UNIVERSIDAD TECNOLÓGICA DE TULANCINGO
DEPARTAMENTO DE SISTEMAS Y SOPORTE TÉCNICO
PLAN DE RECUPERACIÓN DE DESASTRES
FECHA ÚLTIMA ACTUALIZACIÓN: 22 SEPTIEMBRE 2022

Contenido|

INTRODUCCIÓN

La implementación de un proceso de preservación de la información de la Universidad Tecnológica de Tulancingo ante situaciones disruptivas, permite minimizar el impacto y recuperación por perdida de activos de información de la Institución, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación.

En este proceso es conveniente identificar los procesos críticos para la Universidad e integrar los requisitos de la gestión de la seguridad de la información, de la continuidad de los procesos institucionales con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, materiales, transporte e instalaciones.

Las consecuencias de eventos disruptivos (desastres, fallas de seguridad, perdida del servicio y disponibilidad del servicio) se deben someter a un análisis del impacto del negocio (BIA). Se debe desarrollar e implementar un plan de continuidad que permita garantizar la restauración oportuna de las operaciones esenciales.

La correcta implementación de la gestión de la continuidad de la institución disminuirá el impacto al presentarse incidentes disruptivos y en caso de producirse, la Universidad estará preparada para responder en forma adecuada y oportuna, de esa manera se reduce de manera significativa un daño potencial que pueda ser ocasionado por de ese incidente.

TÉRMINOS Y DEFINICIONES

El ítem de términos y definiciones se elabora para lograr entendimiento de forma clara y unificación de la terminología, definiciones y abreviaturas que tengan lugar en el presente documento.

Actividades prioritarias: Actividades a las que se les debe dar prioridad después de un incidente a fin de mitigar los impactos.

Nota: Los términos que comúnmente se utilizan para describir las actividades dentro de este documento son: critico, esencial, vital, urgente y principal.

Amenaza: Percepción de la posibilidad de ocurrencia de algún hecho dañino sobre los recursos involucrados en el desarrollo de un proceso (humano, financiero, medio ambiente, información e imagen corporativa), representando pérdidas para el sistema o la Universidad.

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Nota 1: El análisis de riesgo proporciona las bases para la evaluación del riesgo y las decisiones sobre el tratamiento del riesgo.

Nota 2: El análisis del riesgo incluye la estimación del riesgo.

Árbol de llamadas: Documento que describe gráficamente las responsabilidades y el orden en que deben producirse las llamadas a los diferentes niveles de la Universidad, así como a los alumnos, administrativos, académicos y otros contactos clave en caso que se produzca una emergencia, catástrofe o situación de indisponibilidad grave.

Centro Alterno de Procesamiento de Datos (CAPD): Lugar en donde se procesa la información de una entidad cuando no es posible hacerlo en el CPD.

Centro de Procesamiento de Datos (CPD): Lugar en donde se concentran los recursos necesarios para el procesamiento de la información de la Universidad.

Crisis: Situación anormal e inestable que amenaza los objetivos estratégicos, la reputación o la viabilidad de la Universidad.

Desastre: Un evento repentino, no planeado y catastrófico que causa daño o pérdida no aceptable a la Universidad.

- Un evento que pone en peligro la capacidad de la Universidad para proporcionar funciones críticas, procesos o servicios por un cierto período de tiempo inaceptable.
- Un evento en el que la gestión de la Universidad invoca sus planes de recuperación.

Directorio activo: Base de datos distribuida que permite almacenar información relativa a los recursos de una red (objetos, dominios, árboles y bosques) con el fin de facilitar su localización y administración, el cual ofrece la ventaja de suponer un único punto de entrada para los usuarios a la red de toda la Institución.

Ejercicio: Proceso para entrenarse, prepararse, practicar y mejorar el desempeño de la Universidad.

Emergencia: Un evento o incidente imprevisto que sucede repentinamente y demanda acción e intervención inmediata para minimizar pérdidas potenciales de vidas, destrucción de propiedades o la pérdida o interrupción de las operaciones de la Institución hasta el punto que pueda representar una amenaza.

Estrategia de continuidad de los procesos de la Institución: Curso de acción definido previamente (y aprobado por el Comité Directivo - Dirección) con el fin de proteger la viabilidad de la Universidad y reanudar sus actividades críticas en los plazos establecidos. Las estrategias seleccionadas deben cubrir los RTOs identificados en el BIA.

Evento: Hecho o suceso imprevisto. Es la ocurrencia o cambio de un conjunto particular de circunstancias.

Nota 1: Un evento puede ser una o más ocurrencias, y puede tener varias causas.

Nota 2: Un evento puede consistir en algo que no está sucediendo.

Nota 3: Un evento puede ser algunas veces referido o conocido como incidente o accidente.

Nota 4: Un evento sin consecuencias puede ser referido como “evento fallido”,
“incidente”, “evento cercano”, “evento de aviso”

Gestión de riesgos: Actividades coordinadas para dirigir y controlar la Universidad con respecto al riesgo.

Infraestructura: Sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de la Universidad.

Impacto: Efecto, aceptable o no, que un evento tiene en la Universidad. Los tipos de impactos a la Institución son normalmente descritos como financieros y no financieros, y posteriormente se dividen en tipos específicos, dependiendo del sector.

Incidente: Suceso que tiene el potencial para generar una interrupción, alteración, pérdida, emergencia, crisis, desastre o catástrofe.

Mitigación: Implementación de medidas para disminuir o eliminar la ocurrencia o impacto de un evento.

Plan de Recuperación ante Desastres (Disaster Recovery Plan – DRP): Documento que contiene un conjunto de acciones y procedimientos definidos previamente, con responsabilidades claramente establecidas, para la recuperación del componente tecnológico, sistemas y servicios de telecomunicaciones.

Procesos críticos: Son aquellos procesos que debido a su importancia deben estar disponibles y operativos constantemente o lo antes posible, después de un incidente, emergencia o desastre.

Proveedor: Persona, natural o jurídica responsable de suministrar bienes y servicios.

Respuesta a incidentes: Conjunto de acciones realizadas por la Universidad ante un desastre u otro evento importante que pueda afectar significativamente a la Institución, a su gente o su capacidad de operación normal. Puede incluir: evacuación, activación de un DRP, evaluación de daños o cualquier otra medida necesaria para llevar a la Universidad a un estatus más estable.

Recovery Time Objective (RTO): Tiempo después de un incidente en el que la operación o el servicio deben ser reanudados.

Recovery Point Objective (RPO): Punto en el cual la información usada por una actividad debe ser restaurada para permitir la reanudación de la operación.

DSST: Departamento de Sistemas y Soporte Técnico

OBJETIVO

Describir las acciones necesarias a ejecutar para la activación del plan de recuperación de desastres DRP en la Universidad Tecnológica de Tulancingo para respaldar las aplicaciones críticas bajo la modalidad de hosting cloud con el fin de asegurar la continuidad de la operación ante un desastre o contingencia e iniciar con el correcto funcionamiento de los servicios identificados como críticos por la Universidad.

ALCANCE

La necesidad de desarrollar un plan de contingencia está relacionada con el impacto potencial que provoca la interrupción parcial o total de los servicios de aplicaciones críticas de la información de la entidad, sobre el normal desarrollo de las actividades; específicamente, para afrontar la contingencia relacionada con el eventual cese de actividades e inoperatividad de equipos. Buscando mantener funcionando a los sistemas de misión críticos y a los servicios esenciales que esta casa de estudios ofrece.

Como parte de la construcción del presente documento se incluye el desarrollo de los ejercicios DRP, fundamental en el procedimiento paso a paso para la activación y recuperación de los servicios contemplados en el presente alcance. El documento preliminar contempla los procesos a seguir durante las pruebas y en caso de un evento adverso en que se requiera la activación del plan.

Servidores que hacen parte integral del DRP:

FUNCIÓN O SERVICIO ASOCIADO	RPO	RTO
SIGEES	2 Horas	2 Horas
SIES	2 Horas	2 Horas
GESTIÓN DE CALIDAD	2 Horas	2 Horas
SIENIN	2 Horas	2 Horas
BUZÓN DE QUEJAS Y SUGERENCIAS	2 Horas	2 Horas
SAIIUT	2 Horas	2 Horas
BD SAIIUT	2 Horas	2 Horas
INDETEC	2 Horas	2 Horas
BIOTIME	2 Horas	2 Horas
PFSENSE	2 Horas	2 Horas
IPCOP	2 Horas	2 Horas

Tabla 1 - Alcance DRP - UTEC

El cumplimiento del RPO y RTO se verificará en las pruebas formalmente realizadas y en las ocasiones en que se requiera activar los servicios en el Centro de Datos Alterno.

GENERALIDADES DEL PLAN DE RECUPERACION DESASTRES - DRP

De acuerdo con la descripción del alcance el Departamento de Sistemas y Soporte Técnico definió los tiempos de RTO y RPO para cada uno de los servicios, luego de realizar un análisis de criticidad de las mismas, mediante:

RPO (RECOVERY POINT OBJECTIVE): Se define como el periodo máximo tolerable en el cual la información de un servicio de IT no estaría disponible con motivo de la ocurrencia de un desastre, puede ser especificado en segundos, minutos, horas o días

RTO (RECOVERY TIME OBJECTIVE): Corresponde al tiempo que se toma y el nivel de servicio mediante el cual un proceso de negocio puede ser restablecido después de la ocurrencia de un desastre o una interrupción del servicio, esto en orden de evadir las consecuencias asociadas a la interrupción de un proceso de negocio que debe estar disponible permanentemente, es especial, los procesos de carácter sempiterno.

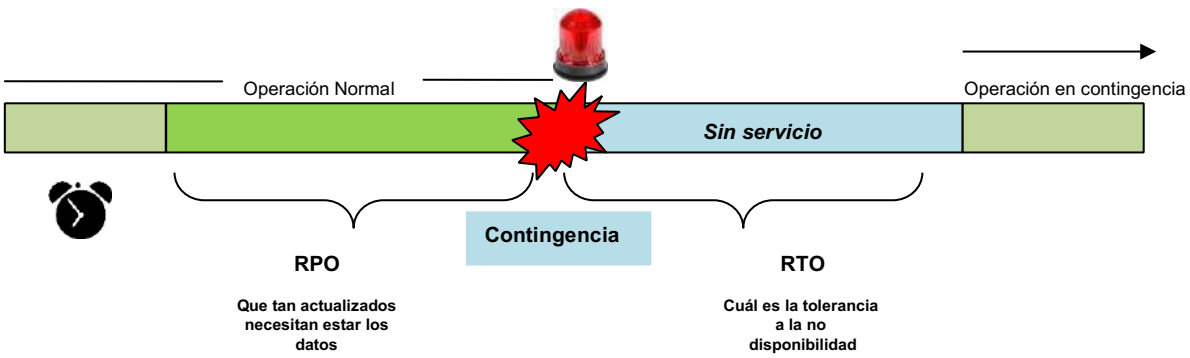

Figura 1 - RTO - RPO

Estrategia general de recuperación

Este plan está basado en el hecho de que por alguna situación crítica interna o externa, no haya acceso a los servicios de cómputo centrales o las instalaciones donde se ubica el centro de cómputo o son inaccesibles por completo por un período inaceptable de tiempo.

Las estrategias para seguir serán acordes a la magnitud y duración tentativa del incidente y se deberán tomar en cuenta los siguientes aspectos:

- Evaluación de los daños
- Evaluación del tiempo estimado de la recuperación
- Análisis exhaustivo para determinar las acciones específicas que deberán seguirse de acuerdo con el tipo de incidente.

Este plan solo podrá ser activado únicamente cuando el DSST lo apruebe. Con base en los resultados obtenidos por el departamento en donde se determinó contar con un Centro de Datos Alterno, se estableció la estrategia de recuperación, la cual se conforma de elementos tales como la ubicación del centro de datos alterno, la preparación y puesta en funcionamiento de un respaldo.

Estrategia de acción

Las estrategias y planes de acción considerados para la recuperación del DSST, han sido orientados a cubrir cualquier contingencia mayor o catastrófica que inhabilite el acceso del personal al edificio donde se ubica el centro de cómputo o bien a los servicios de cómputo y telecomunicaciones en que se apoyan todos los sistemas y servidores de la entidad, las cuales se definieron como:

1. SIGEES
2. SIES
3. GESTIÓN DE CALIDAD
4. SIENIN
5. BUZÓN DE QUEJAS Y SUGERENCIAS
6. SAIIUT
7. BD SAIIUT
8. INDETEC
9. BIOTIME
10. PFSENSE
11. IPCOP

La decisión para desarrollar este plan, se basó en las características de la operación actual de la Universidad, así como el nivel de dependencia de tecnología de información y comunicaciones.

Incidencia Menor:

En caso de presentarse una incidencia menor, esta podrá ser subsanada o corregida rápidamente por medio de los mecanismos de detección, diagnóstico y reparación de fallas, activando los procedimientos de atención de problemas utilizados día a día por el personal del DSST.

Incidencia Mayor:

De presentarse una incidencia mayor en los equipos y sistemas del centro de cómputo principal que impida la función general de la UTT, esta deberá ser identificada y corregida a la brevedad. Si el tiempo estimado de reparación que determinen los equipos de recuperación responsables de las aplicaciones o recursos técnicos críticos, es superior al tiempo identificado para que este operativo, el DSST tomará la decisión de activar o no el Plan DRP.

Incidencia Catastrófica:

Si se presenta un incidente que provoque una contingencia catastrófica evidente y que por consiguiente interrumpa las operaciones del DSST en sus instalaciones ubicadas en Av. Ahuehuetitla 301, Reforma la Presa, 43642 Tulancingo de Bravo, Hgo. Siendo importante recalcar que la declaración de contingencia es responsabilidad del comité de protección civil de la Universidad.

Clasificación de los escenarios de desastre

En esta sección se incluye una clasificación de los posibles escenarios de desastre que pueden ocurrir.

Figura 3 - Clasificación escenarios de desastre

Pérdida total o parcial de las instalaciones del centro de datos principal

La pérdida total o parcial de las instalaciones del Centro de Datos principal de la Universidad Tecnológica de Tulancingo, puede deberse a diferentes situaciones y/o motivos tales como:

- Guerras internacionales o civiles.
- Actos perpetuados por terroristas y/o grupos armados ilegales.
- Hostilidades u operaciones bélicas ya sea o no declarada una guerra.
- Rebelión, sedición, usurpación o retención ilegal del mando.
- Asonada, motín, o conmoción popular.
- Huelgas, conflictos colectivos de trabajo o suspensión de hecho de labores y por movimientos subversivos y/o acciones terroristas y/o de grupos armados ilegales que conlleven a daños materiales en las instalaciones.
- Deslizamientos de tierra y/o otros elementos, avalanchas, fallas geológicas, terremoto, temblor, asentamientos, inconsistencias del suelo, inundaciones, erupción volcánica, vientos o cualquier otra convulsión de la naturaleza.
- Reacción o radiaciones nucleares o contaminación radioactiva.

Pérdida total o parcial de los servicios pactados dentro del alcance del plan

La pérdida total o parcial de los servicios pactados dentro del alcance del plan puede originarse por las siguientes causas y/o motivos:

- Daños causados directamente por personas encargadas de la infraestructura de IT, en el curso de la ejecución de las operaciones llevadas a cabo con el propósito de dar cumplimiento a sus obligaciones.
- Por la pérdida de aquellos bienes cuyo valor excede el de los materiales que los componen tales como planos, modelos, metodologías, documentos de cualquier clase, archivos magnéticos y/o cualquier otro medio de archivo computacional, que traiga como consecuencia que no se pueda efectuar la operación normal de los servicios del negocio.
- Por la reticencia u omisión de los procedimientos establecidos para la prestación de los servicios del negocio.
- Por delitos por computador y/o medios electrónicos que puedan afectar la prestación de los servicios del negocio.
- Por utilización de técnicas como el acceso a los activos de información por medio de una identidad falsa, la alteración de datos en forma no autorizada, la negación de la ocurrencia de un acción o transacción, la visualización de información no autorizada, la negación del servicio y/o operación de la(s) aplicación(es) y la obtención del acceso a la plataforma y/o a los aplicativos con todos los privilegios y/o roles que conlleven a la pérdida total o parcial de los servicios del negocio.
- Por las vulnerabilidades en sistemas operativos y/o en las aplicaciones que estén alojadas en el centro de datos.
- Por la disminución en el rendimiento laboral de las personas a cargo de los procesos de negocio.
- Por exposición de accesos lógicos tales como puertas traseras, ataques asíncronos, fuga de datos, cierre de computadoras (shutdown), ataques de negación de servicio, redondeo hacia abajo, técnicas de salami, caballos de Troya, virus, gusanos y bombas lógicas que generen la pérdida total o parcial de los servicios de negocio.
- Por exposición de acceso físico tales como entradas no autorizadas, daño, vandalismo o robo de equipos o documentos, copia o visualización de información privada, alteración de equipos e

información sensible, revelación al público de información privada, abuso de los recursos de procesamiento de datos que conlleven a la pérdida total o parcial de los servicios de negocio.

- Por problemas y exposiciones ambientales tales como falla eléctrica, voltaje severamente reducido, depresiones, picos y sobre voltajes, interferencia magnética, caída de backbones que alteren y/o interrumpan el normal funcionamiento de los equipos que se utilicen para los procesos de la UTT.
- Por problemas y exposiciones en bases de datos tales como procesamiento interno erróneo, actividad errónea de administración de base de datos, corrupción de la base de datos, acceso indebido a la base de datos para modificarla, errores en puesta en producción / regresión con impacto en base de datos y errores en generación y restauración de respaldos que conlleven a la pérdida total o parcial de los servicios de negocio.
- Por problemas y exposiciones en aplicación y componentes del sistema tales como código malicioso en el software, fuga de información de claves de usuarios, ataques externos para obtención indebida de claves, suplantación de usuarios externos al pedir cambio de clave, ataques externos para obtención/modificación indebida de información, y la inestabilidad del rendimiento del hardware y/o software que conlleve a la pérdida total o parcial de los servicios del negocio.
- Por acciones tomadas por personas que terminen en el sabotaje de los procesos de la UTT a causa de chantaje, fraude, descontentos, huelgas, amenazas (acción disciplinaria o con despido), adictos y/o experimentación de problemas financieros o emocionales.
- Dolo y/o imprudencia manifiesta por parte de personas directa y/o indirectamente involucrada en los procesos de la UTT que conlleven a la suspensión total o parcial de los servicios.
- Pérdida del hardware, software y data de propiedad y/o tenida a cargo, en custodia y/o control del DSST.
- Pérdida o daño debido al cálculo o diseño erróneo del hardware y software.
- Falla y/o daño eléctrico interno o desarreglo de los equipos y dispositivos del centro de datos.
- Daños y/o fallas atribuibles a la falta y/o carencia de diligencia en los mantenimientos predictivos, preventivos y correctivos a los equipos y dispositivos del centro de datos.
- Daño total o parcial del hardware debido a los deterioros causados por el calor, el humo, el vapor, y/o los medios empleados para extinguir y/o contener un incendio ya sea por acción directa e inmediata del mismo, y las demoliciones que sean necesarias a consecuencia del incendio y que sean ordenadas en tal carácter por la autoridad competente.
- Por la combustión espontánea de algún elemento que forme parte de algún equipo y/o dispositivo del centro de datos.

Interrupciones a la UTT o incidentes que podrían afectar el cumplimiento de las labores de la comunidad universitaria.

Las interrupciones a la UTT o incidentes que podrían afectar el cumplimiento de las labores de los docentes y administrativos puede deberse a diferentes situaciones y/o motivos tales como:

- Pérdidas de personal (Cesación, muerte, accidentes laborales, enfermedades)
- Cortes de servicio de transporte
- Fallas en los proveedores

Centro de datos alterno

El sitio alterno para la Universidad Tecnológica de Tulancingo está ubicado dentro de las instalaciones de la Universidad, en el edificio H.

Este Data Center está ubicado a una distancia lineal de 90 m respecto al Centro de Datos Principal de la Universidad.

Figura 4 – Distancia lineal del centro de datos alterno

La infraestructura del centro de datos provista para el alojamiento de los componentes de Hardware que hacen parte de la solución la Universidad Tecnológica de Tulancingo, es la siguiente:

- Suministrar toda la infraestructura tecnológica de servidores.
- Suministrar mínimo 2 TB de almacenamiento.
- Monitoreo y administración en contingencia.
- Replicación en línea y dos canales de datos de 20 Mbps para redundancia
- Solo se contempla la implementación de los servidores replicando, mas no pruebas reales para la fase de implementación.

Conectividad

Los diferentes componentes físicos instalados en los racks, se encuentran conectados a través de los switches FC que hacen parte de la solución, permitiendo la gestión y comunicación adecuada. Toda la conectividad de la administración se centralizará en el Switch Management, generando separación física de tráfico y garantizando optimizar el tráfico productivo.

Centro de operaciones alterno - COA

La Universidad Tecnológica de Tulancingo tiene de manera exclusiva un puesto de trabajo en el sitio alterno para ser utilizados por personal de la entidad. Estos deben disponer de área física de trabajo, equipo de cómputo con capacidad para atender las necesidades mínimas de oficina y aplicaciones, conexión segura al sitio alterno.

A continuación, se enuncian las principales características y servicios que presta el Centro de Operaciones Alterno (COA):

- Conexión con el Centro de Datos Alterno (CDA).
- Los equipos cuentan con salida a internet y conexión al Centro de Datos Alterno y al Centro de Datos Principal en la Institución

Centro de monitoreo

El Centro de Monitoreo se encuentra ubicado en las instalaciones de la Universidad tecnológica de Tulancingo, en la planta baja del edificio C.

A continuación, se enuncian las principales características y servicios que presta el Centro de Monitoreo:

- Verificación de la operatividad de los equipos.
- Notificación en caso de alarmas o de alteraciones en los sistemas.

A continuación, se muestran las fotografías del Centro de Monitoreo:

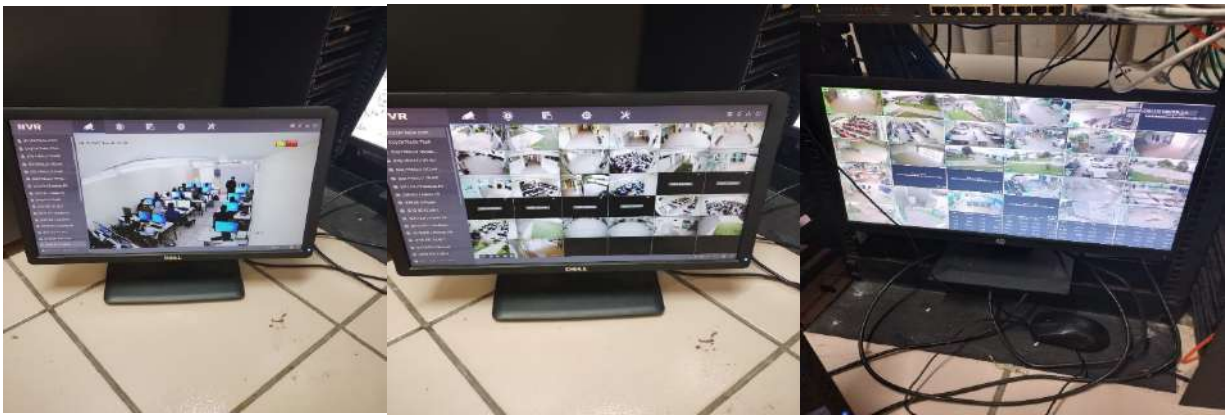

Figura 6 - Centro de monitoreo ROC – CDA

PROCEDIMIENTO DE NOTIFICACIÓN, ACTIVACIÓN Y RETORNO

Como parte de las estrategias inmediatas ante una posible crisis, se contemplan las tareas que deben efectuarse lo más rápido posible, después de que se presente el incidente, para reducir posibles impactos. En muchos casos, estos procedimientos contemplan la comunicación inicial con clientes y otros contactos externos, así como también direccionamiento de las estrategias de recuperación de las funciones de negocio más críticas.

A continuación, se listan las actividades a ejecutar cuando se active la contingencia, de acuerdo con la presentación de cualquier tipo de evento adverso:

Tipo de evento	Características	Ejemplos	Respuesta
DESASTRE	Evento que inhabilita el Centro de Datos Principal para prestar sus servicios. No permite seguir laborando en las instalaciones principales del Instituto.	Terremotos, incendio general, fallo eléctrico en el sector.	DRP
INTERRUPCIÓN	Evento que requiere ser evaluado para ser tratado como desastre o como contingencia. Puede llegar a ser considerado como un desastre o una contingencia, dependiendo del impacto que se determine en el manejo de incidentes.	Incendio localizado, atentado terrorista, huelga interno o externo.	DRP Planes de contingencia
CONTINGENCIA	Evento que afecta puntualmente un recurso necesario para la prestación de los servicios de Informática. No impide el acceso al CDP. En ausencia de plan de contingencia, requiere evaluación que puede llevarla a categoría de desastre.	Fallo de sistemas o servicio, ausencia de personal clave.	Planes de contingencia

Tabla 2 - Clasificación de eventos

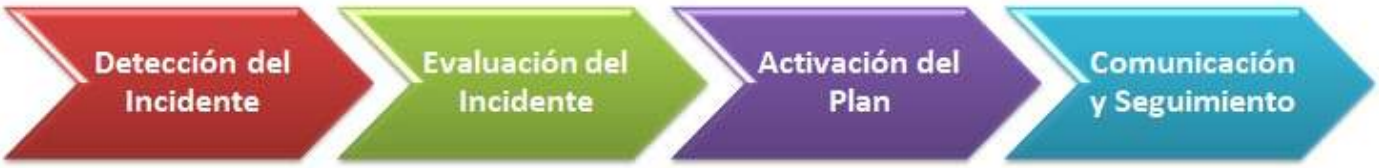

Figura 7 - Fases de activación

Así mismo se listan algunas actividades anexas a las fases definidas anteriormente:

1. Registro de Incidentes
2. Evaluación inicial del alcance del incidente y fallos
3. Validar la criticidad de la falla (Contingencia menor, mayor o catastrófica)
4. Comunicar al comité
5. Activar Alertas
6. Activar Desastre
7. Activación del plan de recuperación de desastres
8. Ejecución Procedimientos de contingencia
9. Notificación Contingencia
10. Monitoreo y Seguimiento periodo de contingencia
11. Comunicación continúa interna/externa a involucrados
12. Activación de plan de retorno de contingencia
13. Declaración de fin de contingencia
14. Regreso a modo normal de operación
15. Notificación formal de fin de contingencia
16. Actualización del plan de recuperación de desastres
17. Documentación de lecciones aprendidas
18. Actualización Planes de Prueba
19. Fin de Contingencia

Procedimiento de notificación

Cuando se presenta una emergencia, hay que tener en cuenta que se debe gestionar la notificación de la misma con el ánimo de iniciar con el proceso de activación del Plan de Recuperación de Desastres (DRP). Esta notificación corresponde a una gestión para la activación del plan la cual se describe a continuación:

Figura 8 - Procedimiento de notificación

La notificación de la indisponibilidad de los sistemas de información o servicios de TI puede llegar por diferentes fuentes, esto va a depender de la naturaleza del evento, del momento en el cual éste suceda y de la fuente que lo causa. Es importante tener en cuenta que el procedimiento de notificación debe estar ligado a los procedimientos de Emergencia definidos y establecidos por el DSST.

Así mismo se describe el proceso mediante el cual se activa la gestión del plan, previa notificación del desastre, y hasta el momento en que el servicio es restaurado en el Sitio Principal en producción:

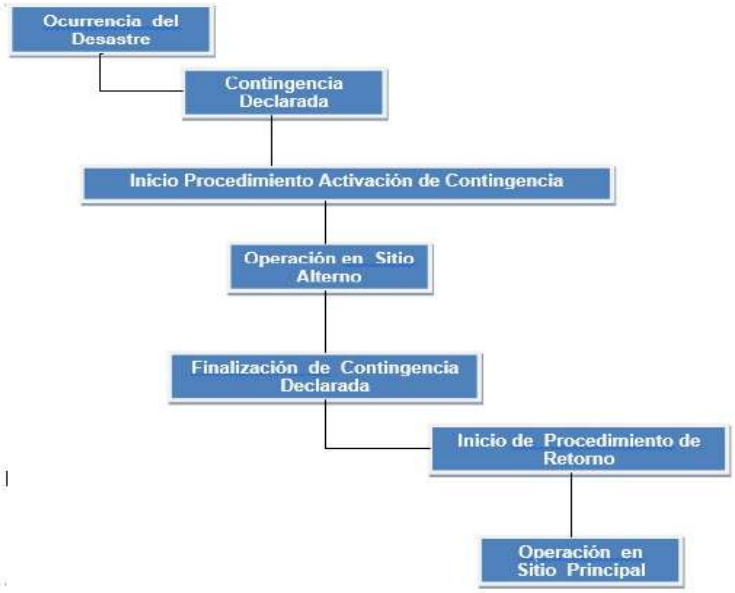

Figura 9 - Proceso de activación gestión del plan

El procedimiento de entrada a contingencia describe las actividades requeridas para la activación de los diferentes servicios que se encuentran respaldados en el centro de datos, cuando se activa el plan.

Detección del evento

Los eventos que afectan la continuidad de las operaciones de los servicios identificados como críticas por el DSST, podrán ser reportados una vez identificados con el fin de iniciar a trabajar en una pronta atención y por ende el cumplimiento de los tiempos de atención definidos.

Esta detección de eventos se realizará una vez se presenten interrupciones de los servicios:

1. SIGEES
2. SIES
3. GESTIÓN DE CALIDAD
4. SIENIN
5. BUZÓN DE QUEJAS Y SUGERENCIAS
6. SAIIUT
7. BD SAIIUT
8. INDETEC
9. BIOTIME
10. PFSENSE
11. IPCOP
12. Servicio de correo electrónico

Los anteriores servicios descritos, fueron definidos por la entidad como críticos, y en ellos se relacionan la totalidad de los servicios que se encuentran en el alcance para su correcto funcionamiento.

Definición de recursos

Como parte del Plan de Recuperación de Desastres (DRP), se realizó la definición de los siguientes recursos, cuyos miembros de los equipos de trabajo atenderán las solicitudes realizadas por la institución, teniendo en cuenta las responsabilidades específicas que les han sido asignadas.

- **Comité de Emergencias:** Hace parte de la contingencia en la presentación de un evento adverso, este equipo de emergencias debe ser definido internamente en la entidad y en él se debe mantener informado al responsable de la activación de la contingencia.
- **Comité responsable de activación DRP:** se encuentra conformado por los responsables de la activación del plan de recuperación de desastres DRP.
- **Equipo de Recuperación DRP:** Incluye todo el personal técnico de la oficina de informática de la entidad, encargados de realizar la activación de los servicios definidos como críticos y la puesta en funcionamiento de las maquinas contempladas dentro del alcance.
- **Responsables del proceso del Departamento de Sistemas y Soporte Técnico**

Comité de Protección de Civil

Realiza la evaluación de los daños y la magnitud del suceso, trabaja de la mano con el equipo de DRP, y su principal función es salvaguardar las vidas humanas, este comité es informado lo antes posible de cualquier incidencia para la toma de decisiones efectivas para la superación de eventos y dar alcance a la comunicación oportuna al jefe de DRP para iniciar a la activación de los servicios definidos en el alcance. La intervención de este grupo durante una situación de contingencia está determinada por el tipo de daño, siendo necesaria su gestión en la ocurrencia de algún evento.

Hace parte del comité de emergencias el equipo evaluador de daños quienes validan los daños a la infraestructura de IT con el fin de determinar la afectación y poder informar con el Comité de Emergencias al comité de activación DRP si se debe declarar una contingencia. La intervención de este grupo durante una situación de contingencia está determinada por el tipo de daño, siendo necesaria su gestión en la ocurrencia de algún evento.

Participante	Equipo Evaluador de Daños
Funciones Principales **Evaluar** **Comunicación** **Aprueba**	▯Evaluar los daños físicos que se presenten en la infraestructura de IT, cuando haya ocurrencia de un desastre. ▯Presentar al comité de Emergencias el status de afectación de la infraestructura. ▯Participar en la toma de decisión para declarar un desastre y activación del DRP. ▯Realizar un análisis de las instalaciones físicas con el fin de determinar si los funcionarios responsables de las aplicaciones críticas se deben desplazar al COA.

Tabla 3 – Equipo evaluador de daños

Comité de responsable de activación del DRP

Está conformado por el Jefe del departamento de Sistemas y Soporte Técnico. Esto no es una limitante en caso que se decida invitar a participar dentro de este equipo a algunos funcionarios del nivel directivo de la Institución. No se debe perder de vista el carácter técnico del DRP y por tanto el nivel de especialización del equipo.

Se debe asegurar la comunicación permanente con el área directiva de la universidad en cada momento (antes, durante y después) por la naturaleza de las decisiones que se deban tomar.

Algunas de las responsabilidades de este equipo son:

- Establecer las directrices y políticas del DRP enmarcadas en un Plan de Continuidad
- Mantener contacto con las áreas de dirección.
- Toma de decisiones estratégicas durante la crisis o incidente.
- Declarar la activación del DRP.
- Comunicación efectiva con los medios de comunicación, en caso de no existir un equipo a nivel institucional.
- Supervisión de la efectividad de las actividades de recuperación.

Equipo de recuperación DRP

Recibe la confirmación de activación del Plan de Recuperación de Desastres DRP del comité responsable de activación del DRP y se encarga de restablecer la operación de los servicios de hardware, software, telecomunicaciones, energía y seguridad física que dificulten la continuidad de la operación en el sitio principal.

Equipo de Base de Datos.

Es el responsable de planear y ejecutar las actividades que permitan la activación de los servicios específicos sobre los cuales funcionan las bases de datos de las aplicaciones identificadas como muy críticas y los servicios que las apoyan. Igualmente es responsable de todas las actividades que garanticen la adecuada disponibilidad del servicio de respaldo en cuanto la actualización de datos y documentación, y las que conduzcan al restablecimiento de los servicios desde el Centro de Cómputo Principal.

Algunas de las responsabilidades de este equipo son:

- Mantener actualizados los procedimientos de instalación y arranque de los servidores de base de datos y los planes recuperación.
- Conocer y divulgar a los miembros de los equipos los procedimientos de notificación de contingencia.
- Verificar la realización de las copias de seguridad.
- Verificar el estado de la actualización, se debe procurar que los datos del centro de datos principal y el del centro de datos alterno, esté al mismo nivel de actualización.
- Tener disponibilidad de los medios de instalación de los gestores de Bases de Datos.

- Apoyar las labores que garanticen la disponibilidad del esquema de respaldo de datos.
- Definir y ejecutar pruebas del DRP en lo referente a esta plataforma periódicamente o cuando se tenga contemplado con el proveedor.
- Determinar el impacto en caso de falla y emitir concepto para toma de decisiones.
- Activar servicios de la plataforma en el Centro Computo Alterno.
- Asistir la recuperación de la plataforma en el Centro Computo Principal.
- Documentar fallas y su solución.
- Proveer soporte técnico según requerimientos del momento.
- Restaurar el servicio en el Centro Computo Principal.
- Alistar el Centro Computo Alterno para usarlo nuevamente después de un retorno a la normalidad.

Equipo de Conectividad.

Es el responsable de planear y coordinar las actividades que permitan la activación de los servicios específicos de conectividad sobre los cuales se apoya la entrega de los servicios de TIC en un Centro de Cómputo Alterno. Igualmente es responsable de todas las actividades que garanticen la adecuada disponibilidad del servicio de respaldo en cuanto la actualización de los sistemas, aplicativos y datos, y las que conduzcan al restablecimiento de los servicios desde el Centro de Cómputo Principal (CCP) o desde el COA Centro de Operación Alterna (CCA).
Algunas de las responsabilidades de este equipo son:

- Mantener actualizados los procedimientos de instalación y arranque de los Equipos de conectividad.
- Conocer y divulgar a los miembros de los equipos los procedimientos de notificación de contingencia. Definir y ejecutar pruebas del DRP cuando se tenga establecido con el proveedor.
- Determinar el impacto en caso de falla y emitir concepto para toma de decisiones.
- Activar servicios de la plataforma en el CCA.
- Asistir la recuperación de la plataforma en el CCP.
- Documentar fallas y su solución.
- Proveer soporte técnico según requerimientos del momento.
- Restaurar el servicio en el CCP.
- Alistar el CCA para usarlo nuevamente después de un retorno a la normalidad.

Equipo de Administradores de la Aplicación.

Es el responsable de planear y ejecutar las actividades que permitan la activación de las aplicaciones en los respectivos servidores de tal forma que se restablezcan los servicios de TI en un Centro de Cómputo Alterno.

- Mantener actualizados los procedimientos de instalación y arranque de las aplicaciones.
- Mantener actualizado los requerimientos para la operación de las aplicaciones.
- Conocer y divulgar a los miembros de los equipos los procedimientos de notificación de contingencia.
- Velar porque las configuraciones de los equipos del CCP y del CCA, en HW y SW sean apropiadas para el correcto funcionamiento de las aplicaciones.
- Velar porque las versiones de las aplicaciones disponibles en el CCP y el CCA sean las mismas.
- Definir y ejecutar pruebas del DRP en lo referente a las aplicaciones.
- Definir y apoyar la ejecución de las pruebas del DRP.
- Velar porque se realicen los respaldos a la aplicación de acuerdo con las necesidades.
- Mantener los medios de instalación disponibles.
  Mantener los contratos de soporte de acuerdo a lo requerido por el Instituto.
- Atender los requerimientos de auditoria
- Determinar el impacto en caso de falla y emitir concepto para toma de decisiones.
- Activar servicios de la plataforma en el CCA.
- Proveer soporte técnico según requerimientos del momento.
- Documentar fallas y su solución.

- Asistir la recuperación de las aplicaciones en el CCP.
- Restaurar el servicio en el CCP.
- Alistar el CCA para usarlo nuevamente después de un retorno a la normalidad.

Equipo de Usuarios.

Corresponde a las personas que han sido identificadas como responsables funcionales de los aplicativos que utilizan los servicios prestados por la oficina de informática para ejecutar las funciones propias de su proceso y otras complementarias al trabajo diario.

Algunas de las responsabilidades de los usuarios son:

- Información y notificación de eventos identificados a nivel de sus procesos que puedan afectar las operaciones.
- Participar en las actividades de continuidad (Capacitaciones, divulgación, pruebas y auditorias)
- Actualizar la información de continuidad de las operaciones internas de su proceso y divulgarlos al interior del mismo. En este proceso se deberá seguir los lineamientos de control documental y de versiones del Instituto.
- Participar en los ajustes a las actividades de entrevista de valoración de impacto de negocio y evaluación de riesgos a nivel de proceso.
  Apoyar al interior de su proceso los aspectos de continuidad, indicando acciones de mejora, cambios al interior del proceso y otros factores que deban ser revisados a nivel de comité para su aprobación

El equipo de Soporte a Usuarios debe brindar el soporte a los usuarios finales de la entidad para el desarrollo de sus actividades tareas durante el tiempo que esté operativa la contingencia.

El equipo está conformado por:

- Jefe de departamento
- Coordinador
- Ingeniero en Sistemas 1
- Ingeniero en Sistemas 2

Responsabilidades:

- Conocer y entender el Plan de Contingencia.
- Verificar con los usuarios finales la estabilidad de las aplicaciones y reportar anomalías.
- Cooperar con el Equipo de Recuperación de Contingencias en la puesta en marcha del Plan de Contingencia.
- Verificar con los usuarios finales la estabilidad de las aplicaciones y reportar anomalías.
- Actualizar los procedimientos existentes en el Manual de Contingencias que esté relacionado con su trabajo.

Responsables del departamento de Sistemas y Soporte Técnico para la activación de DRP

Una vez declarada la activación del DRP se procede a dirigirse al personal del departamento de Sistemas y Soporte Técnico para habilitar los servicios y las comunicaciones según corresponda:

JEFE DE DEPARTAMENTO DE SISTEMAS Y SOPORTE TÉCNICO

COORDINADOR DE DEPARTAMENTO DE SISTEMAS Y SOPORTE TÉCNICO

INGENIERO EN SISTEMAS

INGENIERO EN SISTEMAS

NOTA: Es importante destacar que el personal relacionado anteriormente es el que se encuentra actualmente disponible en el Departamento de Sistemas y Soporte Técnico.

Árbol de llamadas

El árbol de llamadas representa la cadena de llamadas que se debe seguir y cumplir para comunicar a los integrantes del DRP la activación del plan, esta se ejecuta después de la declaración de contingencia realizada por el comité de protección civil de la UTEC.

Cada nivel está encargado de llamar al nivel inferior según la estructura del plan y el llamado a cada integrante debe ser verificado por el nivel superior. Jefe de Departamento de Sistemas y Soporte Técnico y su líder DRP son los encargados de efectuar las llamadas y son los responsables de la intercomunicación con el primer nivel de llamadas.

El llamado a los integrantes del plan se debe realizar siguiendo el procedimiento de comunicación necesario y utilizando los medios de comunicación disponibles para realizarlo.

A continuación, se relacionan algunos medios de comunicación a ser utilizados al momento de un evento adverso, así como su prioridad en usabilidad:

MEDIOS DE COMUNICACIÓN		
Prioridad	**Tipos de Medio**	**Descripción**
1	Persona a Persona	La forma más fácil y efectiva de comunicar el evento es hacerlo persona a persona. Esté medio permite ser más explícito y detallar lo sucedido con el evento. La comunicación depende de factores socio-ambientales y/o factores de riesgo (catástrofes) que afecten este tipo de comunicación.
2	Telefonía Celular	La comunicación telefónica es un medio facilitador para acortar distancias y tener una conversación interpersonal. Con él se puede al igual que en la comunicación persona a persona ser más explícito y ahondar dentro de la comunicación del evento.
3	Telefonía Fija	
4	Skype - Viber (requiere Smartphone e internet)	
5	Mensajería Instantánea – Link (requiere Computador Personal e internet Whats Up (requiere Smartphone e internet)	La mensajería instantánea como un tipo de correo permite interactuar más rápida y efectivamente entre una o varias personas. Depende de los medios y restricciones impuestos por la corporación y de la disposición de los intercomunicadores.
6	Correo Electrónico	El correo electrónico se ha establecido como un medio efectivo para comunicarse a cualquier distancia y en el menor tiempo. Este tipo de comunicación depende del grado de consulta de los intercomunicadores.

Mtro. Francisco Ramos Lozano	**Mtro. Carlos A. Torres Estrada**
Jefe de Departamento de Desarrollo de Sistemas y soporte Técnico	Director de Planeación y Evaluación
Elaboro	Autorizó