Soporte a infraestructura: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	2

Nombre:	Sistema PAIP (Programa de Acompañamiento Integral Permanente)
Código:	SSIS019
Descripción:	Sistema de apoyo a Bienestar Universitario, integrado con la plataforma académica para el análisis de los casos de deserción estudiantil
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Funcionarios de Bienestar Universitario Estudiantes Docentes
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	3

Nombre:	Sistema local SNIES y SPADIES
Código:	SSIS021
Descripción:	Sistema de información local que permite consolidar y enviar los reportes solicitados por el Sistema de Información de Instituciones de Educación Superior (SNIES) y el Sistema para la Prevención de la Deserción en las Instituciones de Educación Superior (SPADIES)
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Oficina de Planeación
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	3

Nombre:	Sistema para Evaluación Docente
Código:	SSIS020
Descripción:	Sistema de información de apoyo a la oficina de Gestión Humana que permite medir la calidad de cada docente de acuerdo al desempeño de sus actividades académicas
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Funcionarios de Gestión Humana

	Estudiantes Docentes
Contacto de Soporte:	Soporte al servicio: Gestión del Talento Humano. Ext. 118 Email: talentohumano@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. 12:00 m y 2:00 p.m. – 6:00 p.m. Soporte a infraestructura: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	3

Nombre:	Sistema para Carnetización
Código:	SSIS022
Descripción:	Sistema de Información integrado con la plataforma académica y administrativa, que permite la generación e impresión de los carnets institucionales para la identificación de toda la comunidad universitaria
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Estudiantes Docentes Funcionarios Contratistas
Contacto de Soporte:	Soporte al servicio: Atención al usuario. Ext. 118 Email: carnetizacion@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. 12:00 m y 2:00 p.m. – 6:00 p.m. Soporte técnico a infraestructura: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	2

Nombre:	Ambientes de Desarrollo y Pruebas de Software
Código:	SSIS023
Descripción:	Plataformas conformadas por un conjunto de herramientas y sistemas de información orientados al desarrollo y pruebas de software académico y administrativo incluyendo un sistema de control de versiones y un gestor de administración de proyectos de desarrollo de software
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Desarrolladores de software
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	1

Nombre:	Aplicación móvil App ITSa
Código:	SSIS024
Descripción:	Solución móvil que amplía el alcance de los sistemas de información a los dispositivos móviles Android e iPhone, permitiendo consultar información institucional y académica de interés de manera fácil y rápida

Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Comunidad Universitaria
Contacto de Soporte:	Soporte al servicio: Oficina de Acreditación. Ext. 113 Email: djruiz@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. 12:00 m y 2:00 p.m. – 6:00 p.m. Soporte técnico a infraestructura: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	2

Nombre:	Sistema de Monitoreo de red
Código:	SSIS025
Descripción:	Software para el monitoreo en tiempo real del comportamiento de la red, permitiendo conocer fallas y cuellos de botella, analizar los casos y brindar las soluciones pertinentes para la optimización de la red institucional
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Comunidad Universitaria
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	1

Nombre:	Sistema NTP de sincronización horaria de dispositivos
Código:	SSIS026
Descripción:	Servicio de sincronización de reloj de dispositivos y equipos conectados a través de la red para controlar y registrar eventos en tiempo real con exactitud horaria
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Comunidad Universitaria
Contacto de Soporte:	Soporte al Servicio: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m. y sábados de 8:00 a.m. – 1:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	2

Nombre:	Repositorios bibliográficos virtuales
Código:	SSIS027
Descripción:	Publicación en los sistemas de información institucionales el acceso a diferentes repositorios bibliográficos virtuales como Scopus, Normas técnicas ICONTEC sobre soldadura, administración logística y portuaria, E-libro, ScienceDirect
Responsable:	Biblioteca y Extensión Cultural

Usuario Objetivo:	Comunidad Universitaria
Contacto de Soporte:	Soporte al servicio: Biblioteca y Extensión Cultural. Ext. 128 Email: ldonado@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. 12:00 m y 2:00 p.m. – 6:00 p.m. Soporte técnico a infraestructura: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	3

Nombre:	Sistema Web I-Business
Código:	SSIS028
Descripción:	Sistema de Información de apoyo a la Facultad de Ciencias Económicas y Administrativas, relacionado con actividades académicas sobre trámites aduaneros
Responsable:	Tecnologías y Sistemas de Información
Usuario Objetivo:	Facultad de Ciencias Económicas y Administrativas Docentes Funcionarios Contratistas
Contacto de Soporte:	Soporte al servicio: Facultad de Ciencias Económicas y Administrativas Email: hjaafar@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. 12:00 m y 2:00 p.m. – 6:00 p.m. Soporte técnico a infraestructura: Tecnología y Sistemas de la información. Ext. 120 - 215 Email: soportevirtualesistemas@itsa.edu.co Horario: lunes a viernes de 8:00 a.m. – 6:00 p.m.
Acuerdos de nivel de servicios:	Disponibilidad: 99%
Rango de Criticidad:	3

5. Responsables de la Continuidad de los Servicios de TI en la Institución

La siguiente tabla presenta los responsables del mayor nivel de continuidad de los servicios de TI en la Institución Universitaria ITSA:

Tabla 4. Responsables Continuidad del Servicio de TI

INTEGRANTES
Rector
Vicerrector Administrativo y Financiero
Responsable de TSI
Responsable Comunicaciones Estratégicas
Responsable Planta Física

En este orden de ideas, se propone la creación de un comité que será el encargado de gestionar la Continuidad de Servicios de TI. Éste debería formarse al interior del proceso de Tecnologías y Sistemas de Información como lo muestra la siguiente Ilustración:

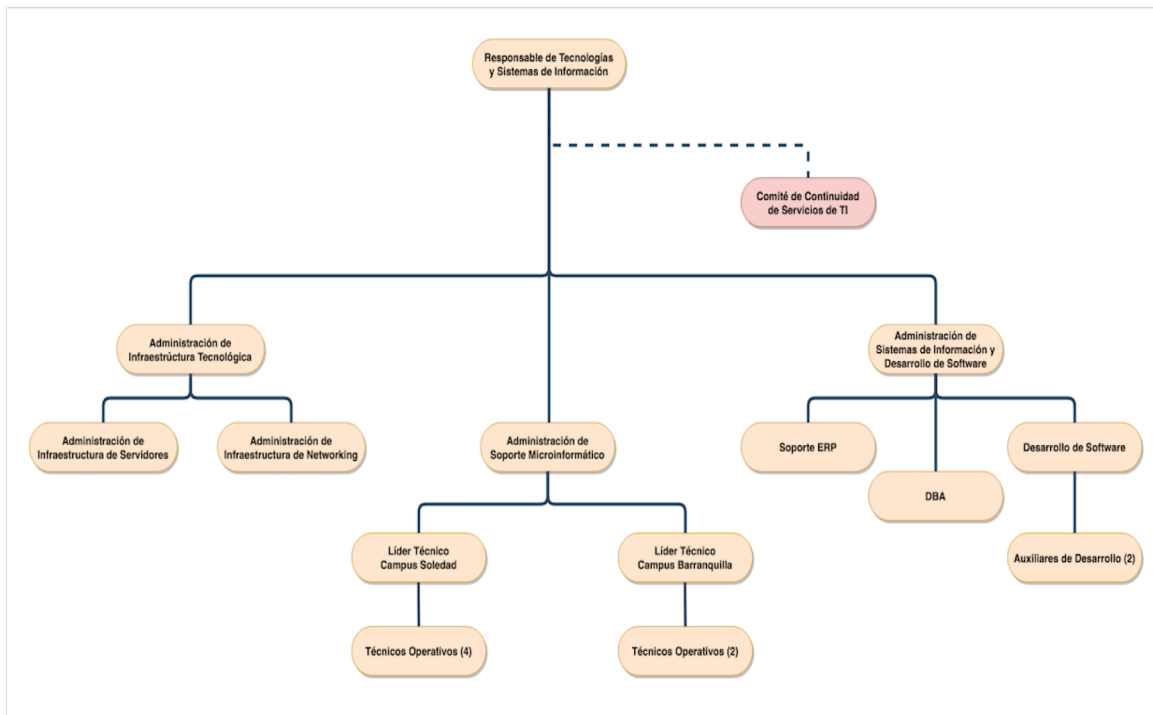


Figura 4. Organigrama Proceso de Tecnologías y Sistemas de Información con el comité propuesto de Continuidad de Servicios de TI

6. Identificación de Activos

Para los subprocesos de TSI, se realiza un inventario de los activos (recursos de una compañía que son necesarios para la consecución de sus objetivos y que sería delicado que se vieran comprometidos ante un incidente que afecte la continuidad del negocio). Para ello, se determina quién tiene a cargo cada activo, su ubicación y su valor estimado. El inventario de activos va a permitir conocer de manera puntual qué es lo que se tiene que proteger, su categoría, su responsable, su ubicación actual y valor monetario.

Tabla 5. Determinación de procesos críticos dentro de los subprocesos de TSI

DETERMINACIÓN DE LOS PROCESOS CRÍTICOS	
NOMBRE DEL SUBPROCESO	PRIORIDAD
Administración de Infraestructura Tecnológica	ALTA
Soporte Microinformático	ALTA
Administración de Sistemas de Información y Desarrollo de Software	ALTA

Tabla 6. Identificación de Activos – Subproceso Administración de Infraestructura Tecnológica

IDENTIFICACIÓN DE ACTIVOS – SUBPROCESO ADMINISTRACIÓN DE INFRAESTRUCTURA TECNOLÓGICA				
ACTIVO	RESPONSABLE	UBICACIÓN	VALOR ESTIMADO	OBSERVACIONES
Datacenter Institucional	Proc. Tecnologías y Sistemas de Información	Oficina Sistemas	\$1.200.000.000	
Servicio de Datacenter en la Nube	Proc. Tecnologías y Sistemas de Información	Datacenter Proveedor de Servicio	\$200.000.000	Valor anual del servicio de Cloud Datacenter
Servicios de Conectividad	Proc. Tecnologías y Sistemas de Información	Institución	\$250.000.000	Valor anual de los servicios de Internet, Conectividad y Troncales SIP
Servidor de Correo Electrónico	Proc. Tecnologías y Sistemas de Información	Oficina Sistemas	\$10.000.000	
Firewall	Proc. Tecnologías y Sistemas de Información	Oficina Sistemas	\$150.000.000	
Cableado Estructurado	Proc. Tecnologías y Sistemas de Información	Institución	\$100.000.000	
Infraestructura de redes	Proc. Tecnologías y Sistemas de Información	Institución	\$350.000.000	
Servidores Virtualizados	Proc. Tecnologías y Sistemas de Información	Oficina Sistemas	\$30.000.000	
Sistema de respaldo Eléctrico (Planta eléctrica y UPS)	Proc. Tecnologías y Sistemas de Información	Oficina Sistemas	\$200.000.000	
Sistema de Antivirus	Proc. Tecnologías y Sistemas de Información	Institución	\$30.000.000	Valor anual de la suscripción al antivirus
Suscripción servicios de Microsoft	Proc. Tecnologías y Sistemas de Información	Institución	\$90.000.000	Valor anual de la suscripción a servicios de Microsoft
Total de Activos			\$2.610.000.000	

Tabla 7. Identificación de Activos – Subproceso Soporte Microinformático

IDENTIFICACIÓN DE ACTIVOS – SUBPROCESO SOPORTE MICROINFORMÁTICO				
ACTIVO	RESPONSABLE	UBICACIÓN	VALOR ESTIMADO	OBSERVACIONES
Servicios de Conectividad	Proc. Tecnologías y Sistemas de Información	Institución	\$250.000.000	Valor anual de los servicios de Internet, Conectividad y Troncales SIP
Servidor de Correo Electrónico	Proc. Tecnologías y Sistemas de Información	Oficina Sistemas	\$10.000.000	
Cableado Estructurado	Proc. Tecnologías y Sistemas de Información	Institución	\$100.000.000	
Impresoras	Proc. Tecnologías y Sistemas de Información	Oficinas	\$80.000.000	
Equipos de Cómputo Académicos	Proc. Tecnologías y Sistemas de Información	Salas de cómputo y Laboratorios	\$3.500.000.000	
Equipos de Computo Administrativos	Proc. Tecnologías y Sistemas de Información	Oficinas	\$1.000.000.000	
Softwares Académicos	Proc. Tecnologías y Sistemas de Información	Salas de cómputo y Laboratorios	\$1.600.000.000	Conjunto de licencias académicas, dentro de las cuales encontramos licenciamientos por suscripción y licenciamientos perpetuos
Sistema de Antivirus	Proc. Tecnologías y Sistemas de Información	Institución	\$30.000.000	Valor anual de la suscripción al antivirus
Suscripción servicios de Microsoft	Proc. Tecnologías y Sistemas de Información	Institución	\$90.000.000	Valor anual de la suscripción a servicios de Microsoft
Medios Audiovisuales (Televisores y Video Beams)	Proc. Tecnologías y Sistemas de Información	Institución	\$200.000.000	
Sistema de Control de Acceso	Proc. Tecnologías y Sistemas de Información	Institución	\$200.000.000	
Sistema de Videovigilancia (CCTV)	Proc. Tecnologías y Sistemas de Información	Institución	\$300.000.000	
Total de Activos			\$7.360.000.000	

Tabla 8. Identificación de Activos – Subproceso de Administración de Sistemas de Información y Desarrollo de Software

IDENTIFICACIÓN DE ACTIVOS – SUBPROCESO ADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN Y DESARROLLO DE SOFTWARE				
ACTIVO	RESPONSABLE	UBICACIÓN	VALOR ESTIMADO	OBSERVACIONES
Servicios de Conectividad	Proc. Tecnologías y Sistemas de Información	Institución	\$250.000.000	Valor Anual de los servicios de Internet, Conectividad y Troncales SIP
ERP Institucional (Academusoft y Gestasoft)	Proc. Tecnologías y Sistemas de Información	Oficina Sistemas	\$250.000.000	
Aula Virtual Moodle	Proc. Tecnologías y Sistemas de Información	Oficina Sistemas	\$50.000.000	
Sistema de Información Triple A	Proc. Tecnologías y Sistemas de Información	Oficina Sistemas	\$140.000.000	
App Móvil ITSA	Proc. Tecnologías y Sistemas de Información	Oficina Sistemas	\$80.000.000	
Demás Sistemas de Información de desarrollo propio, adquiridos y/o libres adaptados	Proc. Tecnologías y Sistemas de Información	Oficina Sistemas	\$500.000.000	Siabuc, Sinevo, Limsurvey, GLPI, Orfeo, SIRA, PAIP, OJS, etc
Bases de datos (General)	Proc. Tecnologías y Sistemas de Información	Oficina Sistemas	\$300.000.000	
Servidores Virtualizados	Proc. Tecnologías y Sistemas de Información	Oficina Sistemas	\$30.000.000	
Suscripción servicios de Microsoft	Proc. Tecnologías y Sistemas de Información	Institución	\$90.000.000	Valor anual de la suscripción a servicios de Microsoft
Total de Activos			\$1.690.000.000	

7. Definición de Impactos

Como primer paso de la definición de impactos, se establece una tabla asociada a las pérdidas financieras (se usa una escala de 1 a 5, donde 1 es el rango más bajo, y 5 el rango más alto). Se considera el valor de los activos identificados en el literal anterior. No obstante, es importante anotar que la valoración de pérdidas no es una cuestión sencilla, ya que pueden concurrir aspectos intangibles, tales como la imagen de la organización ante sus clientes (algunos criterios que pueden ayudar: costo de horas de trabajo perdidas, al no poder usar las aplicaciones que no tengan alternativa manual o cuyo tratamiento manual suponga una pérdida de eficiencia importante, ingresos dejados de percibir, penalizaciones por incumplimiento de contratos con clientes, sanciones administrativas por incumplimiento de leyes debido a la falta de control en situación de desastre, gastos financieros, etc.).

Teniendo en cuenta que el total de los activos necesarios para el funcionamiento de los tres(3) subprocesos críticos de Continuidad de Servicio de TI son:

Tabla 9. Identificación de Activos necesarios para el funcionamiento de los procesos de Continuidad del Servicio de TI

NOMBRE DEL SUBPROCESO	TOTAL DE ACTIVOS
Administración de Infraestructura Tecnológica	\$2.610.000.000
Soporte Microinformático	\$7.360.000.000
Administración de Sistemas de Información y Desarrollo de Software	\$1.690.000.000

A continuación se presenta la tabla asociada a las pérdidas financieras por cada uno:

Tabla 10. Pérdidas financieras asociadas al subproceso Administración de Infraestructura Tecnológica

PÉRDIDA FINANCIERA - ADMINISTRACIÓN DE INFRAESTRUCTURA TECNOLÓGICA	
VALOR	DESCRIPCIÓN
5	\$2.088.000.000 - \$2.610.000.000
4	\$ 1.566.000.000 - \$2.088.000.000
3	\$1.044.000.000 - \$1.566.000.000
2	\$ 522.000.000 - \$1.044.000.000
1	\$0 - \$ 522.000.000

Tabla 11. Pérdidas financieras asociadas al subproceso Soporte Microinformático

PÉRDIDA FINANCIERA - SOPORTE MICROINFORMÁTICO	
VALOR	DESCRIPCIÓN
5	\$ 5.888.000.00- \$7.360.000.000
4	\$4.416.000.000 - \$5.888.000.00
3	\$2.944.000.000 - \$4.416.000.000
2	\$1.472.000.00 - \$2.944.000.000
1	\$0 - \$ 1.472.000.00

Tabla 12. Pérdidas financieras asociadas al subproceso Administración de Sistemas de Información y Desarrollo de Software

PÉRDIDA FINANCIERA - ADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN Y DESARROLLO DE SOFTWARE	
VALOR	DESCRIPCIÓN
5	\$1.352.000.000 - \$1.690.000.000
4	\$1.014.000.000 - \$1.352.000.000
3	\$676.000.000 - \$1.014.000.000
2	\$338.000.000 - \$676.000.000
1	\$0 - \$338.000.000

7.1 Pérdida de la Continuidad

Como segundo paso de la definición de impactos, se establece una tabla asociada a la pérdida de continuidad en los servicios (escala de 1 a 5). Para ello se define y se considera para el proceso de TSI, el Periodo Máximo de Interrupción o Inactividad (Maximun Tolerable Downtime - MTD) que es aquel en que las pérdidas sufrirían un aumento significativo, afectarían de forma grave a la Institución y las funciones no podrían ser reasumidas. Además, se determinan tres parámetros estrechamente relacionados con la recuperación: Tiempo de trabajo de Recuperación (WRT), Tiempo de Recuperación Objetivo (RTO) y Punto de Recuperación Objetivo (RPO). El RTO: urgencia que las diferentes unidades de negocio precisan para volver a su funcionamiento habitual. El RPO: punto más reciente en el tiempo en el que los sistemas pueden ser recuperados, reflejando cuánta es la cantidad de información que una organización puede permitirse perder sin que le afecte negativamente. Por tanto, el RPO determina la periodicidad con la que deben salvaguardarse los datos para todos aquellos procesos de negocio. El WRT: máxima cantidad de tiempo tolerable requerido para verificar la integridad de los sistemas y de los datos.

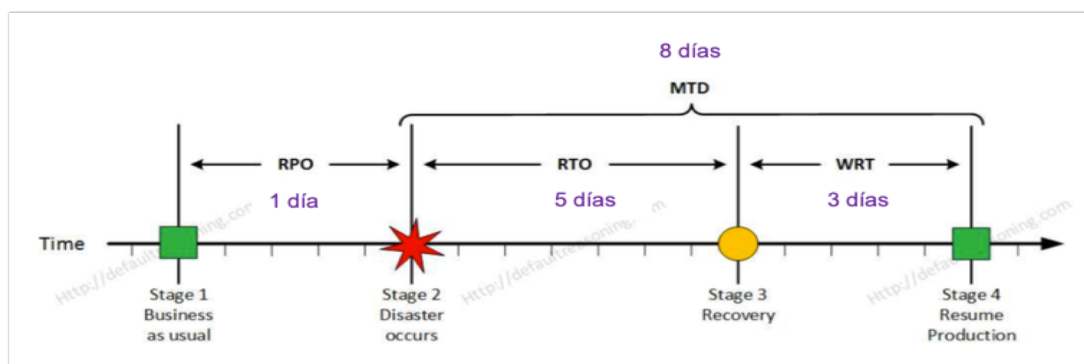


Figura 5. Parámetros RTO,RPO,WRT,MTD

Tabla 13. Pérdida de Continuidad de los Servicios de TI en términos de MTD, RTO y RPO

NOMBRE DEL SUBPROCESO	TOTAL DE ACTIVOS
Administración de Infraestructura Tecnológica	MTD: 8 días calendario RTO: 5 días calendario RPO: 1 día
Soporte Microinformático	MTD: 5 días calendario RTO: 2 días calendario RPO: 2 días calendario
Administración de Sistemas de Información y Desarrollo de Software	MTD: 5 días calendario RTO: 4 días RPO: 1 día

Tabla 14. Pérdida de Continuidad de los Servicios de TI

NIVEL	PÉRDIDA DE CONTINUIDAD
1	< =1 día
2	2
3	4
4	5
5	8 días

8. Riesgos Asociados

A continuación, se definen los principales riesgos asociados a la gestión de la continuidad de servicios de TI, para cada uno de los subprocesos de TSI.

Tabla 15. Pérdida Riesgos Asociados Subprocesos TSI
ADMINISTRACIÓN DE INFRAESTRUCTURA TECNOLÓGICA

R1	Impacto en la continuidad de los servicios debido a falla tecnológica.
R2	Impacto en la continuidad de los servicios por la gestión indebida de las configuraciones de los dispositivos tecnológicos.
R3	Impacto financiero producido por la pérdida total de los dispositivos tecnológicos, debido a desastres naturales.
R4	Impacto financiero por la no prestación del servicio de inscripción de matrículas debido a fallas en los dispositivos tecnológicos.

SOPORTE MICROINFORMÁTICO

R1	Impacto en la continuidad de los servicios debido a la propagación de malware/ransomware.
R2	Impacto en la continuidad de los servicios debido a la no disponibilidad de repuestos de hardware informático.
R3	Impacto financiero producido por la pérdida total de los dispositivos tecnológicos, debido a desastres naturales.
R4	Impacto financiero por la no prestación del servicio académico debido a la gestión inoportuna de fallas en la plataforma Microsoft Teams.

ADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN Y DESARROLLO DE SOFTWARE

R1	Impacto en la continuidad de los servicios debido a un fallo en la plataforma de gestión académica y administrativa.
R2	Impacto en la continuidad de los servicios debido a caída del servicio de Base de Datos.
R3	Impacto financiero producido por la no disponibilidad de la plataforma de gestión de matrículas.
R4	Impacto financiero producido por la no disponibilidad de la plataforma de aula virtual.

Luego se valoran los riesgos inherente, de exposición y residual. Dentro de las medidas de tratamiento se deben considerar la creación, complemento o mejoramiento de los planes de continuidad:

Tabla 16. Valoración de Riesgos de Administración de Infraestructura Tecnológica

ADMINISTRACIÓN DE INFRAESTRUCTURA TECNOLÓGICA											
RIESGO	IMP	PROB	RI	MEDIDAS EXISTENTES	IMP	PROB	RE	MEDIDAS PROPUESTAS	IMP	PROB	RR
Impacto en la continuidad de los servicios debido a falla tecnológica.	5	0,8	4,0	ME1: Se tiene redundancia de máquinas virtuales. ME2:Se cuenta con una UPS que permite por un tiempo corto mantener los sistemas funcionando. ME3:Se cuenta con una planta eléctrica que permite por un tiempo moderado mantener los sistemas funcionando.	3	0,5	1,5	MP1: Contar con una sistema de sensores en el Data Center que a través de alertas adviertan de fallas con el sistema eléctrico, de refrigeración, entre otros. MP2: Mantener en buenas condiciones la infraestructura eléctrica. MP3: Contar con una planta eléctrica con capacidad suficiente para permitir por mayor tiempo la continuidad de los servicios. MP4: Creación de Planes de Continuidad para identificar y gestionar las amenazas actuales y futuras del proceso de Tecnologías y Sistemas de Información.	2	0,2	0,4
Impacto en la continuidad de los servicios por la gestión indebida de las configuraciones de los dispositivos tecnológicos.	4	0,9	3,6	ME1:Documentación básica de las configuraciones realizadas a los dispositivos. ME2:Capacitación al personal de tecnología sobre la gestión de configuraciones.	3	0,7	2,1	MP1: Implementar estándares del sector, por ejemplo ITIL.	2	0,4	0,8
Impacto financiero producido por la pérdida total de los dispositivos tecnológicos, debido a desastres naturales.	5	0,3	1,5	ME1: Contratación de una póliza de seguro contra todo riesgo. ME2: Punto de redundancia de datos en otra ciudad.	3,5	0,2	0,7	MP1: Acondicionamiento del cuarto de servidores de acuerdo a estándares TIER.	2	0,1	0,2
Impacto financiero por la no prestación del servicio de inscripción de matrículas debido a fallas en los dispositivos tecnológicos.	5	0,8	4,0	ME1: Se tiene redundancia de máquinas virtuales. ME2:Se cuenta con una UPS que permite por un tiempo corto mantener los sistemas funcionando. ME3:Se cuenta con una planta que permite por un tiempo moderado mantener los sistemas funcionando.	3	0,5	1,5	MP1: Contar con un sistema de sensores en el Data Center que a través de alertas adviertan de fallas con el sistema eléctrico, de refrigeración, entre otros. MP2: Mantener en buenas condiciones la infraestructura eléctrica. MP3: Contar con una planta eléctrica con capacidad suficiente para permitir por mayor tiempo la continuidad de los servicios. MP4: Creación de Planes de Continuidad para identificar y gestionar las amenazas actuales y futuras del proceso de Tecnologías y Sistemas de Información.	2	0,2	0,4
PROMEDIOS	4,8	0,7	2,3		3,1	0,5	1,1		2,0	0,2	0,2

Tabla 17. Valoración de Riesgos de Soporte Microinformático

ADMINISTRACIÓN DE SOPORTE MICROINFORMÁTICO											
RIESGO	IMP	PROB	RI	MEDIDAS EXISTENTES	IMP	PROB	RE	MEDIDAS PROPUESTAS	IMP	PROB	RR
Impacto en la continuidad de los servicios debido a la propagación de malware/ransomware.	4	0,8	3,2	ME1: Implementación de Antivirus. ME2: Implementación de un IPS (Intrusion Prevention System).	3	0,3	0,9	MP1: Detección de amenazas de día 0. MP2: Implementación de Estándares de la norma ISO 2700:1.	1	0,2	0,2
Impacto en la continuidad de los servicios debido a la no disponibilidad de repuestos de hardware informático.	3,8	0,9	3,42	ME1: Contratación de Garantía con el fabricante por un tiempo de 5 años. ME2: Mantenimiento Preventivo de los Equipos.	3	0,5	1,5	MP1: Disminución del tiempo para contar con los equipos o repuestos en caso de daño. MP2: Contar con redundancia de equipos físicos en bodega.	2,5	0,2	0,5
Impacto financiero producido por la pérdida total de los dispositivos tecnológicos, debido a desastres naturales.	5	0,3	1,5	ME1: Contratación de una póliza de seguro contra todo riesgo. ME2: Punto de redundancia de datos en otra ciudad.	3,5	0,2	0,7	MP1: Acondicionamiento del cuarto de servidores de acuerdo a estándares TIER.	2	0,1	0,2
Impacto financiero por la no prestación del servicio académico debido a la gestión inoportuna de fallas en la plataforma Microsoft Teams.	4	0,7	2,8	ME1: Monitoreo de la herramienta ante reporte de fallas. ME2: Soporte actual por parte del proveedor.	2,5	0,4	1	MP1: Contar con una herramienta virtual de enseñanza alterna. MP2: Capacitación al personal administrativo en la herramienta alternativa.	1,5	0,2	0,3
PROMEDIOS	4,2	0,7	2,7		3,0	0,4	1,0		1,8	0,2	0,3

Tabla 18. Valoración de Riesgos de Administración de Sistemas de Información y Desarrollo de Software

ADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN Y DESARROLLO DE SOFTWARE											
RIESGO	IMP	PROB	RI	MEDIDAS EXISTENTES	IMP	PROB	RE	MEDIDAS PROPUESTAS	IMP	PROB	RR
Impacto en la continuidad de los servicios debido a un fallo en la plataforma de gestión académica y administrativa.	5	0,8	4	ME1: Copia de seguridad de la Base de Datos y de la Aplicación.	4	0,6	2,4	MP1: Cumplimiento de los Estándares del Sector. MP2: Uso de sistema de gestión de versiones.	2	0,3	0,6
Impacto en la continuidad de los servicios debido a caída del servicio de Base de Datos.	5	0,7	3,5	ME1: Copia de Seguridad de la Base de Datos. ME2: Redundancia en el Servidor de Base de Datos.	3	0,4	1,2	MP1: Realización de copias de seguridad automatizadas en integradas. MP2: Replicación Geográfica activa.	1	0,1	0,1
Impacto financiero producido por la no disponibilidad de la plataforma de gestión de matrículas.	5	0,8	4	ME1: Copia de seguridad de la Base de Datos y de la Aplicación.	4	0,6	2,4	MP1: Cumplimiento de los Estándares del Sector. MP2: Uso de sistema de gestión de versiones.	2	0,3	0,6
Impacto financiero producido por la no disponibilidad de la plataforma de aula virtual.	5	0,8	4	ME1: Copia de seguridad de la Base de Datos y de la Aplicación. ME2: Existencia de Estructura Compleja compuesta por seis (6) servidores.	4	0,6	2,4	MP1: Cumplimiento de los Estándares del Sector. MP2: Uso de sistema de gestión de versiones.	2	0,3	0,6
PROMEDIOS	5,0	0,8	3,9		3,8	0,6	2,1		1,8	0,6	0,5

A continuación, se propone el siguiente mapa de riesgos, el cual es elaborado en una cuadrícula de impacto y probabilidad, donde se ubica cada subproceso en términos de Riesgo Inherente RI, Riesgo de Exposición RE y Riesgo Residual RR.

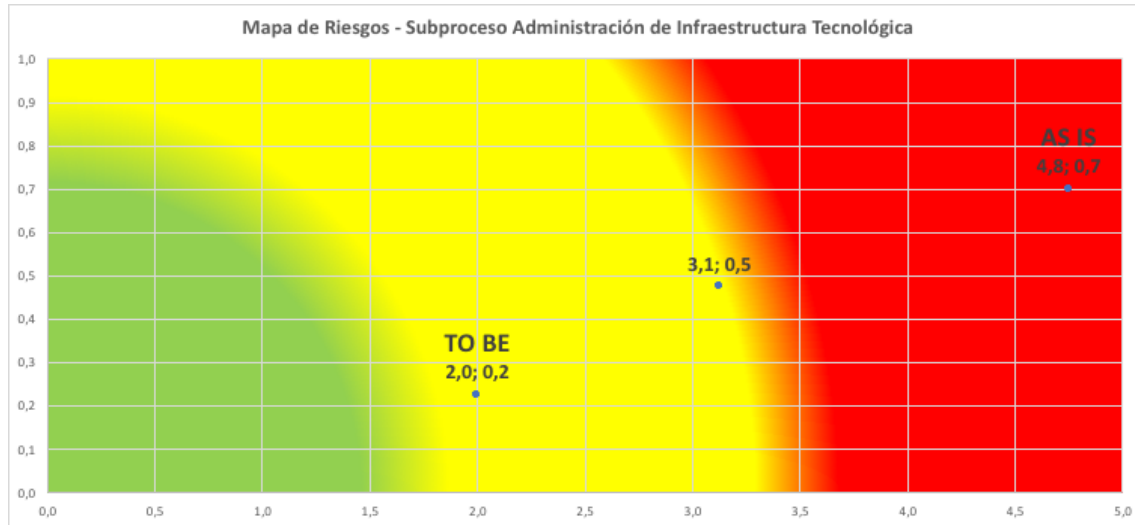


Figura 6. Mapa de Riesgos para el Subproceso Administración de Infraestructura Tecnológica

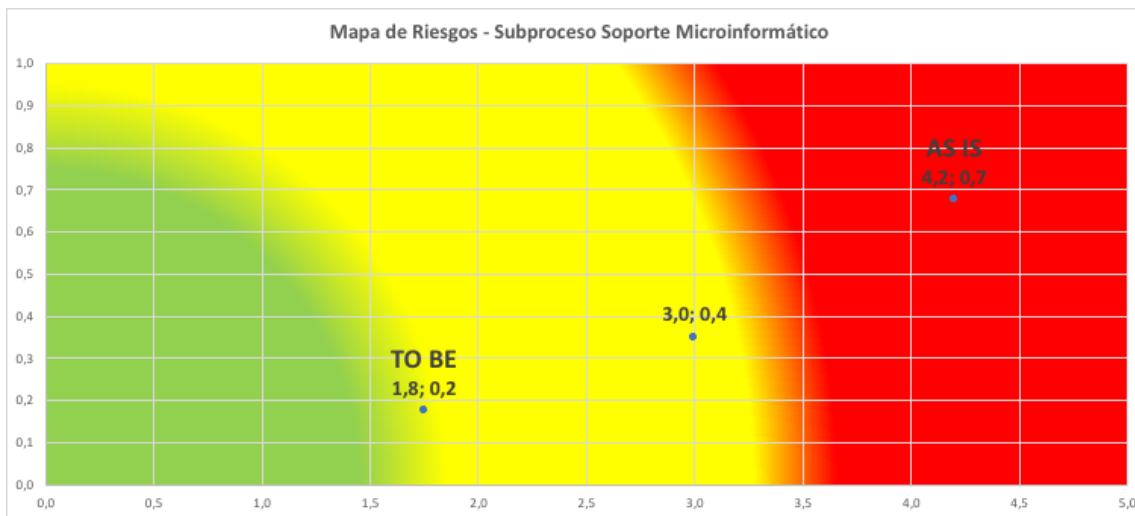


Figura 7. Mapa de Riesgos para el Subproceso Soporte Microinformático

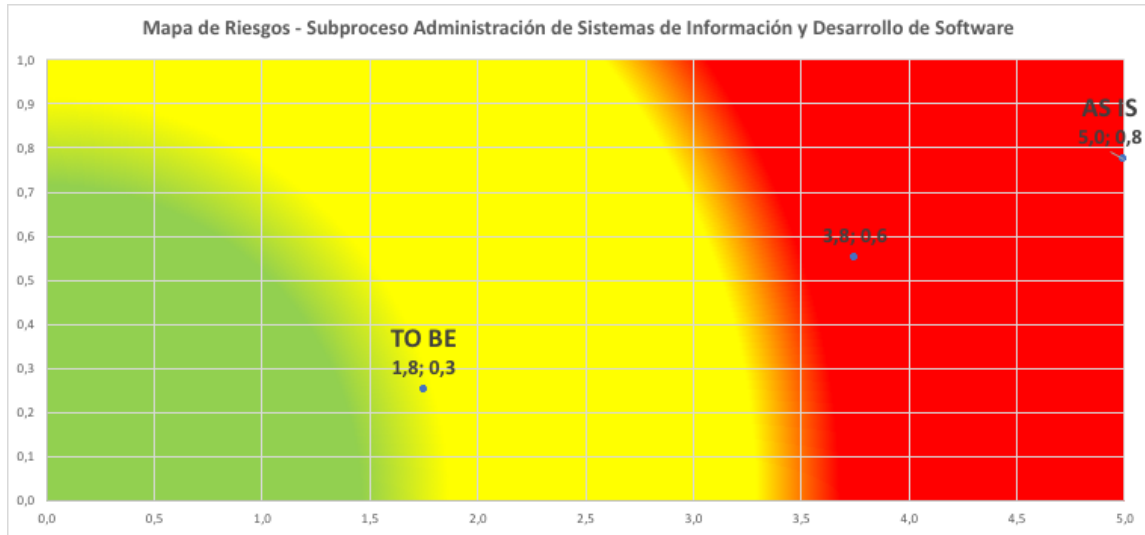


Figura 8. Mapa de Riesgos para el Subproceso Administración de Sistemas de Información y Desarrollo de Software

9. Línea de Madurez ITIL

Dada la evaluación de riesgos previa, se diagrama una línea de madurez ITIL para el proceso de Tecnologías y Sistemas de Información, en términos de la Gestión de su Continuidad, teniendo en cuenta el estándar ITIL v4.

Tabla 19. Gestión de Continuidad ITIL v4

ID DE PRÁCTICA	NOMBRE DE PRÁCTICA
PR.01	Establecer políticas de Continuidad de TI en la Institución
PR.02	Establecer estrategias de continuidad del Servicio de TI en la Institución
PR.03	Evaluar el Nivel de impacto en el negocio de una interrupción de los Servicios de TI en la Institución
PR.04	Desarrollar Planes de Contingencia en la Institución
PR.05	Formar al personal de TSI, sobre los procedimientos necesarios para la pronta recuperación del Servicio en la Institución
PR.06	Disponer de procedimientos alternativos para trabajar en caso de una interrupción

Para determinar la madurez del proceso, se calificó en un rango de 0 a 5 la madurez del proceso acorde al criterio, la experiencia y la percepción de un juicio de expertos, que en este caso fueron personas responsables de algunas actividades críticas del proceso Tecnologías y Sistemas de Información. Por consiguiente, se calificaron cada una de las seis (6) actividades en dos estados, **Anterior**, medición que se realizó en el año 2020 antes de empezar a realizar actividades de continuidad y **Actual**, medición realizada en el mes de agosto 2021 tiempo presente, como se visualiza en la siguiente tabla:

Tabla 20. Leyenda de Calificación de Madurez de Procesos

LEYENDA DE CALIFICACIONES		
0	Inexistente	No se aplica ningún proceso de gestión
1	Inicial	Los procesos son ad hoc y desorganizados
2	Repetible	Los procesos siguen un patrón regular
3	Definido	Los procesos son documentados y comunicados
4	Administrado	Los procesos son monitoreados y medidos
5	Optimizado	Se siguen y automatizan las mejores prácticas

En la siguiente tabla y gráfico se visualiza que el proceso de Tecnologías y Sistemas de Información antes de realizar este Plan de Continuidad, se encontraba en un estado **Inicial** (1,58), debido a que la Institución Universitaria ITSA no había dado inicio a procesos de implementación del Plan de Continuidad de la Institución; las pocas actividades que se habían desarrollado eran esfuerzos individuales (silos) para cumplimiento de auditorías o

reportes para los entes de control. Se propuso entonces alcanzar un nivel **Administrado** (4), en donde se definieron actividades, roles, políticas, riesgos, los procesos y procedimientos se encuentran en etapa de documentación, además que se comunicaron y se instruyó al personal de TSI sobre los procedimientos necesarios para la pronta recuperación del Servicio de TI en la Institución.

Tabla 21. Evaluación Línea de Madurez Proceso Tecnologías y Sistemas de Información de acuerdo al estándar ITIL

PRÁCTICA	ANTERIOR	ACTUAL
PR.01	2	4
PR.02	1	4
PR.03	2	3,5
PR.04	2,5	5
PR.05	1	4
PR.06	1	3
Promedios	1,58	3,92

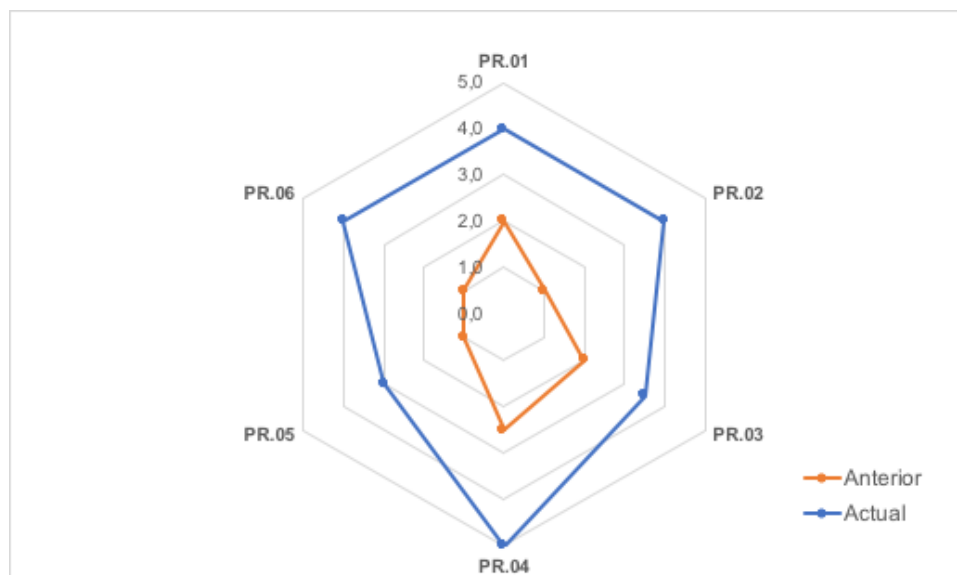


Figura 9. Evaluación Línea de Madurez Proceso Tecnologías y Sistemas de Información

10. Equipos de Emergencia para Activación del Plan de Continuidad

A partir del organigrama de la Institución y el organigrama interno del Proceso de Tecnologías y Sistemas de Información, se definen los equipos de emergencia requeridos para la activación y desarrollo del Plan de Continuidad. Cada equipo tiene unas funciones y procedimientos que tendrán que desarrollar en las distintas fases del Plan.

Dependiendo de cuán grande sea la contingencia, ciertos grupos internos de trabajo deben actuar durante las fases del Plan, los cuales se pueden conformar como se presenta a continuación:

- **Grupo Interno de Respuesta a Incidentes:** Para incidencias, detectadas tempranamente, se recurre a este grupo interno de trabajo el cual dará respuestas en el menor tiempo, sin que sea necesario recurrir a la activación del Plan de Continuidad de Servicios de TI de la Institución. (P.Ej. ataques externos a la red corporativa, daño de un disco de un servidor, etc.).

Tabla 22. Integrantes Grupo Interno Respuesta a Incidentes

LISTADO DE INTEGRANTES	
Coordinador del Grupo	<p>Nombre: Carlos Javier Prasca Aya Cargo: Responsable del Proceso TSI Teléfono: 3112370 Ext. 120 - 3017893307</p>
Miembros del Grupo	<p>Nombre: Diego Fabián Domínguez Tapia Cargo: Líder Administración de Infraestructura Tecnológica Teléfono: 3112370 Ext. 120 - 3107295727</p>
	<p>Nombre: Alvenis Álvarez Pinto Cargo: Líder Administración de Sistemas de Información y Desarrollo de Software Teléfono: 3112370 Ext. 120 - 3015994155</p>
	<p>Nombre: Maciel Paola Rodelo Álvarez Cargo: Líder Soporte Microinformático Teléfono: 3112370 Ext. 120 - 3015413667</p>

- **Grupo Interno de Crisis:** Es el encargado de activar el Plan de Continuidad de Servicios de TI y dirigir las acciones durante la contingencia. Dentro de sus principales tareas y responsabilidades, se encuentra el análisis de la situación, decisión de activar o no el Plan de Continuidad, notificación a las áreas pertinentes, reunir todos los medios necesarios para contribuir a la reactivación de la actividad y el seguimiento del proceso de recuperación, con relación a los tiempos estimados para el mismo.

Tabla 23. Integrantes Grupo Interno de Crisis

LISTADO DE INTEGRANTES	
Coordinador del Grupo	Nombre: Emilio Armando Zapata Cargo: Rector Teléfono: 3112370 Ext. 103
Miembros del Grupo	Nombre: Carlos Javier Prasca Aya Cargo: Responsable del Proceso TSI Teléfono: 3112370 Ext. 120 - 3017893307
	Nombre: Diego Fabián Domínguez Tapia Cargo: Líder Administración de Infraestructura Tecnológica Teléfono: 3112370 Ext. 120 - 3107295727
	Nombre: Alvenis Álvarez Pinto Cargo: Líder Administración de Sistemas de Información y Desarrollo de Software Teléfono: 3112370 Ext. 120 - 3015994155
	Nombre: Maciel Paola Rodelo Álvarez Cargo: Líder Soporte Microinformático Teléfono: 3112370 Ext. 120 - 3015413667
	Nombre: Ismenides Montero Fábregas Cargo: Responsable Planta Física Teléfono: 3112370 Ext. 111

- **Servicios Civiles de Emergencia:** Localizables en caso de catástrofe (como por ejemplo los bomberos) que generalmente constituyen la primera figura de respuesta.

Tabla 24. Servicios Civiles de Emergencia

LISTADO DE SERVICIOS	
Bomberos	119
Policía	112
Emergencias	123
Defensa Civil	144
Cruz Roja	132
CRU - Ambulancias	125

- **Grupo Interno de Recuperación:** Asume la puesta en servicio de la infraestructura tecnológica (sistemas, servidores, aplicaciones, líneas de comunicación y cualquier otro elemento necesario para la restauración de un servicio). Además, son los encargados de diseñar y realizar las pruebas de funcionamiento para verificar la operatividad de los sistemas y comenzar a funcionar.

Tabla 25. Integrantes Grupo Interno de Recuperación

LISTADO DE INTEGRANTES	
Coordinador del Grupo	Nombre: Carlos Javier Prasca Aya Cargo: Responsable del Proceso TSI Teléfono: 3112370 Ext. 120 - 3017893307
Miembros del Grupo	Nombre: Diego Fabián Domínguez Tapia Cargo: Líder Administración de Infraestructura Tecnológica Teléfono: 3112370 Ext. 120 - 3107295727
	Nombre: Alvenis Álvarez Pinto Cargo: Líder Administración de Sistemas de Información y Desarrollo de Software Teléfono: 3112370 Ext. 120 - 3015994155
	Nombre: José Jaider Ramírez Rojas Cargo: Ingeniero de Soporte Infraestructura Tecnológica Teléfono: 3112370 Ext. 120 - 3004815660
	Nombre: Luis Carlos Osbón Pupo Cargo: Ingeniero Desarrollador Teléfono: 3112370 Ext. 120 - 316047639
	Nombre: Michael Javier Arias Restrepo Cargo: Ingeniero Desarrollador Teléfono: 3112370 Ext. 120 - 3015815958

- **Grupo Interno de Comunicaciones:** Es el encargado de canalizar la información que se deba transmitir a la comunidad institucional y/o personal externo a la Institución desde una sola fuente oficial.

Tabla 26. Integrantes Grupo Interno de Comunicaciones

LISTADO DE INTEGRANTES	
Coordinador del Grupo	Nombre: Lorena Barros Moreno Cargo: Responsable de Comunicaciones Estratégicas Teléfono: 3112370 Ext. 107
Miembros del Grupo	Nombre: Carlos Javier Prasca Aya Cargo: Responsable del Proceso TSI Teléfono: 3112370 Ext. 120 - 3017893307
	Nombre: Maciel Paola Rodelo Álvarez Cargo: Líder Soporte Microinformático Teléfono: 3112370 Ext. 120 - 3015413667

11. Procedimientos para ejecución del Plan de Continuidad

Se debe definir procedimientos a seguir determinando el rol para cada participante, tanto para la atención de incidentes como para la ejecución del Plan de Continuidad. Igualmente, éste debe ser divulgado y probado periódicamente, y el personal debe ser entrenado para su aplicación, asegurando su mantenimiento en el tiempo.

Se definirá un procedimiento para el plan de continuidad de los servicios de TI de la Institución, como sigue:

Tabla 27. Procedimiento Plan de Continuidad de los Servicios de TI

Procedimiento Plan de Continuidad Proceso Tecnologías y Sistemas de Información	
ACTIVIDAD	GRUPO INTERNO RESPONSABLE
Activación de Procedencia de la Emergencia	Crisis
Investigación de Causas y Orígenes del Desastre	Incidentes y Crisis
Movilización de Recursos	Crisis, Comunicaciones y Recuperación
Coordinación de las tareas a realizar por los equipos de soporte	Crisis y Recuperación
Coordinación de las tareas a realizar por los proveedores	Crisis y Recuperación

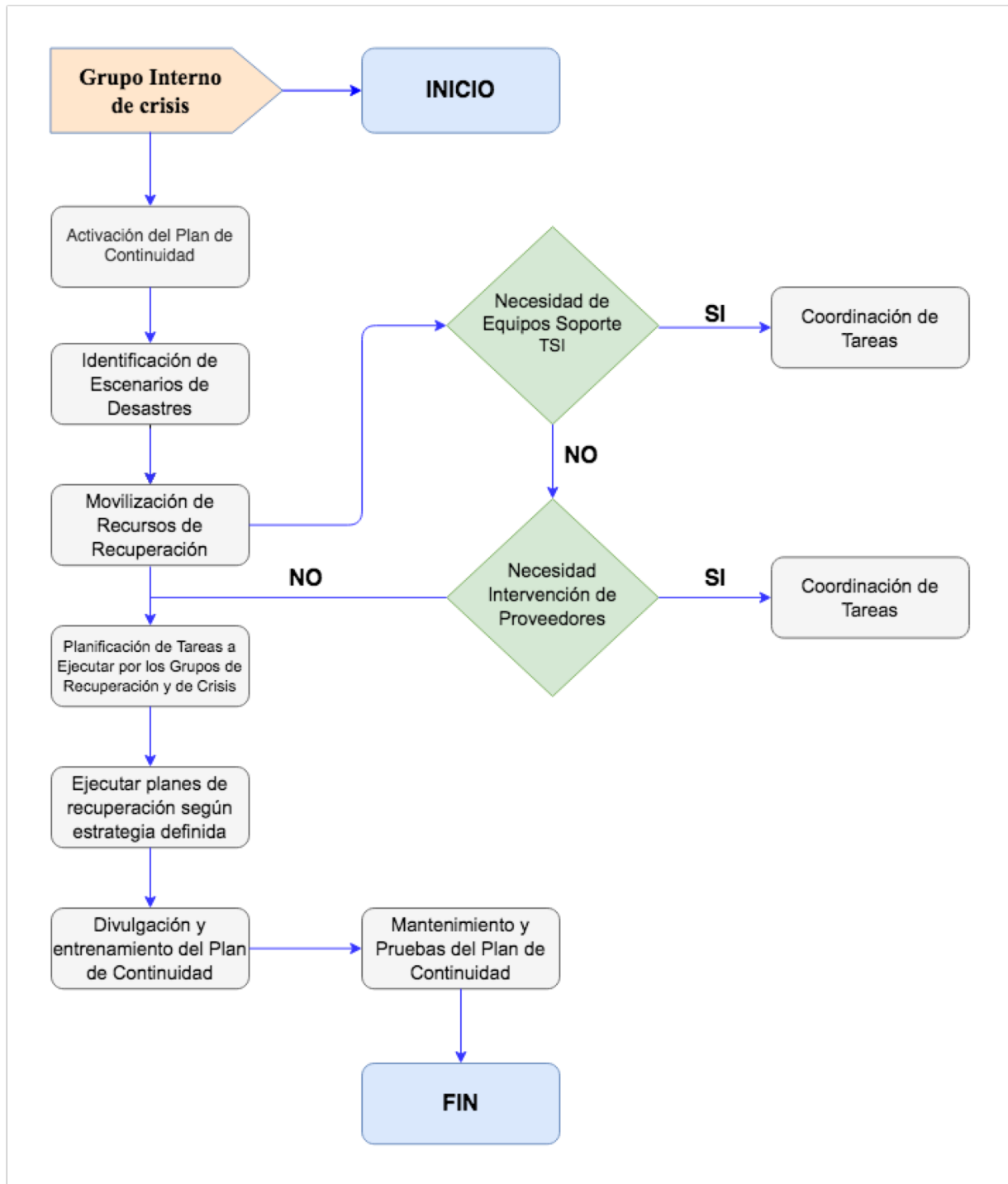


Figura 10. Procedimiento Plan de Continuidad de los Servicios de T