UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA

OFICINA DE TECNOLOGIAS DE LA INFORMACION (OTI)

PLAN DE CONTINGENCIA DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION DE LA UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA

Iquitos, enero del 2022

ÍNDICE

INTRODUCCIÓN

El siguiente Plan de Contingencia de la Oficina de Tecnologías de la Información (OTI) de la Universidad Nacional de la Amazonía Peruana (UNAP), es un documento cuyo propósito es la de establecer los lineamientos de respuesta para atender en forma oportuna, eficiente y eficaz, daños en equipos informáticos o alteraciones producto de eventos naturales u otros, a causa de algún incidente tanto interno como externo a tecnologías de la información.

Mediante el desarrollo del plan de contingencia, se presentan diversas actividades propias de la gestión que deberá tomar en cuenta la Oficina de Tecnologías de la Información, cubriendo así los posibles incidentes que afecten el sistema de información. Al mismo tiempo, aspectos conceptuales que permitan un mayor panorama acerca del entendimiento de las contingencias y que servirán como marco de referencia, para la elaboración de las políticas, normas y procedimientos de contingencia.

Los motivos para aplicar el plan de contingencia pueden ser variadas, como, por ejemplo: Daños en los equipos de cómputo o diversos dispositivos de comunicación), daños en los activos de redes, daños de los servidores de la institución.

La elaboración del plan de contingencia implica un importante avance a la hora de superar situaciones de interrupción de las actividades y servicios prestados por la Oficina Central de Informática de la UNAP.

Es indispensable para el éxito del plan de contingencia, contar con personal capacitado y comprometido con la institución.

ORGANO RESPONSABLE:

- Oficina de Tecnologías de la Información de la UNAP.

I. ETAPAS DEL PLAN:

- Análisis de Riesgos.
- Plan de Respaldo.
- Plan de Recuperación.

II. DEFINICIÓN:

El plan de contingencia informático de la Oficina de Tecnologías de la Información, es un documento que establece los lineamientos de respuesta para atender en forma oportuna, eficiente y eficaz, daños en equipos de cómputo o desastres producto de eventos naturales u otros, a causa de algún incidente tanto interno como externo a tecnologías de información.

El plan de contingencia propone una serie de procedimientos alternativos al funcionamiento normal de la organización, cuando alguna de sus funciones usuales se ve perjudicada por una contingencia interna o externa.

Este plan, por lo tanto, intenta garantizar la continuidad del funcionamiento de la organización frente a cualquier eventualidad, ya sean materiales o personales. Un plan de contingencia incluye cuatro etapas básicas: la planificación, la identificación de riesgos, la identificación de soluciones y la implementación.

III. DIAGNÓSTICO SITUACIONAL:

La Oficina de Tecnologías de la Información (OTI), es una oficina de apoyo que depende directamente de la Oficina de Rectorado; siendo el Rector de la UNAP el jefe inmediato superior del jefe del OTI.

El jefe de la Oficina de Tecnologías de la Información, ejerce autoridad sobredicha oficina; y por la naturaleza de sus actividades, ejerce autoridad funcional sobre el personal de las unidades operativas.

La Oficina de Tecnologías de la Información por naturaleza de sus funciones, mantiene coordinación interna con las unidades organizativas de la Universidad Nacional de la Amazonía Peruana y, en el ejercicio de sus funciones, mantiene coordinación externa con las instituciones y otras entidades que le son afines o necesarias.

Se anexa los equipos o dispositivos con los que cuenta la Oficina de Tecnologías de la Información.

IV. NECESIDAD DE REALIZAR EL PLAN DE CONTINGENCIA:

Es necesario por tanto la identificación previa de cuáles de los procesos son críticos y cuáles son los recursos necesarios para garantizar el funcionamiento de las aplicaciones de gestión.

Debe contemplar los planes de emergencia, Backup, recuperación, comprobación mediante simulaciones y mantenimiento del mismo. Un plan de contingencia adecuado debe ayudar a la Oficina de Tecnologías de la Información de la UNAP a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal de la Oficina.

V. FINALIDAD:

El referido plan tiene como finalidad identificar los riesgos, establecer los procedimientos y mecanismos necesarios para afrontar cualquier eventualidad que se produzca, preservando la seguridad de los equipos de cómputo, protegiendo la información almacenada en ellos y garantizando la continuidad de las funciones de la Oficina de Tecnologías de la Información.

VI. OBJETIVO GENERAL:

Garantizar la continuidad de las operaciones de los elementos considerados que componen los Sistemas de información, para la Oficina de Tecnologías de la Información de la UNAP.

Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

VII. OBJETIVOS ESPECÍFICOS:

- Prevenir o minimizar la pérdida o la corrupción de archivos de datos críticos para la continuidad de las operaciones de los diversos sistemas que cuenta la Institución.
- Proteger la propiedad de la Universidad Nacional de la Amazonia Peruana.
- Continuar con las funciones, en el ámbito informático, de las diferentes áreas de la UNAP, que se haya visto afectada por una situación adversa.
- Prevenir o minimizar el daño permanente a los recursos informáticos.

VIII. LOGRO QUE SE ESPERA ALCANZAR:

Brindar un óptimo funcionamiento y proteger toda la información que se procesa día a día la misma que es almacenada en los servidores que utiliza la Oficina Central de Informática.

IX. ÁMBITO DE APLICACIÓN:

Universidad Nacional de la Amazonía Peruana.

X. ACTIVIDADES A REALIZAR:

A. El Plan de Contingencia y Seguridad de la Información:

El Plan de Contingencia se elabora en la Oficina de Tecnologías de la Información de la UNAP; Este plan está diseñado para ser aplicado en las instalaciones de la OTI, involucrando al personal y equipos que intervienen en las funciones de la UNAP que emplean recursos informáticos y contemplan el los equipos, las aplicaciones informáticas y los datos que la institución procesa.

Los resultados esperados son establecer las acciones necesarias en la función informática que permitan la continuidad del negocio, ante cualquier siniestro que pudiera ocurrir.

B. Esquema General:

El Plan de Contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos las instalaciones, equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que en el Plan de Contingencia se hará un análisis de los riesgos (Antes), cómo reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentará el problema (Durante).

Pese a todas las medidas se seguridad con las que cuenta la institución puede ocurrir un desastre, por tanto, es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres (Después), el cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles. Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo posible.

Comenzaremos por identificar los tipos de riesgos y los factores para proceder a un plan de recuperación de desastres, así como las actividades previas al desastre, durante y después del desastre.

C. Definiciones de Términos Empleados:

- **Amenaza**: Evento de origen natural o causado por el ser humano que puede ocurrir, y que cuando sucede tiene consecuencias negativas sobre las personas, bienes, servicios, sistemas informáticos y datos.

- **Vulnerabilidad**: debilidad que presentan los activos y que facilita la materialización de las amenazas.

- **Contingencia**: Interrupción no planificada de la disponibilidad de recursos informáticos.

- **Plan de Contingencia**: Son procedimientos que definen cómo un negocio continuará o recuperará sus funciones críticas en caso de una interrupción no planeada debido a la materialización de una amenaza.

- **Proceso crítico**: Proceso considerado indispensable para la continuidad de las operaciones y servicios de del área de TI, y cuya falta o ejecución deficiente puede tener un impacto operacional o de imagen significativo para la institución.

- **Impacto**: Es la consecuencia de la materialización de una amenaza sobre un activo, aprovechando una vulnerabilidad. El impacto de una amenaza es la magnitud del daño que ocasiona en la institución, y se encuentra clasificado en: Alto, Medio y Bajo.
  Hay que indicar que hay amenazas que, si bien no representan un impacto alto en la inmediatez, puede volverse de impacto Alto si se mantiene por un tiempo más allá de lo tolerable por el negocio.

D. Análisis e Identificación de Riesgos:

En la Oficina Central de Informática, se ha identificado las siguientes Amenazas y el impacto que causa en continuidad del negocio:

Cód.	Amenaza	Impacto
A-01	Infección por acción de virus.	Medio
A-02	Falla de suministro eléctrico.	Alto
A-03	Incendio.	Alto
A-04	Intrusión en las redes informáticas.	Alto

A-05	Daño de componente en los servidores.	Medio
A-06	Caída de Acceso a Internet del proveedor.	Medio
A-07	Falla de comunicación vía Radio-Enlace entre locales.	Medio

a) Infección por acción de virus:
La Oficina Central de Informática cuenta con el antivirus NOD32 para los servidores y para las estaciones de trabajo; asimismo a través de la red se hacen las actualizaciones del antivirus hacia las máquinas correspondientes. Sin embargo, hay muchos factores de riesgo para una posible infección por virus.

b) Falla de suministro eléctrico:
Es el corte intempestivo del suministro de la energía eléctrica, ocasionado por algún factor externo (corte de la línea de transmisión, accidentes, falla en los sistemas de protección, etc.). en muchos casos puede generar fallos en los dispositivos.

c) Incendio:
La Oficina Central de Informática, a pesar de contar con sistemas de protección contra incendios, (extintores manuales, alarmas contra incendios, vías de acceso y de evacuación, etc.). algún incidente involuntario puede ocasionar el inicio de un incendio.

d) Intrusión en las redes informáticas:

- **Intrusión mediante la red cableada.**
  Sólo personal autorizado deberá ingresar a las áreas restringidas donde se encuentra la Sala de Servidores y/o otros lugares donde se encuentren los equipos informáticos; si otras personan ingresan debe ser con autorización y coordinación de la jefatura inmediata y en los tiempos establecidos y/o coordinados.

- **Intrusión mediante la red inalámbrica.**
  Sólo personal autorizado (Administrativos, Docentes y Estudiantes) podrán ingresar a la red de la UNAP, los alumnos tienen una conexión libre a una red paralela exclusivamente para ellos, la cual no necesita configuración previa de los dispositivos. Cabe recalcar que toda la red de la UNAP cuenta con unas reglas de bloqueo de páginas no autorizadas a cualquier usuario (YouTube, Facebook, Twitter, etc.).

  Para preservar un estado óptimo la administración de la red de la UNAP es necesario tener en cuenta lo siguiente:
  - Restringir el acceso a las redes inalámbricas de la UNAP usando siempre claves de acceso a la conexión y filtrado MAC en todos los Access Point montados en las instalaciones de la UNAP.
  - Configurar cada dispositivo con las opciones de red de la UNAP (Proxy, IP, Máscara de subred y Puerta de Enlace.
  - Solicitar clave de ingreso a los servidores y sistemas.

- Mantener siempre activo el filtrado de las direcciones MAC de los dispositivos conectados al Punto de Acceso de la Oficina de Tecnologías de la Información.
- Realizar un registro de todos los dispositivos conectados a la red de la UNAP mediante IP, para mayor control de dichos dispositivos en la red.
- Registrar toda la actividad de la estación de trabajo con el visor de sucesos y los logs de los servidores.
- Mantener siempre activo el Firewall PfSense para evitar ataques DDoS o algún tipo de intrusión informática.

e) Daño de componente en los servidores:

Los servidores de la UNAP son parte elemental del adecuado funcionamiento de la Universidad, pues albergan a todos los sistemas que la UNAP requiere para brindar una educación de calidad, siendo estos, también un requisito fundamental para la conectividad entre los trabajadores administrativos, docentes y estudiantes.

Dichos servidores se encuentran ubicados en el Data Center de la Oficina de Tecnologías de la Información, por lo tanto, está bajo la responsabilidad de la misma.

f) Caída de Acceso a Internet del proveedor:

El servicio de acceso a Internet de la UNAP es suministrado por proveedores externos, los cuales han sido seleccionados a través de procesos de adjudicación. La UNAP actualmente tiene contrato por 2 líneas independientes:

- Línea de Internet dedicada de 10 Mbps, exclusiva para la parte administrativa.
- Línea de Internet dedicada de 5 Mbps, exclusiva para las aulas y laboratorios de las facultades.

Las 2 líneas de internet ingresan físicamente del proveedor al Data Center de la UNAP (local Herbario), y de ahí se distribuyen a los demás locales de la UNAP vía Radio-Enlace, ya que los locales están dispersos por la ciudad de Iquitos y alrededores, imposibilitando su distribución por cables.

La UNAP dispone de equipos de comunicaciones y software que permite distribuir este recurso, y controlarlo.

g) Falla de comunicación vía Radio-Enlace entre locales:

Para la interconexión de sus locales, la UNAP dispone en cada uno de ellos de al menos una torre de comunicaciones con su respectiva antena de radio-enlace, la cual le permite enviar y recibir la información.

Lamentablemente, estas antenas están expuestas a las condiciones climatológicas (sol y lluvia) y en muchos casos a descargas eléctricas

producto de los rayos y subidas de tensión del suministro eléctrico, lo que hace que eventualmente se malogren.

XI. ANÁLISIS DE RIESGOS:

Para realizar un análisis de los riesgos, se procede a identificar y evaluar los objetos que deben ser protegidos, los daños que éste pueda sufrir, sus posibles fuentes de daño, su impacto dentro de la Oficina de Tecnologías de la Información 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 éstos, se procede a fijar un plan de emergencia para su recomposición o minimización de las pérdidas y/o los tiempos de reemplazo o mejoría.

A. Bienes susceptibles de un daño:

Se puede identificar los siguientes bienes afectos a riesgos:

- Personal.
- Hardware.
- Software y Utilitarios.
- Datos e información.
- Documentación.
- Suministro de energía eléctrica.
- Suministro de telecomunicaciones.

Los posibles daños pueden referirse a:

a) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, sea por causas naturales o por causas humanas.

b) Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, por ejemplo:
Cambios de claves de acceso, datos maestros claves, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

c) Divulgación de información y que afecte su patrimonio estratégico y/o Institucional, sea mediante robo o infidencia.

B. Prioridades:

La estimación de los daños en los bienes y su impacto, fija una prioridad con relación a la cantidad de tiempo y los recursos necesarios para la reposición de los Servicios que se pierden en dicho acontecimiento.

Por lo tanto, los bienes que tienen más alta prioridad serán los primeros a considerarse en el procedimiento de recuperación ante un evento de desastre.

C. Fuentes de daño:

Las posibles fuentes de daño que pueden causar la no operación normal de la institución son:

a) Acceso no autorizado:

- Por vulneración de los sistemas de seguridad en operación (Ingreso no autorizado a las instalaciones).
- Ruptura de las claves de acceso a los sistemas computacionales.
- Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso (virus, sabotaje, ejecución de scripts malintencionados)
- Intromisión no calificada a procesos y/o datos de los sistemas, ya sea por curiosidad o malas intenciones.

b) Desastres Naturales:

- Movimientos telúricos que afecten directa o indirectamente a las instalaciones físicas de y/o de operación (equipos computacionales y/o servidores).

- Por fallas causadas por la agresividad del ambiente.

- Inundaciones causadas por falla en los suministros de agua.

c) Fallas de Hardware y Equipos de Soporte:

- Falla en el Servidor de Aplicaciones, Servidor Proxy, Servidor Controlador Dominio y Datos, tanto en su(s) disco(s) duro(s) como en sus demás componentes.
- Falla en los Switches.
- Falla en el Cableado de la Red.
- Falla en el Router.
- Falla en el Firewall.
- Falla en el Aire Acondicionado en la Sala de Servidores.
- Incendios.
- Por fallas de red de energía eléctrica pública por diferentes razones ajenas.
- Por fallas de la comunicación.
- Por fallas en el tendido físico de la red local.
- Por fallas en las telecomunicaciones con instalaciones externas.

d) Por fallas de Personal Clave:

Se considera personal clave a aquel que cumpla una función vital en el flujo de procesamiento de datos u operación de los Sistemas de Información: Administrador de servidores y servicios en línea, Unidad de atención y soporte al usuario, etc. Pudiendo existir los siguientes inconvenientes: Enfermedad, accidentes, renuncias, abandono de sus puestos de trabajo, otros imponderables.

D. Medidas Preventivas:

a) Control de Accesos:

La Oficina de Tecnologías de la Información de la UNAP cuenta con el documento “Directiva de Seguridad DataCenter”, en la cual están indicadas las medidas restrictivas para el acceso a sus instalaciones y al área específica de los servidores.

b) Previsión de desastres Naturales:

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en la Oficina de Tecnologías de la Información, correspondientes en la medida de no dejar objetos en una posición tal que ante un movimiento telúrico de cierta magnitud pueda generar mediante su caída y/o destrucción, la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación

de los archivos, discos externos, discos con información vital de respaldo de aquellos que se encuentren aún en las instalaciones. Se deberán tener el respaldo en lugares diferentes y con un código de identificación que maneje el personal de sistemas.

c) Adecuado Soporte de Utilitarios:

El tiempo de paro por fallas de los equipos deberá minimizarse mediante el uso de otros equipos, a los cuales también se les debe controlar periódicamente su buen funcionamiento; La OTI-UNAP cuenta con:

- UPS para respaldo de energía.
- Servidor en stock ante cualquier eventualidad que pudiera suceder.

d) Seguridad otorgada por el Personal:

Se incentiva al personal a compartir sus conocimientos con sus colegas dentro de cada área o unidad, en lo referente a la utilización de los software y elementos de soporte relevantes

El área de Service Desk registra las incidencias que los usuarios reportan, en el software GLPi, se hace seguimiento de las atenciones que el personal de soporte está realizando.

Para el caso que el personal requiera subir a las torres de comunicaciones, se dispone de arnés de seguridad.

e) Seguridad de la Información:

Los datos y los Sistemas de Información que se encuentran en los servidores del OTI-UNAP, se protegen mediante:

- Claves de acceso.
- Niveles de uso de los usuarios de la información.
- Discos duros para el respaldo de softwares y bases de datos.
- Política de Copia de Seguridad (Backup) de la información.

XII. PLAN DE RESPALDO (BACKUP) DE LA INFORMACIÓN:

La OTI-UNAP cuenta con el “Manual de Procedimientos”, en dicho documento, se encuentra detallado el procedimiento para la realización de las copias de seguridad (respaldo o backup) total e incremental.

Se han identificado para los respaldos:

a) Los Sistemas de Información que utiliza la UNAP.
b) Las Bases de Datos de los Sistemas de Información.
c) El Portal Web.

Está establecido la relación de los sistemas informáticos y las bases de datos a respaldar.

Los respaldos se hacen mediante los discos duros externos adquiridos para dicho fin, se controla la capacidad de almacenamiento.

El personal pertinente realiza el respaldo de la información en la periodicidad indicada, y está entrenado para ello. El respaldo de la información se realiza con éxito.
El horario de respaldo se ha establecido fuera del horario de oficina, con el fin de que el uso de los sistemas informáticos por parte de los usuarios no interfiera con el proceso de Backup.

- **Sistemas de Información de la UNAP:**

SISTEMA DE INFORMACIÓN	USUARIOS	IMPACTO
Sistema Central	Abastecimiento, Almacén Central, Tesorería.	Alto
SIAF (Sistema Integrado de Administración Financiera)	Abastecimiento, Contabilidad, Programación y presupuesto, Almacén Central, Tesorería, Personal – Planilla.	Alto
ConCais	Abastecimiento, Tesorería.	Alto
COA (Confrontación de Operaciones Auto declaradas)	Abastecimiento, Contabilidad, Tesorería.	Alto
SIMI (Control Patrimonial de Bienes Estatales)	Patrimonio	Alto
Sicarf (Sistema de Administración de Recursos Financieros) (cobranza)	Tesorería	Alto

Banco de la Nación Depósitos a cuentas del banco.	Personal - Planilla	Alto
Sistema de Boletas Sistema de Boletas de Pagos.	Personal - Planilla	Alto
Universitas XXI (Sistema integrado de Gestión Académica)	DRAA, Dependencias Académicas	Alto
Sistema de Resoluciones (Registro de Resoluciones emitidas)	Dependencias Académicas, Rectorado	Medio
Win ISIS Registro de Tesis, Folletos y Libros en físico.	Biblioteca Central	Alto
DSpace (Repositorio digital de Tesis, Revistas, Folletos)	Biblioteca Central	Medio
Libro de Reclamaciones	Imagen Institucional,	Medio
Portal web	OTI	Alto
PfSense (Sistema de seguridad perimetral – Firewall)	OTI	Alto
Correo Institucional	OTI	Medio
Moodle (Sistema de Aula Virtual)	OTI	Medio
GLPI (Gestionnaire libre de parc informatique – Sistema de Help Desk)	OTI	Medio

XIII. PLAN DE CONTINGENCIA:

A. Activación del Plan:

El Plan de Contingencia de la OTI-UNAP se activará inmediatamente detectado o reportado la materialización de la amenaza.
El Plan de Contingencia debe ser ejecutado por el personal designado en cada caso.

Ante el acontecimiento del desastre, se debe reportar inmediatamente al Jefe de OTI para su conocimiento.

B. Duración del Proceso:

Cada caso descrito en este plan es particular, y el tiempo en restablecer el servicio varía en función de la magnitud del daño.

Otro factor que influye es el restablecimiento del servicio, es la disponibilidad de los recursos de contingencia, por ejemplo, ante el malogro de una antena de Radio-Enlace, se debe esperar la adquisición de un equipo nuevo, el cual demora dependiendo de la disponibilidad económica de la institución.

La OTI-UNAP está comprometido en restablecer el servicio en el menor tiempo posible.

C. Aplicación del Plan:

Se aplicará el plan en los siguientes casos:

- Si se identifica que la amenaza detectada o reportada puede malograr un bien físico o alterar los datos.
- Hay una pérdida de disponibilidad del servicio.
- Si se recibe una llamada de urgencia que se está desarrollando un proceso administrativo sumamente importante en el cual la UNAP debe responder ante entidades externas (MEF, SUNEDU, MINEDU, etc.).
- Si se recibe una llamada de urgencia que se está desarrollando un proceso académico sumamente importante (Matrícula, ingreso de notas, u otros).

D. Procedimientos del Plan de Contingencia:

A-01: Infección por Acción de Virus.
En caso de infección masiva de virus se debe de seguir el siguiente plan de contingencia: 1. Revisar las alertas que envía el antivirus y ver el tipo de virus que se está propagando detectando el origen del virus. A su vez desconectar de la red el equipo que está infectado y que está reenviando el virus. 2. Comprobar si tiene carpetas compartidas en forma total y proceder a no compartirlas. 3. Proceder a limpiar los archivos con la opción de: LIMPIAR (o CLEAN INFECTED FILES); No con DELETED porque esta opción podría borra archivos del sistema operativo, quedando inutilizada la máquina. 4. Una vez limpio el equipo, proceder a realizar una copia de Seguridad sólo de la Data. 5. Si no se lograra limpiar en forma satisfactoria, el equipo, porque los archivos del sistema operativo han sido dañados se procederá a formatear el disco reinstalándole el sistema operativo y transfiriendo la data de seguridad, que se tiene en caso de servidores y de los archivos personales en caso de PC y/o Servidor de Archivos si los hubiera; donde se custodia la data de los usuarios.
Personal Responsable: − Administrador de servidores y servicios en línea. Personal de Apoyo: − Administrador de la Red y Seguridad Perimetral.
Recursos Necesarios: − Software de monitoreo de tráfico de red Zabbix. − Software antivirus NOD32.

A-02: Falla de suministro eléctrico.

Esta falla, tanto en el origen como al final (retorno de la energía) pueden causar daños a los equipos de cómputo, por lo que se debe de seguir el siguiente procedimiento:

1. Se activarán las luces de emergencia en la Oficina de Tecnologías de la Información.
2. Revisar la carga del UPS que alimentan los equipos, para los casos de corte de energía y determinar el tiempo que queda de energía auxiliar.
3. Llamar a la Oficina de Mantenimiento y Servicios Generales de la UNAP, para identificar si la falla es del sistema general de la empresa de energía eléctrica privada que suministra el fluido eléctrico, o es un problema interno, en el tablero de alimentación del local del Herbarium de la Facultad de Ciencias Biológicas (donde se encuentra la Oficina de Tecnologías de la Información).
4. Por seguridad, utilizar la energía que se tiene en los UPS para apagar los equipos en forma correcta.
5. Si la falla es originada en el sistema general, se debe esperar a que se normalice, para proceder a encender los equipos y levantar los servicios de las aplicaciones informáticas.
6. Si la falla es originada por algún factor interno, deberá, proceder a solicitar la atención correspondiente a la Oficina de Mantenimiento y Servicios Generales de la UNAP, para así, ellos puedan revisar los elementos del tablero del local el Herbarium, como son: Llaves térmicas, cables flojos, o revisar si existe algún equipo que esté ocasionando la falla.

   Si no se detecta localmente, se debe de proceder a revisar las conexiones, en la subestación de donde se está independizando la energía, revisar los bornes flojos u otros.

   Si aún no se detecta la falla, ubicar si están realizando algún trabajo con equipos de alto consumo, como son máquinas soldadoras, etc., y que hayan conectado a la red ocasionando un corto circuito, y que no permita, restituir la energía, en forma normal.
7. Si la falla es localizada, proceder a la reparación, o reemplazo, de los componentes que causaron la falla.

   Una vez reparada la falla se debe de conectar la energía para ver el comportamiento, de ésta, y no encender los equipos de cómputo hasta después de 15 minutos aproximadamente después de la restitución de la energía).

Corriente de emergencia, aquella brindada por grupo electrógeno y/o UPS. **Corriente normal**, la que es otorgada por la compañía eléctrica.
Personal Responsable: − Administrador de servidores y servicios en línea. Personal de Apoyo: − Soporte técnico de software y hardware.
Recursos Necesarios: − UPS. − Luces de emergencia. − Linterna.

A continuación, se presenta una tabla donde se listan las consecuencias de interrupción de fluido eléctrico.

Consecuencia	Áreas Afectadas
Cierre Inapropiado de la Base de Datos.	Todas las áreas
Finalización Incompleta de los Backups.	Todas las áreas
Falla de un componente de equipo Servidor.	Todas las áreas
Pérdida total o parcial de la operatividad de los sistemas informáticos.	Todas las áreas

A-03: Incendio.

Algún incidente involuntario puede ocasionar el inicio de un incendio para lo cual se deberá proceder de la siguiente manera:

1. Si el inicio del incendio se produce en horas de labores, deberá de proceder a dar la alarma a todo el personal de la oficina, colindantes, y a los bomberos.

   Teléfonos:
   - Compañía de bomberos Punchana: 065 – 253566
   - Compañía de bomberos Belén: 065 – 233333

2. Desconectar las fuentes de alimentación eléctricas (No ejecutar este paso si la vida e integridad de alguna persona se ve en riesgo).

3. Se deberá proceder a sofocar el fuego utilizando el extintor correcto para el tipo de fuego (No ejecutar este paso si la vida e integridad de alguna persona se ve en riesgo).

   Tipo:
   - Polvo Químico Seco (PQS)

4. Si la fuente del siniestro está lejos, pero se puede propagar hacia los equipos principales de cómputo (servidores) deberá retirar los equipos hacia un lugar seguro, discos o últimas copias que tenga a la mano (hacer esto si el tiempo lo permite, sin que esto signifique riesgo de exponer la vida).

Personal Responsable:
- Administrador de servidores y servicios en línea.

Personal de Apoyo:
- Todo el personal disponible de la oficina.

Recursos Necesarios:
- Detectores de incendio.
- Extintor de fuego.

A-04: Intrusión en las redes informáticas.

- **Intrusión mediante la red cableada.**

Si la Intrusión se efectuó dentro de las instalaciones del Herbarium:

1. Si fue en horario laboral, solicitarle a la persona su respectiva identificación, proceder a dar conocimiento inmediatamente al personal de seguridad del local del Herbarium
2. En caso de que la intrusión se haya realizado fuera del horario laboral:
   2.a. Revisar los registros del firewall para identificar la fecha y hora de la actividad.
   2.b. Revisar las cámaras de seguridad para conocer la persona que realizó la intrusión.
   2.c. Dar conocimiento al personal de seguridad para evitar el acceso de la persona en otra oportunidad.

Si la Intrusión se efectuó en otro local de la UNAP:

1. La OTI-UNAP, tiene segmentados los números IPs de los locales, por lo que se puede identificar fácilmente la ubicación general de la intrusión.
   1.a. Acceder a los registros del firewall para identificar el punto de red del switch desde donde se originó la intrusión, determinando la fecha y hora de la actividad.
   1.b. Acceder a la grabación de las cámaras para identificar a la persona que realizó la intrusión.
   1.c. Dar conocimiento al personal de seguridad para evitar el acceso de la persona en otra oportunidad.

3. Verificar si hubo pérdida de datos o alteración en algún servidor; de haberlo, realizar un restablecimiento total de los sistemas utilizando un Backup como está establecido en el Manual de Procedimientos.
   Realizar un informe dirigido al jefe de la Oficina de Tecnologías de la Información.

En cualquiera de los casos, el personal de OTI que vela por la seguridad de las redes, debe elaborar un informe detallado al Jefe de OTI; el cual podría iniciar una acción penal al intruso, de ameritar el caso.

- **Intrusión mediante la red inalámbrica.**

  En caso de que un usuario logre acceder a la red LAN de la UNAP, ya sea por obtención y/o crackeo de contraseñas o uso de VPNs para saltar el bloqueo de páginas no autorizadas, se realizan los siguientes pasos:

  1. Monitorear mediante el Firewall PfSense la IP, dirección MAC del intruso o usuario y la VLAN del local desde donde se conectó, proceder a bloquearlo definitivamente de la red.
  2. En caso el atacante ya se encuentre dentro de la red y tenga intenciones de dañar los servicios de los servidores mediante ataques de denegación de servicios (DDoS), el Firewall PfSense será capaz de bloquear ese tipo de ataques y dará un aviso en tiempo real al encargado de dicho Firewall. El encargado deberá realizar el paso uno (1).
  3. En caso el atacante haya logrado entrar a los servidores, el Firewall notificará la intrusión al responsable de la seguridad, quien deberá inmediatamente dejar fuera de la red a los servidores para salvaguardar la información.
     El responsable de la seguridad de las redes deberá notificar a las demás áreas de la UNAP, que los servicios serán interrumpidos temporalmente por fuerza mayor, y que esperen hasta nueva comunicación para acceder a ellos.
  4. En caso la información se haya visto afectada, realizar el restablecimiento total de los sistemas y aplicaciones instalados en los servidores utilizando los Backups de respaldo.
  5. Cambiar los parámetros de seguridad de acceso a los servidores y a las redes (contraseñas de equipos, contraseñas de accesos, puertos).
  6. Superado la intrusión, restablecer el funcionamiento de las redes e informar a las oficinas de la UNAP que los servicios ya están disponibles.

  El personal de OTI que vela por la seguridad de las redes, debe elaborar un informe detallado al Jefe de OTI.

Personal Responsable:
- Administrador de la Red y Seguridad Perimetral.

Personal de Apoyo:
- Personal de Soporte técnico de redes y comunicaciones.

Recursos Necesarios:
- Software Firewall PfSense.
- Software de monitoreo de tráfico de red Zabbix.

- DVR y video cámaras.
- Software de extracción de vídeo del DVR.
- Disco Duro de Backup.

A-05: Daño de componente en los Servidores.

A. <u>Error Físico de Disco de un Servidor (Sin RAID)</u>:

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

1. Ubicar el disco malogrado.
2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y telefonear a los jefes de área.
3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
4. Bajar el sistema y apagar el equipo.
5. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.
6. Restaurar el último Backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
7. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
8. Habilitar las entradas al sistema para los usuarios.

B. <u>Error de Memoria RAM</u>:

En este caso se dan los siguientes síntomas:

- El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
- Ante procesos mayores se congela el proceso.
- Arroja errores con mapas de direcciones hexadecimales.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

1. Avisar a los usuarios que deben salir del sistema informático que le corresponde al servidor, utilizando mensajes por red, asimismo, informar a los jefes de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Identificar los módulos de memorias malogradas.
4. Retirar los módulos de memorias malogradas y reemplazarlas por otras iguales o similares.

5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que, al encender el sistema, los usuarios ingresen.
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Probar los sistemas que están en red en diferentes estaciones.
8. Finalmente, luego de los resultados, habilitar las entradas al sistema para los usuarios.

C. <u>Error Lógico de Datos</u>:

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

- Caída del servidor de archivos por falla de software de red.
- Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
- Bajar incorrectamente el servidor de archivos.
- Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

1. Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos, cargar el sistema operativo de red.
2. Deshabilitar el ingreso de usuarios al sistema.
3. Descargar todos los volúmenes del servidor, a excepción del volumen raíz. De encontrarse este volumen con problemas, se deberá descargarlo también.
4. Cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.
5. Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que índices en la base de datos estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente. Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

Personal Responsable:

- Administrador de servidores y servicios en línea.

Personal de Apoyo:

- personal de Soporte técnico de software y hardware

Recursos Necesarios:

− Disco duro de contingencia. − Memoria RAM de contingencia. − Software de recuperación de archivo. − Disco duro de Backup.

A-06: Caída de Acceso a Internet del proveedor.
En caso de la caída de acceso a internet del proveedor se realizan los siguientes pasos: 1. Se realiza el monitoreo del acceso a internet del proveedor utilizando el software de monitoreo Zabbix, el cual muestra gráficamente una alarma sobre la caída del servicio de las redes WAN provenientes del proveedor de internet en tiempo real. 2. Se prosigue a reportar al representante asignado del proveedor, sobre la caída del servicio de internet, solicitando el inmediato aviso en el momento de la reanudación del servicio. 3. Proceder a dar aviso a los usuarios sobre la caída del acceso a internet del proveedor, de preferencia a los jefes de cada área y decanos de las facultades de la UNAP. 4. Al recibir el aviso sobre la reanudación del servicio de internet por parte del proveedor, se prosigue a informar de la misma a los usuarios, de preferencia jefes de área y decanos de las facultades de la UNAP.
Personal Responsable: − Administrador de la Red y Seguridad Perimetral. Personal de apoyo: − Ninguno.
Recursos Necesarios: − Software de monitoreo de tráfico de red Zabbix.

A-07: Falla de comunicación vía Radio-Enlace entre locales.
En caso de algún fallo de comunicación de fibra oscura: 1. Se realiza el monitoreo de las redes utilizando el software de monitoreo Zabbix, el cual muestra gráficamente una alarma sobre el fallo de comunicación vía fibra oscura, en tiempo real, entre los locales o dependencias de la UNAP, determinando de esa forma, el local específico con el problema de red; así también, se reciben llamadas telefónicas de los usuarios reportando los fallos de comunicación. 2. Se realiza una llamada al encargado del Área de informática o trabajador de cargo superior, con el fin de consultar sobre el estado del fluido eléctrico de su dependencia o facultad, para descartar un desperfecto o desconfiguración de los dispositivos de red. 3. Si el fluido eléctrico se encuentra estable, se asigna al personal de Soporte Técnico de redes y comunicaciones para la visita al local o dependencia con la falla de comunicación y verifica si el gabinete de comunicaciones se encuentra conectado a la fuente de energía establecido y si los dispositivos se encuentran encendidos. 4. El soporte técnico de redes y comunicaciones verifica la correcta conexión medianta la fibra oscura entre las oficinas y facultades. 5. Si la falla continua, se procede a buscar e identificar algún desperfecto en los dispositivos de red de dicha dependencia o facultad, una vez encontrado el dispositivo dañado, se procede a realizar un informe técnico detallado a la máxima instancia de dicho local, recomendando la adquisición y cambio del dispositivo con el desperfecto. 6. Una vez adquirido el dispositivo, la dependencia lo notificará a la Oficina de Tecnologías de la Información. 7. El soporte técnico de redes y comunicaciones realiza (de ser necesaria) la configuración y posterior instalación del dispositivo nuevo. 8. Se realiza la comprobación de la correcta comunicación vía radio-enlace, ingresando al software de monitoreo Zabbix y viendo si la alerta de error desapareció.
Personal Responsable: − Administrador de la Red y Seguridad Perimetral. Personal de apoyo: − Soporte técnico de redes y comunicaciones.
Recursos Necesarios: − Software de monitoreo de tráfico de red Zabbix.

XIV. ANEXOS:

A. Equipos y dispositivos con los que cuenta la Oficina Central de Informática.

Dispositivo	Marca	Modelo	N° Serie
Servidor	DELL	----------	5135
Servidor	DELL	----------	5136
Servidor Backup	iomage	Iomega NAS 435r 640GB	W9BAF090034
Servidor Backup	iomage	Iomega NAS 435r 640GB	W9BF520024
Servidor	IBM	System X3500 M2	KQTLLWL
Servidor	IBM	System X3500 M2	KQTLLWT
Servidor	IBM	System X3500 M2	KQTLLWR
Servidor	IBM	System X3500 M2	KQTLLWZ
Servidor	IBM	System X3500 M2	KQXRM93
Servidor	IBM	System X3500 M2	KQTLLWY
Servidor	advance	advance SERVER	ECPP5080547
Switch 7700	3Com	3C16852	9FFF590000012
Switch	3Com	3C10202	TBG9533722D5F8
Switch	3Com	3892D190	VLNCB4F40585C1
Switch	3Com	3226	0200/7G1F5AD15B260
Monitor	advance	ET-0025-TA	740881870277
Monitor	advance	ET-0025-TA	740881870313
Monitor	LG	StudioWorks 700E	403DIVWP2399
Monitor	IBM	Raqueable	172317X23CR812
Monitor	IBM	Raqueable	172317X23CR814
Monitor	IBM	E74	55-VWK90
Monitor	COMPAQ	V500	908BF28RQ155
UPS Chico	PCM	SMK-1000A	10044460504
Teclado	advance	5137AU	740895001664
Teclado	advance	9000A	740895001179
Teclado	advance	2001	740895000794
Teclado	IBM	SK - 8809	2063542
Teclado	advance	2001	740895000977
Acces Point	3Com	WL - 525	0102/M3BA66EADA7D9
Console Switch	IBM	----------	23HH056
Computador	advance	OPEN-6657TEM	74089950-1623
Computador	advance	OPEN-6657TEM	74089950-1630
2 Gabinete	SATRA	Gabinete de Pared	S/N
3 Gabinete	SATRA	Gabinete de Piso	S/N
Gabinete	IBM	Gabinete de Piso	S/N
Switch	3Com	4226	LY1V48B578720
Switch	3Com	3226	0200/7G1F5AD1595E0
Switch	3Com	3226	0200/7GF15NDD47B60

B. Procedimiento de crear y restaurar Backups de los sistemas informáticos.

F10-P01:

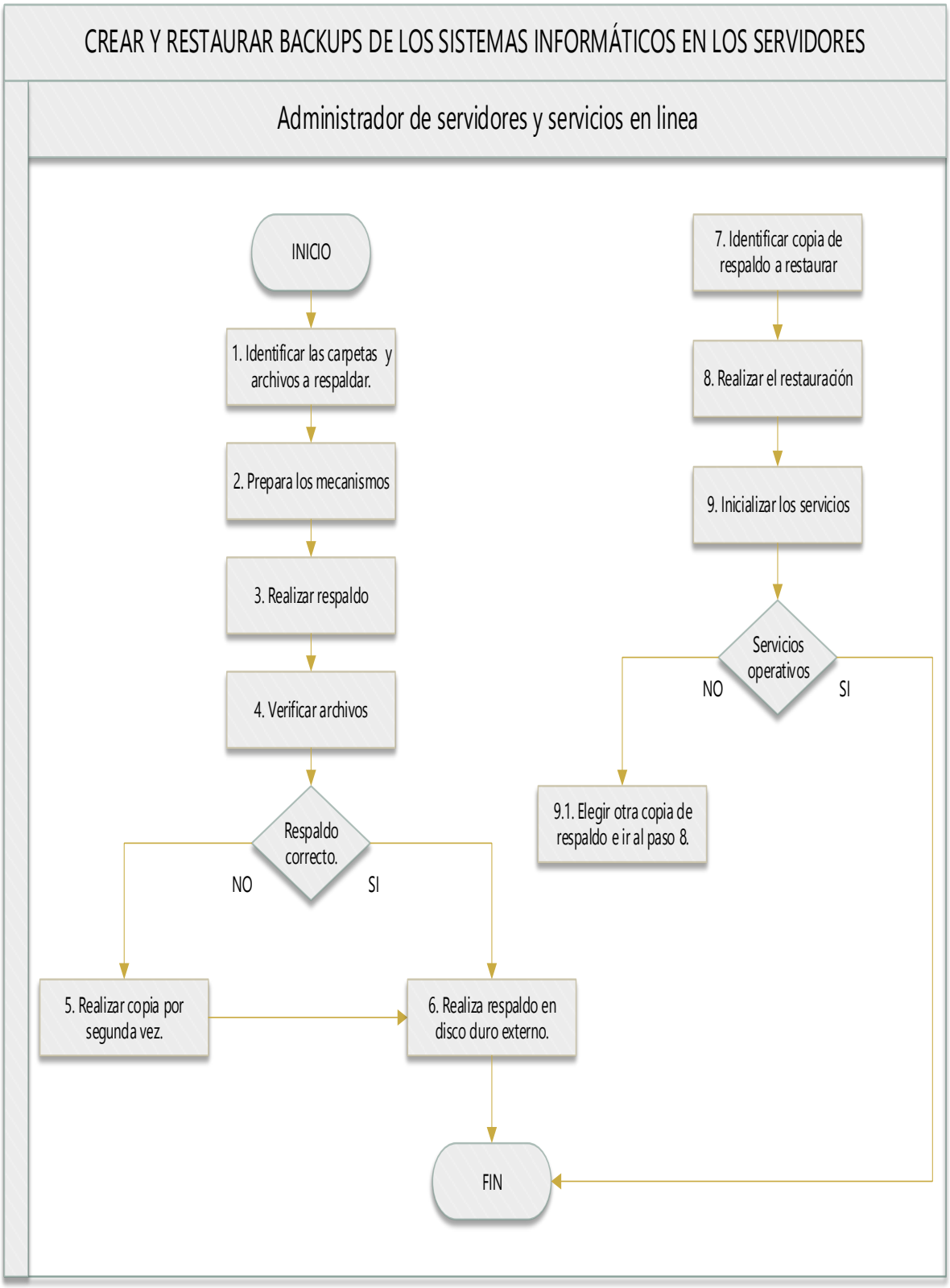
	UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA **OFICINA CENTRAL DE INFORMÁTICA**
F10-P01: CREAR Y RESTAURAR BACKUPS DE LOS SISTEMAS INFORMÁTICOS EN LOS SERVIDORES	
Oficina Responsable del Proceso:	Oficina de Tecnologías de la Información.
Objetivo	Proteger la información, base de datos y documentación crítica para la entidad con el fin que se conserven respaldos, así como la restauración de la misma en el momento que se necesite.

Políticas del Proceso

1. La copia de respaldo de información se realiza en disco (almacenamiento en servidor) y en disco duro externo de uso exclusivo para la realización del Backup.
2. El respaldo se realiza fuera del horario de trabajo y de manera diaria, semanal y mensual.
3. Las copias de respaldo se almacenan con el nombre respectivo a la aplicación y la fecha en la que se realizó dicho respaldo.
4. En el caso que no se puedan hacer las copias de respaldo por algún problema con el servidor se procede a realizarlos lo más pronto posible siempre y cuando no interrumpa el normal desempeño del servidor.

Código:	Revisión:	Fecha:	Elaborado por:
F10-P01	Marcos Tomy Calderon Diaz	Nov. - 2019	Jose Hernan Rios Pinedo.

- DIAGRAMA DE FLUJO DEL PROCEDIMIENTO: CREAR Y RESTAURAR BACKUPS DE LOS SISTEMAS INFORMÁTICOS EN LOS SERVIDORES.



- SECUENCIA DEL PROCEDIMIENTO: CREAR Y RESTAURAR BACKUPS DE LOS SISTEMAS INFORMÁTICOS EN LOS SERVIDORES.

Secuencia	Actividad	Responsable
1. Identificar las carpetas y archivos a respaldar.	El administrador de servidores y servicios en línea identifica y selecciona las carpetas y archivos a respaldar de los diferentes sistemas y aplicaciones alojados en los servidores del Data Center.	El administrador de servidores y servicios en línea
2. Prepara los mecanismos.	El administrador de servidores y servicios en línea cuenta con un servidor exclusivo para Backups, en donde se instala, previamente, el sistema operativo Freenas, en el cual se realiza una configuración para uso compartido de carpetas dentro de la red local, además, instala y configura el software FreeFileSync para la posterior verificación de los archivos y carpetas copiadas.	El administrador de servidores y servicios en línea
3. Realizar copias de respaldo.	El administrador de servidores y servicios en línea realiza el respaldo copiando los archivos y carpetas correspondientes de los sistemas con la información alojada en los servidores utilizando el uso compartido de las carpetas brindado por Freenas.	El administrador de servidores y servicios en línea
4. Verificar archivos	El administrador de servidores y servicios en línea realiza una verificación utilizando el software FreeFileSync, previamente instalado y configurado, para realizar una comparación entre los archivos y carpetas alojados en los servidores y los archivos copiados en los discos duros para Backups.	El administrador de servidores y servicios en línea
5. Realizar copia por segunda vez.	Si al comparar los archivos y carpetas se puede notar la falta de alguno de estos, se realiza un segundo proceso de respaldo de dichos archivos y carpetas.	El administrador de servidores y servicios en línea
6. Realizar copia de respaldo en disco duro externo.	El administrador de servidores y servicios en línea realiza el respaldo de los archivos y carpetas de los diferentes sistemas alojados en los servidores del Data Center almacenándolos en un disco duro extraíble de uso estrictamente para la realización de Backups.	El administrador de servidores y servicios en línea
7. Identificar copia de respaldo a restaurar.	Identificar y seleccionar la copia de respaldo a restaurar más cercana a la fecha de restauración.	El administrador de servidores y servicios en línea
8. Realizar la restauración.	Se realiza la restauración de la copia de respaldo a la carpeta respectiva en el servidor reemplazando todos los archivos involucrados en la transferencia de los datos.	El administrador de servidores y servicios en línea
9. Inicializar los servicios.	Inicializar los servicios respectivos y verificar que sea realice de manera adecuada.	El administrador de servidores y servicios en línea
9.1. Elegir otra copia de respaldo y regresar.	Si los servicios no se inician adecuadamente, se debe elegir la siguiente copia de respaldo más cercana a la restauración y nuevamente 8. Realizar la restauración.	El administrador de servidores y servicios en línea

C. Lista de contactos ante un desastre.

Al materializarse una amenaza, las personas que se deberán ubicar son las siguientes:

Caso	Cargo	Nombre de la Persona	Teléfono
A-01	Administrador de servidores y servicios en línea.	Jose Hernan Rios Pinedo.	942618390
A-02	Administrador de servidores y servicios en línea.	Jose Hernan Rios Pinedo.	942618390
A-03	Administrador de servidores y servicios en línea.	Jose Hernan Rios Pinedo.	942618390
A-04	Administrador de la Red y Seguridad Perimetral.	Jose Hernan Rios Pinedo.	942618390
A-05	Administrador de servidores y servicios en línea.	Jose Hernan Rios Pinedo.	942618390
A-06	Administrador de la Red y Seguridad Perimetral.	Jose Hernan Rios Pinedo.	942618390
	Jefa de la Oficina Central de Servicios Generales y Transporte.	Dolores Pinedo Rengifo.	957-619520
A-07	Administrador de la Red y Seguridad Perimetral.	Jose Hernan Rios Pinedo.	942618390