ITLA INSTITUTO TECNOLÓGICO DE LAS AMÉRICAS Las Americas Institute of Technology	**INSTITUTO TECNOLÓGICO DE LAS AMÉRICAS** **Departamento de Tecnología de la Información**		
	PLAN DE SEGURIDAD DE LA INFORMACIÓN Y ACTIVOS TECNOLÓGICOS		
Código documental: DC-TI-03	**Versión:** 1	**Fecha de actualización:** 17-octubre-2023	**Tipo de proceso:** De soporte o apoyo
Preparado por: Director/a de TIC	**Revisado por:** Encargado/a de Calidad en la Gestión		**Aprobado por:** Rector/a

Plan de Seguridad de la Información y Activos Tecnológicos.

Tabla de Contenidos

Tabla de contenido

Plan de Contingencia

1. Introducción

Este manual es una guía, según los estándares de planes de seguridad física y tecnológica, para que cada Gerente de Departamento de tecnología defina y documente un Informe de Trabajo derivados del Plan de Contingencia de TIC.

El alcance de este plan guarda relación con la infraestructura informática, así como los procedimientos relevantes de cada Departamento asociado con la plataforma tecnológica.

Se entiende como infraestructura informática al hardware, software y elementos complementarios que soportan la información o datos críticos para la función de la institución bajo la responsabilidad del lector. También, se entiende como procedimientos relevantes a la infraestructura informática a todas aquellas tareas que el personal realiza frecuentemente cuando interactúa con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).

Cada uno de los gerentes del Departamento de tecnología deberá leer acabadamente este instructivo, así como generar un "Plan de Trabajo para el Plan de Contingencia de TIC" que involucre a los actores relevantes. Este plan de trabajo considera evaluar las situaciones de riesgo y definir las tareas orientadas a reducir dichos riesgos.

Sugerimos que su respectivo plan de trabajo se genere como *una respuesta* a cada uno de los puntos que contiene esta Guía de Plan de Contingencia del ITLA.

Agradecemos la diligencia que invertirá en este aspecto tan importante del manejo de contingencias informáticas, el que sabemos valorará en la eventualidad de una contingencia mayor.

1.1. Justificación

El ITLA se enfrenta a muchos peligros potenciales que podrían tener un efecto negativo en su capacidad para funcionar y / o podrían colocar a sus estudiantes, personal y visitantes en peligro. Algunos de estos riesgos se pueden anticipar, otros no; sin embargo, el ITLA debe ser capaz de abordar de forma pro-activa cualquier situación de emergencia, independientemente de su naturaleza u origen, y de esta manera garantizar su supervivencia y entregar el mejor servicio a sus Clientes.

El plan está orientado a establecer un adecuado sistema de seguridad física y lógica, en previsión de desastres. En este documento se resalta la necesidad de contar con estrategias que permitan realizar: Análisis de Riesgos, de Prevención, de Emergencia, de Respaldo y de Recuperación, para enfrentar algún desastre.

2. Objetivos del Plan

El objetivo de cada Plan de Continuidad es:

- Minimizar las consecuencias del desastre
- Posibilitar una vuelta al nivel de servicio, normal, rápida y sencilla.
- Mantener el control sobre una serie de eventos donde se pueda producir otro desastre.
- Priorizar las actividades de las personas y las estrategias usadas durante las fases de recuperación y restauración de la información.
- La seguridad de la información y equipos de tal manera que no ocurra otro desastre.
- Prevenir otros daños que puedan ser causados por el desastre.

3. Conceptos

3.1. Desastre

La falla de un sistema crítico, red o fuente de poder en un ambiente de cómputo; las pérdidas irreparables de la información o la interrupción de la funcionalidad del negocio, sin un plan para recuperar las actividades lo más pronto posible.

3.2. Riesgo

La probabilidad de que un suceso que amenaza atacar un sistema, vulnerable en particular, tenga éxito.

3.3. Procesos Críticos

Aplicaciones que han sido definidas como importantes para la operación de la empresa, que no es permitida ni la más mínima pérdida de su disponibilidad.

3.4. Análisis de Riesgo

Método para analizar las amenazas a los sistemas y la vulnerabilidad de estos, para poder establecer las posibles pérdidas y daños basados en la probabilidad que ocurra. El objetivo del análisis de riesgo es valorar el grado de aceptabilidad de cada riesgo para la operación del sistema.

3.5. Plan de contingencia

Secuencia de pasos preestablecidos que permitan recobrar las facilidades computacionales de la institución y/o las aplicaciones contenidas.

3.6. Vulnerabilidad

Cualquier debilidad existente en un sistema; más específicamente, la deficiencia de un sistema para ser atacado por alguna amenaza. La vulnerabilidad de un sistema puede existir independientemente de cualquier amenaza existente.

3.7. Impacto

Daños ocasionados a la empresa, como resultado del ataque de la amenaza a la vulnerabilidad del sistema. Por lo general es cuantificada en unidades monetarias o por pérdidas ocasionadas.

4. Análisis de Riesgo

En este análisis de riesgos se enumeran y describen los distintos equipos/servicios que pueden afectar de una manera u otra la continuidad de las operaciones del ITLA.

Cabe destacar que dentro del Departamento de TIC hay distintas áreas, cada una con distintos tipos de impacto en las operaciones del ITLA, estas áreas son:

- Sistemas.
- Redes.
- Bases de datos.
- Soporte Técnico.
- Audiovisuales.
- Software Factory.

Dentro de las distintas áreas del Departamento de TIC, se pueden identificar los siguientes equipos que deben de ser protegidos, también se muestra el impacto sobre la continuidad de operaciones del ITLA.

Área de Sistemas					
Equipos/servicio	**Cantidad**	**Función**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**
Servidor de archivos (File Server).	2	Este equipo es utilizado para almacenamiento de respaldo de información.	1	2	2
Correo institucional del ITLA.	1	La plataforma de correo institucional se utiliza para el envío de información, así como la comunicación interna y externa, con otras personas/entidades.	1	3	3
Sistema de Ticket.	1	El sistema de ticket se utiliza para gestionar los distintos servicios del Departamento de TIC, así como el de otras áreas de la institución.	1	2	2
Servidor DC/AD/DNS	2	Servidor de dominio y Active Directory.	1	3	3
Servidor de Backup	1	Servidor para realizar copia de seguridad de las instancias virtuales	1	2	2
Servidor MOODLE	2	Servidor para alojar las aulas virtuales del ITLA y todos los cursos virtuales.	1	3	3
Servidor de Virtualización	3	Este equipo se utiliza para fines de virtualización de equipos.	1	3	3
Servidor de Transporte	1	Servidor para compra de tickets para el uso del transporte por parte de los estudiantes.	2	2	4
Servidor de Biblioteca	1	Servidor para reserva y préstamo de libros a los estudiantes.	1	3	3

Portales web Institucionales	3	Estos son los portales Web institucional. Itla.edu.do es usado para ofrecer información y consulta al público. Orbi.edu.do es el portal académico estudiantil. Plataformavirtual.edu.do es la plataforma usada para interacción entre los maestros y estudiantes.	2	3	6

Área de Redes					
Equipos/servicio	**Cantidad**	**Función**	**Probabilidad**	**Impacto**	**Riesgo**
Central Telefónica, mensajería y videoconferencia.	7	Este es el equipo en donde se aloja el sistema de la central telefónica (Call Manager)	1	3	3
T1 de Voz y SIP trunking	2	Servicio de telefonía brindado por una compañía externa a la institución.	1	3	3
Servicio de Internet.	16	Este servicio brindado por una compañía/s externa, para la conexión a Internet.	1	3	3
Sistema de Chat omnicanal y Redes Sociales.	1	Este sistema sirve para habilitar más vía de comunicación con la institución a los usuarios.	1	2	2
Firewall y Switches del Core y Distribution.	11	Estos equipos sirven para conectar las distintas redes internas a Internet.	1	3	3
CISCO Call Manager Gateway.	2	Este equipo es el que se utiliza para realizar la conexión	1	3	3
Switch POE de 24 puertos (Edge Farm)	1	Este es el equipo en donde se conectan directamente todos los servidores de la red	1	3	3

		(telefonía, proxy, VPN, Base de datos, etc)			
Sistema de gestión y monitoreo de red.	3	Utilizado para monitorear la red.	1	2	2

Área de Base de datos					
Equipos/servicio	**Cantidad**	**Función**	**Probabilidad**	**Impacto**	**Riesgo**
Servidor de Base de datos de EXACTUS.	1	Almacena toda la información financiera del ITLA.	1	3	3

Área de Software Factory					
Equipos/servicio.	**Cantidad**	**Función**	**Probabilidad**	**Impacto**	**Riesgo**
Servidor de ORBI	1	Este equipo sirve de alojamiento para el sistema de inscripción ORBI (aplicación)	1	3	3
Servidor de base de datos (ORBI)	1	Este equipo sirve de alojamiento para la base de datos de ORBI (BD)	1	3	3
Servidor de JIRA	1	Servidor plataforma de Gestión de Proyectos	1	1	1
Servidor de Jenkis	1	Servidor para la publicación del desarrollo entre ambientes	1	1	1
Servicio de BITBUCKET.	1	Este servicio se utiliza para alojar el código fuente y otras informaciones importantes del sistema ORBI.	1	2	2
Servidores de Desarrollo y QA	2	Estos servidores son utilizados para el desarrollo y prueba de las aplicaciones	1	1	1

Servidor Demo	1	Servidor de Demostración de las soluciones desarrolladas	1	2	2

4.1. Niveles de Probabilidad:

En el contexto de evaluación de riesgos y probabilidad, los valores que mencionas se utilizan para describir la probabilidad de que ocurra un evento o un riesgo en particular. Aquí están definidos:

- **Improbable**: Significa que es poco probable que ocurra el evento o el riesgo. En otras palabras, las circunstancias que llevarían a este evento son raras o poco frecuentes.
- **Probable**: Indica que hay una buena posibilidad de que el evento o riesgo ocurra. No es seguro, pero es más que una simple posibilidad. Sugiere que las circunstancias propicias para que ocurra son relativamente comunes.
- **Posible**: Significa que existe una posibilidad de que el evento o riesgo ocurra, pero no se puede determinar con certeza si sucederá o no. Es un término intermedio entre "improbable" y "probable".

Estos términos se utilizan en la gestión de riesgos para ayudar a calificar y cuantificar cuán probable es que ocurra un evento y, por lo tanto, qué tan importante es gestionarlo adecuadamente.

4.2. Niveles de Impacto:

- **Alto:** Se refiere a que la inactividad de este equipo/servicio detiene directamente la producción o continuidad de negocio; este equipo/servicio es indispensable para el continuo y el buen funcionamiento de la institución. El tiempo máximo permitido (en hora/días) para recuperar o restablecer la operación de los equipos identificados con nivel de impacto alto es de 1-2 horas.
- **Medio:** Se refiere a que la inactividad o falta de este equipo/servicio puede hasta cierto punto afectar la producción o continuidad de negocio, sin embargo, no detiene el funcionamiento de la institución. El tiempo máximo permitido (en hora/días) para recuperar o restablecer la operación de los equipos identificados con nivel de impacto alto es de 1-12 horas.

- **Bajo:** Se refiere a que la carencia de este equipo/servicio no afecta la producción o continuidad de negocio de la institución. El tiempo máximo permitido (en hora/días) para recuperar o restablecer la operación de los equipos identificados con nivel de impacto bajo es de 1-2 días.

Para realizar un análisis de los riesgos se procede a identificar los objetos que deben ser protegidos, los daños que pueden sufrir, sus posibles fuentes de daño y oportunidad, su impacto en la institución, y su importancia dentro del mecanismo de funcionamiento.

Posteriormente se procede a realizar los pasos necesarios para minimizar o anular la ocurrencia de eventos que posibiliten los daños, y en último término, en caso de ocurrencia de estos, se procede a fijar un plan de emergencia para su recomposición o minimización de las pérdidas y/o los tiempos de reemplazo o mejoría.

4.3. Niveles de Riesgo

Los niveles de riesgo en ciberseguridad, como en otros campos, se utilizan para evaluar y clasificar la gravedad de posibles amenazas y vulnerabilidades. A continuación, se definen estos niveles de riesgo según la ciberseguridad:

- **Riesgo Aceptable:**
  Este nivel de riesgo se refiere a situaciones en las que una organización considera que la amenaza cibernética y sus posibles consecuencias son tolerables y manejables.
  Puede implicar un nivel bajo de vulnerabilidad o una baja probabilidad de que ocurra un incidente cibernético significativo.
  Las organizaciones pueden optar por aceptar este nivel de riesgo y asignar recursos limitados para mitigar o gestionar las amenazas, centrándose en prioridades más críticas.

- **Riesgo Significativo:**
  El riesgo significativo indica que la amenaza cibernética y sus posibles consecuencias tienen el potencial de causar daño sustancial a una organización.
  Puede implicar una mayor probabilidad de que ocurra un incidente o una mayor vulnerabilidad que requiera una atención más seria.
  Las organizaciones suelen tomar medidas activas para reducir este tipo de riesgo, como la implementación de medidas de seguridad adicionales, la inversión en tecnologías más avanzadas o la revisión de políticas y procedimientos de seguridad.

- **Riesgo Catastrófico:**
  El riesgo catastrófico es el nivel más alto de riesgo en ciberseguridad y se refiere a amenazas que pueden tener consecuencias devastadoras para una organización.
  Este nivel de riesgo implica una alta probabilidad de que ocurra un incidente de gran magnitud o una vulnerabilidad extremadamente crítica.
  Las organizaciones generalmente consideran inaceptable cualquier nivel de riesgo catastrófico y toman medidas exhaustivas para prevenirlo, como la inversión en soluciones

de seguridad avanzadas, la implementación de políticas de seguridad estrictas y la realización de pruebas de penetración y evaluaciones de seguridad exhaustivas.

Es importante que las organizaciones evalúen y clasifiquen sus riesgos cibernéticos de manera adecuada para tomar decisiones informadas sobre cómo asignar recursos y tomar medidas para proteger sus activos y datos frente a las amenazas en línea. La gestión eficaz de riesgos cibernéticos es esencial en la actualidad debido a la creciente sofisticación de las amenazas en el mundo digital.

4.4. Tabla de Matriz de Riesgo

Tabla de Matriz de Riesgo		Impacto		
		Bajo (1)	Medio (2)	Alto (3)
Probabilidad	Improbable(1)	1	2	3
	Probable (2)	2	4	6
	Posible (3)	3	6	9

Nivel de Riesgo	
Aceptable	(1-2)
Significativo	(3-4)
Catastrófico	(6-9)

4.5. Activos susceptibles a un daño

Una de las principales medidas que se debe tomar en cuenta a la hora de empezar un análisis de riesgo es identificar cuáles son los bienes y/o activos que pueden ser afectados por un daño y los cuales, en caso de ser afectados, pueden de igual forma afectar los servicios que ofrece la institución. Por ejemplo, en el ITLA se pueden identificar los siguientes:

- **Personal:** El personal clave para el manejo de los sistemas e infraestructura tecnológica.
- **Hardware:** Todos los equipos claves de la infraestructura tecnológica.
- **Software y utilitarios:** Softwares necesarios para la puesta en funcionamiento del instituto.
- **Datos e información:** Toda la información necesaria (Copias de respaldo de BD, información de usuarios, etc.)
- **Documentación:** Documentación física necesaria para la continuidad de operaciones del ITLA.
- **Suministro de energía eléctrica:** Se refiere al servicio eléctrico de la institución.

- **Suministro de telecomunicaciones:** Se refiere a los servicios de telecomunicaciones (Internet, voz, comunicación inalámbrica) que ofrecen las distintas prestadoras de servicio.

Estos bienes son de vital importancia para el buen funcionamiento del ITLA, por lo cual el personal del Departamento de TIC encargado de cada uno de estos bienes debe crear un plan de contingencia.

4.6. Daños

Los posibles daños que pueden ser causados a los sistemas informáticos del ITLA pueden referirse a daños como:

- Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, sea por causas naturales o humanas.
- Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, llámese, por ejemplo, cambios de claves de acceso, datos maestros claves, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.
- Imposibilidad de acceso a los recursos informáticos debido a daños causados por problemas ambientales como lluvias y/o huracanes, terremoto, incendio, impacto de asteroide, tsunami y/o inundaciones.

4.7. Prioridades

La estimación de los daños en los bienes, y su impacto, fija una prioridad en relación a la cantidad del tiempo y los recursos necesarios para la reposición de los servicios que se pierden en el acontecimiento. Por lo tanto, los bienes de más alta prioridad serán los primeros a considerarse en el procedimiento de recuperación ante un evento de desastre.

En el caso del Departamento de TIC las prioridades serán en base a la lista siguiente, tomando en cuenta el número #1 como la prioridad más alta:

1. La información de los sistemas críticos (las bases de datos de los distintos sistemas, información del File Server Administrativo, configuración de equipos, copias de respaldo)
2. El correo institucional.
3. El funcionamiento del sistema ORBI.
4. El funcionamiento del servidor de EXACTUS.
5. Verificar el funcionamiento del servidor de la central telefónica y su Gateway.
6. El funcionamiento de la red interna del ITLA

7. Verificar el funcionamiento de los servicios externos (Telefonía, Internet y electricidad)

4.8. Fuentes de Daño

Las fuentes de daño que han podido ser identificadas y las cuales pueden causar la falla de la operación normal del Departamento de TIC y de su centro de cómputo son:

1. Falla eléctrica general (incluyendo falla del Inversor y UPS del Data Center)
2. Falla de los servicios de Voz, ISP (Internet Service Provider) y comunicaciones inalámbricas (Flotas institucionales)
3. Falla de los equipos del Core y Distribución, ya sea por causas naturales (incendio, inundación, terremoto) y/o negación de servicio.
4. Falla de los equipos de soporte a los servicios internos, tales como servidores físicos.
5. Acceso no autorizado: Por vulneración de los sistemas de seguridad en operación (Ingreso no autorizado a las instalaciones, ya sea físicos o acceso virtual).
6. Ruptura de las claves de acceso a los sistemas computacionales:
    a) Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso (Virus, spybot, sabotaje).
    b) Intromisión no calificada a procesos, equipos y/o datos/bases de datos de los sistemas, ya sea por curiosidad o malas intenciones.
7. Desastres Naturales:
    a) Movimientos telúricos que afectan directa o indirectamente a las instalaciones físicas de soporte (edificios) y/o de operación (equipos computacionales).
    b) Inundaciones causadas por falla en los suministros de agua, entrada del mar, desborde de ríos y huracán.
    c) Incendio causado por cualquier desastre natural o de manera intencional.
    d) Fallas en los equipos de soporte:
        - Por fallas causadas por la agresividad del ambiente
        - Por fallas de la red de energía eléctrica pública por diferentes razones ajenas al manejo por parte de la institución.
        - Por fallas de los equipos de acondicionamiento atmosféricos necesarios para una adecuada operación de los equipos computacionales más sensibles.
        - Por fallas en la comunicación.
        - Por fallas en el tendido físico de la red local.
        - Fallas en las telecomunicaciones con instalaciones externas.
        - Por fallas de la Central Telefónica.
8. Fallas de Personal Clave: Se considera personal clave aquel que cumple una función vital en el flujo de procesamiento de datos u operación de los Sistemas de Información:

    a) Personal de Informática.
    b) Gerencia, supervisores y encargados.

Pudiendo existir los siguientes inconvenientes:

a) Enfermedad.
b) Accidentes.
c) Renuncias.
d) Abandono de sus puestos de trabajo.
e) Otros imponderables.

9. Fallas de Hardware:
   a) Falla en el Servidor de virtualización y Datos, tanto en su(s) disco(s) duro(s) como en el procesador central.
   b) Falla en el hardware de Red:
      - Falla en los Switches.
      - Falla en el cableado de la Red.
   c) Falla en el Router.
   d) Falla en el FireWall. (en caso de existir)

10. Incendios: Cualquier tipo de eventualidad con fuego que pueda causar algún daño en alguno de los equipos informáticos de la institución.

5. Medidas Preventivas

Se deben definir medidas generales para cada uno de los acontecimientos que puedan presentarse y puedan afectar los sistemas de cómputo de la institución.

Algunas, tales como:

- Actualización de los antivirus de los equipos.
- Actualización e instalación de parches de seguridad de los sistemas operativos.
- Escaneo de los equipos en busca de posibles virus/malware/spyware/keylogger y cualquier otro software malicioso, etc.

5.1. Control de Acceso

Los carnets que permiten la entrada a las áreas de acceso restringido son asignados a los usuarios a través del Departamento de Seguridad, con previa autorización del Departamento de Recursos Humanos.

*Referirse a las políticas del Departamento de Seguridad para la asignación de carnet de acceso.

5.2. Roles de usuarios

El Departamento de tecnología asigna roles de usuarios a colaboradores en función de sus necesidades y requisitos. A los colaboradores se les asigna un tipo de usuario cuando forman parte de la institución. El rol de usuario determina los privilegios que se pueden conceder al colaborador a través de un rol predeterminado o personalizado. Cada tipo de usuario incluye también acceso a aplicaciones, sistemas y paquetes de aplicación específicos.

5.3. Respaldos (Backups)

Las copias de respaldo o Backups, son realizados a los siguientes equipos:

- Equipos críticos del área de sistemas.
- Equipos críticos del área de redes.
- Bases de datos de los sistemas con nivel medio y alto de criticidad.
- Equipos de los usuarios finales.

Estas copias de respaldo se realizan tanto manualmente para algunos equipos críticos como de manera automática en los equipos de los usuarios finales; estas copias se guardan tanto en un equipo destinado a esto en el Data Center como en la nube.

*Referirse al procedimiento de realización de Backup del Departamento de TIC.
La copia de respaldo se realiza diario, tanto a la información de los usuarios como a las instancias virtuales.

5.3.1. Periodicidad de Backups:

- Instancias Virtuales: Se realizan Backup incremental tres veces a la semana. Se mantienen los últimos 06 (seis) Backups y los demás se reciclan según configuración del administrador.
- Snapshot. Se realizan en una frecuencia diaria
- Central telefónica y Contact Center. Se realizan en una frecuencia semanal. Se mantienen los últimos 03 (tres) Backups y los demás se reciclan según configuración del administrador.
- Archivo de configuración de Switch y Router. Se realiza en una frecuencia diaria. Se mantienen los últimos 30 (treinta) Backups y los demás se reciclan según configuración del administrador.
- Archivos de los usuarios finales. Se realizan al usuario al cerrar la sesión
- Base de Datos. Backup diferencial cada 2 horas, y full diario dos veces al día

5.4. Desastres Naturales

1- Rondas de revisión por las instalaciones y verificación de los servicios externos.
2- Generar reportes de casos irregulares.
3- Ejecutar planes de acción.
4- Si se conoce el evento organizar los equipos informáticos de manera tal que no sean afectados (colocar fundas, movilidad a un lugar seguro, desconectarlos, entre otras).

6. Plan de Recuperación

6.1. Objetivos del Plan de Recuperación

Los objetivos del plan de Recuperación son:

1) Determinación de las políticas y procedimientos para respaldar las aplicaciones y datos.
2) Planificar la reactivación dentro de las 12 horas de producido el desastre, todo el sistema de procesamiento y sus funciones asociadas.
3) Permanente mantenimiento y supervisión de los sistemas y aplicaciones.
4) Establecimiento de una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un desastre.

6.2. Alcance del Plan de Recuperación

El objetivo es restablecer en el menor tiempo posible el nivel de operación normal del centro de cómputos o de los equipos afectados, basándose en los planes de emergencia y de respaldo a los niveles del Centro de Cómputos y de los demás niveles.

La responsabilidad sobre el Plan de Recuperación es de la Administración, la cual debe considerar la combinación de todo su personal, equipos, datos, sistemas, comunicaciones y suministros.

6.3. Activación del Plan

6.3.1 Replicación de servicios

Actualmente la replicación de los servicios locales se realiza en la misma localidad del ITLA. A diferencia de las copias de seguridad de la información de los usuarios, instancias virtuales, base de datos los cuales se replican en servidores de terceros alojado en otros países.

6.3.2. Decisión

Queda a juicio del Rector, Gerente de Tecnología y/o comité de emergencia determinar la activación del Plan de Desastres, y además indicar el lugar alternativo de ejecución del Respaldo y/o operación de emergencia, basándose en las recomendaciones indicadas por éste.

6.3.3. Duración estimada

Los supervisores de cada área determinarán la duración estimada de la interrupción del servicio, siendo un factor clave que podrá sugerir continuar el procesamiento en el lugar afectado o proceder al traslado del procesamiento a un lugar alternativo.

6.3.4. Tiempos de Recuperación de Equipos y Servicios

Área de Sistemas			
Equipos/servicio	**Cantidad**	**Impacto**	**Tiempo de recuperación (RTO)**
Servidor de archivos (File Server).	2	Medio	0-12 horas
Correo institucional del ITLA.	N/A	Alto	N/A
Sistema de Ticket.	1	Medio	12-24 horas
Servidor DC/AD/DNS	2	Alto	1-4 horas
Servidor MOODLE	2	Alto	30 minutos
Servidor de Backup	1	Medio	4-8 horas
Servidor de Transporte	1	Medio	1 hora
Servidor de Biblioteca	1	Alto	30 minutos – 1 hora
Servidor de Virtualización.	3	Alto	1-4 horas
Portales Web Institucional	4	Alto	1-2 horas

Área de Redes			
Equipos/servicio	**Cantidad**	**Impacto**	**Tiempo de recuperación (RTO)**
Central Telefónica, mensajería y videoconferencia.	8	Alto	1-2 Horas

T1 de Voz y SIP trunking	2	Alto	1-2 horas
Servicio de Internet.	11	Alto	30-60 minutos
Sistema de Chat omnicanal y Redes Sociales.	1	Medio	4-8 horas
Firewall y Switches del Core y Distribution.	11	Alto	30-60 minutos
CISCO Call Manager Gateway.	2	Alto	1-2 horas
Switch POE de 24 puertos (Edge Farm)	1	Alto	30-45 minutos
Sistema de gestión y monitoreo de red.	3		1-2 días

Área de Base de datos			
Equipos/servicio	**Cantidad**	**Impacto**	**Tiempo de recuperación (RTO)**
Servidor de Base de datos de EXACTUS.	1	Alto	30 minutos

Área de Software Factory			
Equipos/servicio.	**Cantidad**	**Impacto**	**Tiempo de recuperación (RTO)**
Servidor de ORBI	1	Alto	1 hora
Servidor de base de datos (ORBI)	1	Alto	30 minutos – 2 horas
Servidor ORBI ADMIN	1	Medio	30 minutos – 2 horas
Servidor de JIRA	1	Bajo	30 minutos
Servidor de Jenkins	1	Bajo	30 minutos
Servicio de BITBUCKET.	1	Medio	30 minutos
Servidores de Desarrollo y QA	2	Bajo	1-3 horas
Servidor Demo	1	Medio	1-3 horas

6.3.5. Aplicación del Plan

Se aplicará el plan siempre que se prevea una pérdida de servicio por un período mayor de 48 horas, en los casos que no sea un fin de mes, y un período mayor a 24 horas durante los fines de mes (durante los cierres contables).

6.3.6. Responsabilidades

Este es el cuadro de responsabilidades según el área correspondiente dentro del Departamento de TIC.

Tabla de Responsabilidades	
Puesto	**Responsabilidad**
Gerente TIC.	Localizar, reunir y coordinar a los distintos responsables del área de TIC, para que los mismos inicien el diagnóstico de lugar y generen sus respectivos reportes.
	Proveer a la alta gerencia de la institución un reporte de daños y la estimación de los costos, así como del tiempo de estimación de la puesta en funcionamiento de los mismos.
	Supervisar las ejecuciones de las tareas del plan de recuperación.
Administrador de Sistemas.	Realizar el levantamiento de los equipos del área de sistemas afectados durante el Desastre, realizar el reporte de lugar y ejecutar las tareas para el restablecimiento de los servicios del área de sistemas.
Administrador de Redes.	Verificar el funcionamiento de los servicios externos y en caso de necesidad contactar a los proveedores para que los mismos provean un tiempo estimado de restablecimiento de los servicios.
	Realización de diagnóstico y revisión de daños ocasionados a la infraestructura de redes.

6.3.7. Acciones del Plan de recuperación Área de TIC.

En esta parte se explican las acciones concretas a seguir para la restauración de los servicios de las distintas áreas del Departamento de TIC.

Área de sistemas			
Equipos/ servicios	**Responsables**	**Porcentaje de daño**	**Acciones a tomar para mitigar el problema**
File Server Administrativo.	Soportes de Sistema	De 0 a 50% (Fallos del sistema operativo)	• Evaluar los daños del sistema operativo. • Verificar la integridad de la data de usuarios finales. • Reparar o reinstalar el sistema operativo y poner en línea el servidor.
		De 51% a 100% (Daños físicos del servidor)	• Evaluar los daños ocasionados al servidor principal. • Verificar la integridad de la data. • Solicitar las piezas/equipos para restaurar el servidor principal. • Realizar la instalación del hardware y/o software. • Realizar las configuraciones de lugar. • Restaurar la data de los usuarios. • Poner en producción el servidor primario.
Sistema de Ticket.	Soporte de Sistema	De 0 a 50% (Fallos del sistema operativo)	• Evaluar los daños del sistema operativo. • Verificar la integridad de la base de datos. • Reparar o reinstalar el sistema operativo y poner en línea el servidor. • Restaurar la base de datos de respaldo (de ser necesario)
		De 51% a 100% (Daños físicos del servidor)	• Evaluar los daños ocasionados al servidor principal. • Verificar la integridad de la base de datos. • Solicitar las piezas/equipos para restaurar el servidor principal. • Realizar la instalación del hardware y/o software. • Realizar las configuraciones de lugar. • Restaurar la base de datos de respaldo. (si es necesario) • Poner en producción el servidor primario.

Servidor de Backup	Administrador de Seguridad y Redes / Soporte de Sistemas.	De 0 a 50%. (Fallos del sistema operativo)	• Evaluar los daños del sistema operativo. • Reparar o reinstalar el sistema operativo y poner en línea el servidor. • Realizar las configuraciones de lugar. • Restaurar la base de datos de respaldo (de ser necesario)
		De 51% a 100% (Daños físicos del servidor)	• Evaluar los daños ocasionados al servidor principal. • Verificar la integridad de la base de datos. • Solicitar las piezas/equipos para restaurar el servidor principal. • Realizar la instalación del hardware y/o software. • Realizar las configuraciones de lugar. • Restaurar la base de datos de respaldo. (si es necesario) • Poner en producción el servidor primario.
Servidor DC/AD/DNS	Soportes de Sistema	De 0 a 50% (problemas de configuración)	• Evaluar los daños del sistema operativo. • Reparar o reinstalar el sistema operativo y poner en línea el servidor. • Realizar las configuraciones de lugar. • Restaurar la base de datos de respaldo (de ser necesario)
		De 51% a 100% (Daños físicos del equipo)	• Evaluar los daños ocasionados al servidor principal. • Verificar la integridad de la base de datos. • Solicitar las piezas/equipos para restaurar el servidor principal. • Realizar la instalación del hardware y/o software. • Realizar las configuraciones de lugar. • Restaurar la base de datos de respaldo. (si es necesario) • Poner en producción el servidor primario.

Servidor de Virtualización	Administrador de Seguridad y Redes / Soporte de Sistemas.	De 0 a 50% (problemas de configuración)	• Evaluar los daños del sistema operativo. • Evaluar la integridad de los sistemas virtualizados. • Reparar o reinstalar el sistema operativo. • Realizar las configuraciones de lugar. • Restaurar las distintas instancias virtuales de las copias de respaldo y/o en caso de no poseer, crearlas. • Poner el servidor en línea.
		De 51% a 100% (Daños físicos del equipo)	• Evaluar los daños ocasionados al servidor principal. • Verificar la integridad de los servidores/instancias virtuales. • Solicitar las piezas/equipos para restaurar el servidor principal. • Realizar la instalación del hardware y/o software. • Realizar las configuraciones de lugar. • Restaurar las instancias virtuales y/o en caso de no poseer, crearlas. • Poner en producción el servidor primario.
Correo institucional	Soporte de Sistemas / Administrador de Sistemas Administrador de Sistemas	De 0 a 50% (Problemas de acceso)	• Revisar el servicio de Internet de la institución. • Revisar la disponibilidad del servicio de correo de Google. • Revisar el archivo de direccionamiento en nuestro portal Web. • Contactar al personal de Google vía Live-chat dentro del portal de administración del correo el cual tienen acceso: el Soporte de Sistemas y el Administrador de Sistemas.
		De 51% a 100% (Problemas con la data de los usuarios)	• Contactar inmediatamente al personal de Google vía Live-chat dentro del portal de administrador de correo, al cual tienen acceso: el Soporte de Sistemas y el Administrador de Sistemas.

Área de redes			
Equipos/ Servicios	**Responsables**	**Porcentaje de daño**	**Acciones a tomar para mitigar el problema**
T1 de voz y IP trunking	Administrador de Redes	De 0 a 50%	• Revisión de los equipos a nivel interno para descartar cualquier avería interna. • Realizar un ticket al proveedor CLARO al 809-220-1212 y conseguir el tiempo de resolución del problema.
		De 51% a 100%	• Realizar un ticket al proveedor CLARO al 809-220-1212 y conseguir el tiempo de resolución del problema. • Pasar el número de ticket al ejecutivo de cuentas (Julio Cesar Delgado) para agilizar el proceso.
Servicio de Internet (proveedor)	Administrador de Redes /Soporte de Adm. Redes	De 0 a 50%	• Revisión de los equipos a nivel interno para descartar cualquier avería interna. • Realizar un ticket al proveedor CLARO al 809-220-1212 y conseguir el tiempo de resolución del problema.
		De 51% a 100%	• Realizar un ticket al proveedor CLARO al 809-220-1212 y conseguir el tiempo de resolución del problema. • Pasar el número de ticket al ejecutivo de cuentas (Julio Cesar Delgado) para agilizar el proceso.
Central Telefónica, mensajería y videoconferencia.	Administrador de Redes	De 0 a 50%. (Fallos del sistema operativo)	• Verificar el estatus de los servicios del Call Manager. • En caso de que el inconveniente persista, reiniciar el equipo para que los servicios vuelvan a su estado normal. • Si el sistema operativo esta corrompido, proceder con la restauración de un backup anterior. • Si no se posee un backup se procedería a reinstalar el sistema operativo con las funciones básicas necesarias para lograr comunicación.
		De 51% a 100% (Daños físicos del servidor)	• Determinar el grado de avería del servidor para ver si se puede reparar.

			• En caso de que no se pueda reparar, se procede a identificar un equipo con la capacidad suficiente para virtualizar el sistema operativo del Call Manager, de forma temporal hasta que sea restaurado el servidor principal. • Solicitar la compra o adquisición de las piezas o equipos de lugar para restaurar el equipo del Call Manager de forma permanente.
CISCO Call Manager Gateway	Administrador de Redes	De 0 a 50% (problemas de configuración)	• Se verifica la configuración del equipo, en caso de que se encuentre alguna anormalidad se restaurara un backup del archivo de configuración. • En caso de que no se encuentre un archivo de configuración se configura el equipo desde cero (0).
		De 51% a 100% (Daños físicos del equipo)	• Verificar la integridad del equipo para determinar la magnitud del daño. • Identificar un equipo que se pueda utilizar de manera temporal y restaurarle el archivo backup de configuración debidamente modificado para que el mismo sea compatible con el nuevo equipo. • Gestionar la compra del equipo definitivo.
Firewall y Switches del Core y Distribution	Administrador de Redes	De 0 a 50% (problemas de configuración)	• Se verifica la configuración del equipo, en caso de que se encuentre alguna anormalidad se restaurara un backup del archivo de configuración. • En caso de que no se encuentre un archivo de configuración se configura el equipo desde cero (0).
		De 51% a 100% (Daños físicos del equipo)	• Verificar la integridad del equipo para determinar la magnitud del daño. • Identificar un equipo (preferiblemente del aula de CCNP) que se pueda utilizar de manera temporal y restaurarle el archivo backup de configuración debidamente modificado para que el

			mismo sea compatible con el nuevo equipo. • Gestionar la compra del equipo definitivo.
Switch POE de 24 puertos (Edge Farm)	Administrador de Redes /Soporte de Adm. Redes	De 0 a 50% (Daños de configuración del equipo)	• Se verifica la configuración del equipo, en caso de que se encuentre alguna anormalidad se restaurara un backup del archivo de configuración. • En caso de que no se encuentre un archivo de configuración se configura el equipo desde cero (0).
		De 51% a 100% (Daños físicos del equipo)	• Verificar la integridad del equipo para determinar la magnitud del daño. • Identificar un equipo (preferiblemente del aula de CCNP) que se pueda utilizar de manera temporal y restaurarle el archivo backup de configuración debidamente modificado para que el mismo sea compatible con el nuevo equipo. • Gestionar la compra del equipo definitivo.

Área de Base de datos			
Equipos/ Servicios	**Responsables**	**Porcentaje de daño**	**Acciones a tomar para mitigar el problema**
Servidor de Base de datos de EXACTUS	Administrador de Sistemas	De 0 a 50% (Fallos del sistema operativo)	• Evaluar los daños del sistema operativo. • Migrar data (ya sea la actual del servidor o un backup) a un servidor virtual o un servidor secundario para continuar las operaciones. • Reparar el sistema operativo y poner en línea el servidor principal. • Restablecer la data del servidor virtual en el servidor principal.

		De 51% a 100% (Fallos físicos del servidor)	• Evaluar los daños ocasionados al servidor principal. • Migrar data (ya sea la actual del servidor o un backup) a un servidor virtual o un servidor secundario para continuar las operaciones de manera temporal. • Solicitar las piezas/equipos para restaurar el servidor primario. • Realizar la instalación del hardware y/o software. • Restaurar la base de datos del sistema secundario en el servidor primario. • Poner en producción el servidor primario.

Área de Software Factory.			
Equipos/ Servicios	**Responsables**	**Porcentaje de daño**	**Acciones a tomar para mitigar el problema**
Servidores de Aplicaciones	Soporte Sistemas / QA Developer	De 0 a 50% (problemas de acceso al servidor)	• Evaluar si el inconveniente de conexión es de red local, externo (ISP) o es problema del proveedor. • Si es problema de red local o del ISP, referir el problema al área de redes. • Si un inconveniente con el proveedor (disponibilidad del servicio, llamar al ejecutivo de cuenta correspondiente. (Julio Cesar Delgado 809-330-2000)
		De 51% a 100% (si se tiene acceso, pero se tiene inconveniente con el sistema/equipo)	• Diagnosticar el problema. • Verificar la integridad de la data/Base de datos del equipo. • Verificar las posibles soluciones e implementarlas. • Probar las posibles soluciones y/o contactar al ejecutivo de cuentas en caso de ser necesario para que el mismo provea un tiempo estimado de resolución del problema. • Restaurar las bases de datos de respaldo (en caso de ser necesario)

7. Redundancia en servicio de internet

Contamos con 2 proveedores de internet y en nuestro firewall tenemos configurado SD-WAN, esto nos facilita configurar failover, de tal forma que, si falla un proveedor, el tráfico se va por el o los proveedores disponibles de forma automática.

- **Proveedor CLARO**
  Consultor de Venta de Servicios Fijos/ Consultor de Servicios
  809-220-5199 / 220-2721

- **Proveedor Altice**
  Consultor de Servicios
  809-629-0353

8. Redundancia en servicio telefónico y centro de contacto

Contamos con redundancia en cada una de las instancias virtuales que conforman el ITLA Voice Collaboration. Tenemos dos proveedores de servicio telefónico.

- **Proveedor CLARO**
  Consultor de Venta de Servicios Fijos/ Consultor de Servicios
  809-220-5199 / 220-2721

- **Proveedor Altice**
  Consultor de Servicios
  809-629-0353

9. Redundancia con los Servidores Locales

Contamos redundancia para los servidores de la Nube con servidores físicos, los cuales además permiten el balanceo de carga en periodos de inscripción.

10. Políticas de contraseñas

Se aplica a todos los usuarios de los Servicios TIC del ITLA la siguiente política de contraseñas:

- La longitud de la contraseña debe ser como mínimo de 8 caracteres, si bien se recomienda usar contraseñas más largas.
- La contraseña debe contener al menos 4 caracteres alfabéticos de los cuales serán, al menos, dos letras mayúsculas y dos minúsculas.
- La contraseña debe contener al menos 2 caracteres numéricos.
- El número máximo de repeticiones de caracteres adyacentes de la contraseña será 2.

- El número máximo de caracteres numéricos en secuencia de la contraseña será 2.
- No compartir la contraseña bajo ningún concepto con otras personas, aunque sean de su mismo entorno.
- Guardar la información de contraseñas en un lugar seguro.
- Política de cambio obligatorio de contraseña cada 3 meses.
- No utilizar fechas de nacimiento propios ni del entorno en la contraseña.
- No utilizar en la contraseña palabras o nombres comunes Ej. Juan
- No se podrá utilizar la última contraseña empleada.
- Modificar la contraseña entregada por primera vez antes de hacer uso de ella.
- Que contenga al menos un símbolo (cualquier otro carácter que no sea alfabético o numérico: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /).