UNIVERSIDAD NACIONAL DE EDUCACIÓN
Enrique Guzmán y Valle
"Alma Máter del Magisterio Nacional"

RECTORADO

RESOLUCIÓN N° 2356-2017-R-UNE

Chosica, 01 de agosto del 2017

VISTO el Oficio N° 225-2017-DCPyDI-UNE, del 21 de julio del 2017, de la Dirección Central de Planificación y Desarrollo Institucional de la Universidad Nacional de Educación Enrique Guzmán y Valle.

CONSIDERANDO:

Que mediante el Oficio N° 067-2017-ORC-OI, del 16 de mayo del 2017, el Jefe de la Oficina de Redes y Comunicaciones, y la Directora de la Oficina de Informática remiten al Jefe de la Oficina de Organización y Procesos la documentación correspondiente, en relación al Plan de Contingencias y Recuperación de Desastres de la Universidad Nacional de Educación Enrique Guzmán y Valle, para que se efectivice el trámite respectivo;

Que el referido plan tiene como objetivo restablecer y/o recobrar el servicio informático en caso de presentarse una emergencia que interrumpa la operatividad de los sistemas informáticos, ante algún desastre ocurrido en el Centro de Informática, ocasionado por fallas en la plataforma informática (infraestructura de red, servidores, PCs, dispositivos de comunicación, y software de aplicaciones) o algún desastre natural;

Que con Oficio N° 311-2017-OOyP/DCPyDI-UNE, del 20 de julio del 2017, el Jefe de la Oficina de Organización y Procesos, conforme a lo coordinado con las áreas pertinentes, remite el referido expediente, a fin de que se efectúe lo que corresponda;

Que mediante el documento del visto, el Director de Planificación y Desarrollo Institucional eleva al Rector todo lo actuado, para su aprobación;

Estando a lo dispuesto por la autoridad universitaria; y,

En uso de las atribuciones conferidas por los artículos 59° y 60° de la Ley N° 30220 - Ley Universitaria, concordante con los artículos 19°, 20° y 23° del Estatuto de la UNE y los alcances de la Resolución N° 1518-2016-R-UNE, con cargo a dar cuenta al Consejo Universitario;

SE RESUELVE:

ARTÍCULO 1°.- APROBAR el PLAN DE CONTINGENCIAS Y RECUPERACIÓN DE DESASTRES DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE, suscrito por el área legal, la Oficina de Informática y las áreas técnicas correspondientes, conforme se detalla en el anexo que consta de cuarenta y uno (41) folios.

ARTÍCULO 2°.- DISPONER que las dependencias correspondientes se encarguen de dar cumplimiento a lo dispuesto en la presente resolución y garanticen su implementación.

Regístrese, comuníquese y cúmplase.

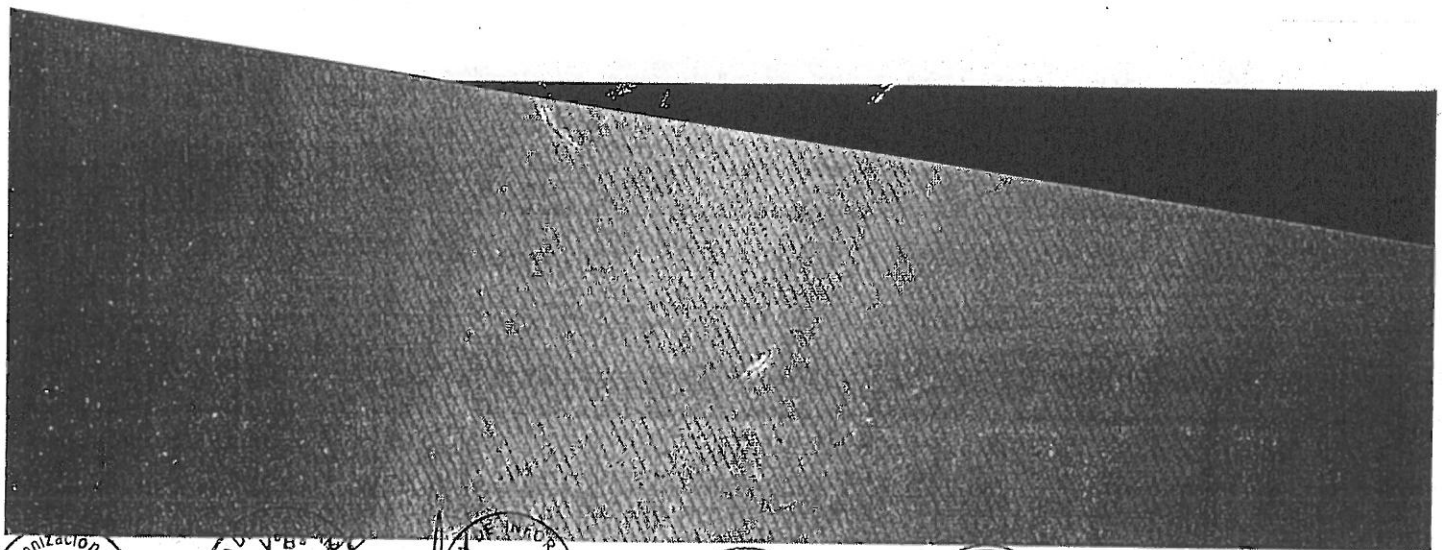
Lic. Anita Luz Chacón Ayala
Secretaria General (e)

Dr. Luis Alberto Rodríguez De Los Ríos
Rector

AMST/ESPJ

UNIVERSIDAD NACIONAL DE EDUCACIÓN
ENRIQUE GUZMÁN Y VALLE
ALMA MÁTER DEL MAGISTERIO NACIONAL
OFICINA DE INFORMÁTICA

PLAN DE CONTINGENCIAS Y RECUPERACIÓN DE DESASTRES



Of. de Organización y Procesos
OFICINA DE ASESORÍA LEGAL
V°B°
OFICINA DE INFORMÁTICA - UNE -
SECRETARÍA GENERAL
Dirección de Educación

PLAN DE CONTINGENCIAS Y RECUPERACIÓN DE DESASTRES

INTRODUCCIÓN

El Plan de Contingencias y Recuperación de Desastres es el documento que contiene los procedimientos y/o actividades para la toma de decisiones en caso que ocurra una emergencia que interrumpa la operatividad de los sistemas informáticos. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para proteger y salvaguardar la integridad y seguridad de la información que maneja el Centro de Informática, en relación con contingencias producidas en los servidores de base de datos, los equipos de comunicación de datos y enlaces de comunicación, el software de aplicaciones y los datos, y garantizar su continuidad en las operaciones.

Pese a todas nuestras medidas de seguridad puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres, el cual tendrá como objetivo restaurar el Servicio de Cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre en el área Informática, considerando todas las áreas de los usuarios que procesan información por medio de la computadora.

Este Plan de Desastres está estructurado de forma sencilla para facilitar una rápida comprensión de sus contenidos y facilitar su uso en caso de ocurrir cualquier desastre que afecte a la disponibilidad de sus sistemas de información. Al tratarse de un documento "dinámico", cualquier cambio en los procedimientos, activos o políticas de la organización deberá quedar reflejado dentro del mismo y ser tenido en cuenta.

Como instrumento de gestión, apoya en el buen manejo de las Tecnologías de la Información y Comunicación (TIC).

El plan de contingencias y recuperación de desastres es revisado/evaluado cuando se materializa u ocurre una amenaza.

I. OBJETIVO

Restablecer y/o recobrar el servicio informático en caso de presentarse contingencias graves y recuperación de la información ante algún desastre ocurrido en el Centro de Informática, ocasionados por fallas de la plataforma informática (infraestructura de red, servidores, PCs, dispositivos de comunicación, y software de aplicaciones) o algún desastre natural.

II. ALCANCE

El presente documento es de aplicación y cumplimiento obligatorio del personal que labora en la Oficina de Informática y otras dependencias administrativas que están en relación directa con la gestión financiera, contable y presupuestal de la Institución.

III. RESPONSABILIDAD

El Director del Centro de Informática es el responsable de la implementación de este dispositivo.

El Personal encargado de la Oficina de Informática es el responsable de supervisar y coordinar las acciones para que se procesen y remitan los respaldos, y que llegan a los sitios externos de respaldo, y de tomar las medidas y acciones de recuperación o restauración del servicio.

Los usuarios y operadores de las dependencias de la Oficina de Informática son los responsables de ejecutar los procedimientos en los cuales estén involucrados para superar las contingencias detalladas en el presente procedimiento.

IV. VIGENCIA

El Plan de contingencias y recuperación de desastres entrará en vigencia al día siguiente de su aprobación mediante Resolución Rectoral.

V. BASE LEGAL

a. Constitución Política.
b. Ley N° 30220. Ley Universitaria.
c. Resolución Nº 009-2016-AU-UNE, que modifica el Estatuto de la Universidad Nacional de Educación Enrique Guzmán y Valle.

d. Resolución N° 2663-2016-R-UNE. Reglamento General de la Universidad Nacional de Educación Enrique Guzmán y Valle.
e. Ley N° 27444, Ley del Procedimiento Administrativo General y establece la publicación de diversos dispositivos legales en el portal del Estado peruano y en portales Institucionales.
f. Decreto Legislativo N° 1246, que aprueba diversas medidas de simplificación administrativa.
g. Directiva Nº 008-95-INEI/SJI. Recomendaciones Técnicas para la Protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Pública.
h. Directiva Nº 010-95-INEI/SJI. Recomendaciones Técnicas para la Organización y Gestión de los Servicios Informáticos para la Administración Pública.
i. Directiva Nº 016-2002-INEI/DTNP. Normas Técnicas para el Almacenamiento y Respaldo de la Información Procesada por las Entidades de la Administración Pública.
j. R.D. Nº 320-2006-CG. Aprueba Normas de Control Interno.

VI. REFERENCIAS

- Guía Teórico-Práctica para la Elaboración de Planes Estratégicos de Tecnologías de Información – Abril, 2002.
- Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información. INEI, febrero, 2001.

VII. MEDIDAS

El Plan de Contingencias contempla la aplicación de tres tipos de medidas:

- **Medidas preventivas:** cuyo objeto es disminuir la probabilidad de que el fallo llegue a producirse (pruebas y revisiones constantes).
- **Medidas alternativas o de respaldo:** orientadas al mantenimiento de la actividad una vez sucedido el fallo, bien sustituyendo el componente que falla o prescindiendo del mismo.
- **Medidas correctivas:** orientadas a la corrección del fallo y recuperación de la operatividad del componente fallido.

Plan de Recuperación de Desastres se pueden clasificar en tres etapas:

- Actividades previas al desastre.
- Actividades durante el desastre.
- Actividades después del desastre.

VIII. POLÍTICAS DE GOBIERNO

Respecto de las políticas y actividades iniciales, en el Plan de Contingencias y Recuperación de Desastres se deben considerar los siguientes aspectos:

- **Apoyo de la Alta Dirección**

  No se podrá conseguir el éxito del Plan de Contingencias y Recuperación de Desastres, si la Alta Dirección no conoce la necesidad de estos en la Institución, ni apoyan su desarrollo y su ejecución.

- **Apoyo de los Usuarios**

  No se podrá conseguir el éxito total del Plan de Contingencias y Recuperación de Desastres, si los usuarios no colaboran en el desarrollo y aplicación del mismo.

IX. ANÁLISIS DE RIESGO

Identificar aquellos elementos de la Institución o funciones que puedan ser críticos ante cualquier eventualidad o desastre y jerarquizarlos por orden de importancia dentro de la Institución.

PLAN DE CONTINGENCIAS

El plan de contingencia es una herramienta que ayudará a que los procesos críticos de la Universidad continúen funcionando a pesar de una posible falla en los sistemas computarizados.

Clasificación de los recursos informáticos en orden crítico:

Definir un sistema de clasificación de los recursos informáticos para determinar la criticidad de los recursos.

En lo fundamental, el análisis de riesgos que se llevará a cabo ha de contestar, con la mayor fiabilidad posible, a las siguientes preguntas:

- ¿Cuánto puede operar un área sin los sistemas?
- ¿Cuál es el riesgo y/o pérdida económica?
- ¿Existe impacto en la imagen de la Institución?
- ¿Se puede perder registros y/o datos vitales como resultado de la discontinuidad de los recursos?
- ¿Existen alternativas de procesamiento ante una falla?

Los recursos informáticos pueden ser clasificados de la siguiente forma:

1. **Hardware**
   - Computadoras de escritorio
   - Portátiles
   - Servidores
   - Impresoras de escritorio
     - Impresoras Servicios Generales
     - Bienestar Universitario
     - Informática
   - de red
2. **Software**
   - Base de datos
   - Aplicaciones locales
   - Aplicaciones integradas
   - Aplicaciones Web
3. **Comunicaciones**
   - Dispositivos para la comunicación local
     - Switches
     - Access Point

- Dispositivos para la comunicación remota
  - Modems
  - Routers
  - UTM

4. **Infraestructura de red**
   - Cableado
   - Fibra óptica
   - Red Inalámbrica
   - Pozos de tierra
5. **Servicios**
   - Central telefónica IP
   - Telefonía Móvil
   - Conexión de Internet
   - Servicios de Red

Niveles de Severidad:

Se definen los siguientes niveles de severidad:

1. **Nivel 4: Crítica**

   Aplicaciones o actividades extremadamente críticas o vitales para la continuidad de la Institución. Estos son recursos informáticos que deben estar disponibles para que la organización sea viable.

2. **Nivel 3: Moderada**

   Actividades o aplicaciones importantes que deben ser recuperadas dentro un periodo razonable de tiempo para mejorar el nivel de las operaciones.

3. **Nivel 2: Baja**

   Funciones que pueden ser excluidas de la lista de criticidad, que podrían ser convenientes para la eficiencia en las operaciones.

4. **Nivel 1: No importante o trivial**

   Recursos que pueden ser excluidos del plan, pues no afectan a las operaciones de la Institución.

Of. de Organización y Procesos - UNE - V°B° OFICINA DE ASESORÍA LEGAL - UNE - V°B° OFICINA DE INFORMÁTICA - UNE - SECRETARÍA GENERAL - UNE - (e) Univ. Nac. de Educ. E. G. Valdivia - RECTOR

Tipos de Riesgos:

Riesgo	Probabilidad del Factor de Riesgo				
	Muy bajo	Bajo	Medio	Alto	Muy Alto
Fallas en los equipos				X	
Fallas en las aplicaciones		X			
Alteración de información	X				
Accesos no autorizados	X				
Virus			X		
Robo (común y de datos)	X				
Incendio				X	
Fallas en la red eléctrica			X		
Fallas en la red LAN - WAN		X			

X. GESTIÓN DEL RIESGO

Realizar un plan de continuidad compuesto a su vez de un conjunto de planes para cada una de las áreas críticas. Cada plan describirá los recursos, papeles de personal, procedimientos y tiempo o fechas para la implantación.

Se podrán llevar a cabo las siguientes acciones con el objeto de minimizar los riesgos:

Minimización del Riesgo:

1. Realizar copias de respaldo o backups de la información.
2. Fortalecer la seguridad física de las instalaciones.
3. Fortalecer el control de acceso.
4. Identificar documentos de seguros y contratos.
5. Revisar procedimientos de personal y de control.

6. Seguridad de la infraestructura informática.
7. Definir acuerdos de continuidad con clientes y proveedores.
8. Utilizar servicios de *outsourcing*.
9. Desarrollo de opciones preventivas y de planeación
10. Capacitación.
11. Servicios generals.
12. Renta de equipos de respaldo.

Procedimientos de backups:

En relación con los procedimientos para la realización de las copias de respaldo o backups se tomará en cuenta lo siguiente:

- Periodicidad de cada tipo de backup:
  a. Base de Datos Oracle 11G (Administrativa y Académica): Diario.
  b. Correo Electrónico Exchange 2013: Semanal.
  c. Directorio Activo: Semanal.
  d. Aula Virtual: Mensual.
  e. Servidor WEB Principal: Semanal.
  f. File Server: Diario.
  g. Central Telefónica DENWA IPBX: Semanal.
  h. UTM Cyberoam: Semanal.
  i. SIAF: Diario.
  j. Otros sistemas: semanal, mensual, anual, a demanda.
- Almacenamiento de los backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- Reemplazo de los Backups, en forma periódica, antes de que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).
- Pruebas periódicas de los Backups (Restore), verificando su funcionalidad.
- Una copia de los backups de la Base de Datos Oracle y SIAF seran guardados en un medio de almacenamiento digital que se encuentra fuera de las instalaciones del Centro de Informática (Escuela de Posgrado – La Molina).

Directivas generales para el adecuado uso de los sistemas y equipos:

1. Salir de las aplicaciones en casos de ausentarse por periodos largos.
2. Apagar los equipos al final de la jornada de trabajo.
3. No crear recursos compartidos en las PCs, salvo que fuera estrictamente necesario por cuestiones de una mejor gestión de la oficina, en cuyo caso, los recursos compartidos deberán ser accesibles solo a usuarios autorizados.
4. Uso de contraseñas "fuertes" (8 caracteres como mínimo, con al menos 1 dígito y 1 signo de puntuación y no tener los nombres, ni apellidos, ni la fecha de nacimiento del usuario).
5. Si fuera empleo de bloqueos de pantalla para el caso de inactividad de la PC por un periodo de tiempo.
6. No abrir mensajes de correo cuya procedencia sea dudosa, no conocida y/o no solicitada.

Directivas generales para el cuidado de los equipos:

1. En las oficinas no deben existir materiales que sean altamente inflamables y que despidan humos sumamente tóxicos.
2. Promover paredes que queden perfectamente selladas y no despidan polvo.
3. Mantener los partes externas de los equipos libres de polvo.
4. Evitar la luz solar directa sobre los equipos.
5. Planificar mantenimientos preventivos programados.

Directivas generales para la prevención del robo:

1. Mantener los servidores, los switches, los UPS y los equipos adicionales tras elementos que limiten el acceso a los mismos y brinden seguridad física del caso.
2. Mantener las PC clientes dentro de ambientes que tengan elementos de seguridad física como puertas, chapas, rejas.
3. A nivel del personal de seguridad de la Institución, promover personal competente, de calidad profesional y que conozca de procedimientos de seguridad.
4. Promover equipos de personas que establezcan y comprueben las técnicas y procedimientos de seguridad.

5. Ejecutar un análisis de riesgo por pérdidas potenciales por delitos intencionados como el robo.
6. Si necesario, elaborar una lista de datos y/o aplicaciones susceptibles de robo por su valor en el mercado ó por su demanda en el mismo; asimismo, establecer los mecanismos de protección correspondientes.

Directivas generales para el adecuado uso del software antivirus:

1. Instalar solo software antivirus con licencia cuya tiempo de vigencia sea de 1 año ó mas.
2. Llevar registro de la fecha de instalación o de caducidad del software antivirus.
3. Permitir que el software del antivirus realice la actualización de su registro de virus, lo cual sucede normalmente al momento de prender el equipo al inicio de la jornada de trabajo.
4. Reportar al responsable del Centro de Informática mensajes de "Antivirus desactivado", "El servicio de antivirus se encuentra desactivado", "Licencia de antivirus vencida", "Periodo de validez de la licencia expirado", "Usuario o contraseña inválidos", "User and password invalid", etc. para que se tomen las acciones del caso.

XI. PROBLEMAS Y TIPO DE SOLUCIÓN

1. Inoperatividad irrecuperable del Servidor de Archivos:

- **Reconocimiento:**
  - No se puede interactuar con las aplicaciones del servidor.
  - No se puede acceder a la consola del servidor.
  - Posibles mensajes de "crash" en la consola del servidor.
  - El servidor se reinicia en forma aleatoria.
  - Mensajes de error de E/S en la consola del servidor.
  - Mensajes de error en el disco en la consola del servidor.
  - Mal funcionamiento del S.O. de red.
- **Severidad:** Crítica
- **Posibilidad de ocurrencia:** Baja
- **Rol(es):** Responsable del Centro de Informática

- **Recursos:**
  - Instalador del SO de la red.
  - Instalador de las aplicaciones o sistemas de software.
  - Última copia de seguridad de los datos.
  - Servidor de contingencias (una PC alternativa para la función de servidor), con el SO de red pre-instalado.
- **Acciones:**
  - Instalación del SO de la red en la PC alternativa (si fuera necesario).
  - Configuración de opciones de red y direcciones IP.
  - Configuración de recursos compartidos.
  - Configuración de grupos de usuarios y usuarios.
  - Instalación de las aplicaciones.
  - Restauración de los datos.
  - Pruebas
  - Luz verde.
  - El responsable del Centro de Informática, solicita al proveedor del fabricante la reparación del servidor dañado, dependiendo de si el equipo servidor está dentro de los límites o no de la garantía respectiva.

2. Inoperatividad del Servidor causada por daño en la tarjeta de red:

- **Reconocimiento:**
  - No se puede interactuar con las aplicaciones del servidor.
  - Mensaje de pérdida de conexión con el servidor.
  - Mensaje de que los recursos compartidos en el servidor no están disponibles.
  - Ping desde el servidor a cualquier otra PC no responde.
  - Diagnósticos de operatividad de la tarjeta de red negativos.
- **Severidad:** Crítica
- **Posibilidad de ocurrencia:** Baja

- **Rol(es):** Responsable del Centro de Informática
- **Recursos:**
  - Tarjeta de red (redundante ya instalada).
  - Tarjeta de red.
  - Instalador (driver) de la tarjeta de red.
- **Acciones:**
  - Reconfiguración de la tarjeta de red redundante.
  - Pruebas.
  - Posteriormente:
    - Instalación de la tarjeta de red.
    - Configuración de la tarjeta de red.
    - Pruebas.
    - Reconfiguración de la tarjeta de red redundante (estado de stand by).
  - Luz verde.

3. **Inoperatividad del Servidor causada por daño severo en el disco duro**

- **Reconocimiento:**
  - Mensajes de error de volumen en la consola del servidor.
  - Mensajes de error de E/S en la consola del servidor.
  - Mensajes de error en el disco en la consola del servidor.
- **Severidad:** Crítica
- **Posibilidad de ocurrencia:** Baja
  - **Rol(es):** Responsable del Centro de Informática
- **Recursos:**
  - Instalador del SO de la red.
  - Instalador de las aplicaciones o sistemas de software.
  - Última copia de seguridad de los datos.
  - Disco duro alternativo de la misma tecnología que el disco duro dañado de repuesto, el mismo que está en estado de stand-by.

- **Acciones:**
  - Retiro del disco duro dañado e instalación del disco duro de repuesto.
  - Instalación del SO de la red.
  - Configuración de opciones de red y direcciones IP.
  - Configuración de recursos compartidos.
  - Configuración de grupos de usuarios y usuarios.
  - Instalación de las aplicaciones.
  - Restauración de los datos.
  - Pruebas.
  - Luz verde
  - Pruebas.

4. **Corrupción de tablas en el SIAF**

- **Reconocimiento:**
  - Mensajes de tabla "xxx" dañada al estar realizando alguna de la siguientes tareas en el SIAF:
    - Transmisión de información entre SIAF-DIGA (UNE) y MEF (Lima)
- **Severidad:** Moderada
- **Posibilidad de ocurrencia:** Baja
- **Rol(es):**
  - Responsable de la Oficina de Informática
  - Responsable del SIAF
- **Recursos:**
  - Utilitarios de la propia aplicación.
- **Acciones:**
  - Cerrar todas las tablas de la BD que pudieran haber quedado abiertas, a través de la consola del servidor.
  - Si es requerido, cerrar todas las sesiones que estén conectadas con la BD, a través de la consola del servidor.
  - Realizar copia de seguridad de los datos.

- Ejecutar el utilitario de la aplicación.
- Pruebas.
- Luz verde

5. Duplicidad de índices en las tablas del SIAF

- **Reconocimiento:**
  - Mensajes de "violación de unicidad de clave" en la tabla "xxx" al estar realizando alguna de la siguientes tareas en el SIAF:
    - Transmisión de información entre SIAF-UNE y MEF
    - Contabilizaciones
- **Severidad:** Moderada
- **Posibilidad de ocurrencia:** Baja
- **Rol(es):**
  - Responsable del Centro de Informática
  - Responsable del SIAF
- **Recursos:**
  - Utilitarios de la propia aplicación.
- **Acciones:**
  - Cerrar todas las tablas de la BD que pudieran haber quedado abiertas, a través de la consola del servidor.
  - Si requerido, cerrar todas las sesiones que estén conectadas con la BD, a través de la consola del servidor.
  - Realizar copia de seguridad de los datos.
  - Editar el archivo de texto y solamente tipear lo siguiente:

    nombre_de_la_tabla.DBF
  - Ejecutar el utilitario de la aplicación.
  - Pruebas.
  - Luz verde

6. **Inoperatividad de una PC o Estación cliente**

- **Reconocimiento:**
  - Diferentes mensajes o señales del mal funcionamiento de la PC o estación cliente.
- **Severidad:** Moderada
- **Posibilidad de ocurrencia:** Baja a mediana
- **Rol(es):**
  - Responsable del Centro de Informática
  - Personal autorizado de apoyo
- **Recursos:**
  - Software utilitario de diagnóstico.
- **Acciones:**
  - Diagnóstico.
  - Se puede ejecutar acciones tales como:
    1. Recuperar la información propia del usuario si es posible y si es necesaria.
    2. Reinstalar o instalar el software dañado.
  - Otras acciones a ejecutar podrían ser:
    - Reparar, cambiar las partes dañadas si es posible o solicitar la reparación y/o mantenimiento a través de terceros, llevando a cabo la solicitud correspondiente a la Unidad de Soporte Técnico.
  - Hacer recomendaciones del caso si fuera necesario.

7. **Interrupción general repentina del suministro de energía eléctrica que afecte directamente al servidor y eventualmente a los switches de borde**

- **Reconocimiento:**
  - Sonido de alerta emitido por los UPS que protegen a los servidores.
- **Severidad:** Moderada a crítica
- **Posibilidad de ocurrencia:** Baja

- **Rol(es):**
  - Responsable del Centro de Informática
  - Oficina de Redes y Comunicaciones
  - Oficina de Infraestructura
  - Personal autorizado
  - Usuarios
- **Recursos:**
  - UPS.
- **Acciones:**
  - En el servidor cerrar todas las tablas de las BDs que pudieran haber quedado abiertas.
  - En el servidor cerrar todas las conexiones.
  - Proceder al apagado normal de los servidores.
  - Proceder al apagado de los switches de red.
  - Proceder al apagado del UPS.
  - Coordinar con la Oficina de Infraestructura sobre la solución de la falta de energía eléctrica y si es necesario lleve a cabo las gestiones correspondientes con el proveedor local de la energía eléctrica.
  - Esperar al retorno de la energía eléctrica.
  - Encender primero el UPS.
  - Encender los switches de red.
  - Encender los servidores.
  - Pruebas.
  - Luz verde

8. **Interrupción de la transmisión de la información entre el SIAF-DIGA y el MEF**

- **Reconocimiento:**
  - Mensajes de error de transmisión de datos entre el SIAF-UNE y el MEF.

- Mensajes de que no se encontró el servidor del MEF o no se pudo validar el usuario.

- **Severidad:** Moderado a Crítico
- **Posibilidad de ocurrencia:** Baja
- **Rol(es):**
  - Responsable del Centro de Informática
  - Responsable del SIAF
- **Recursos:**
  - Canal de comunicación a través de Internet.
  - Línea telefónica directa en la Oficina del SIAF-UNE no compartida.
- **Acciones:**
  - Acceder a la configuración de la transmisión de datos del SIAF.
  - Pruebas de transmission de datos hacial el MEF.
  - Si a pesar de estas acciones la comunicación no se restableciera, llevar a cabo las coordinaciones del caso con la Responsable del SIAF y el Centro de Informática. También se deberá evaluar la posibilidad de que los canales de comunicación del proveedor de servicio de telefonía y de Internet local se hubiera "caído"; en este caso, si es posible, se realizarán las coordinaciones con este proveedor y se deberá esperar hasta que el servicio del proveedor de telefonía e Internet se restablezca.
  - Pruebas.
  - Luz verde

9. Ralentización de la transmisión de la información entre el SIAF-UNE y el MEF

- **Reconocimiento:**
  - Tiempos de transmisión de datos excesivamente largos entre el SIAF-UNE y el MEF.
- **Severidad:** Moderado a Crítico
- **Posibilidad de ocurrencia:** Baja

- **Rol(es):**
  - Responsable del Centro de Informática
  - Responsable del SIAF
- **Recursos:**
  - Canal de comunicación a través de Internet.
  - Línea telefónica directa en la Oficina del SIAF-UNE no compartida.
- **Acciones:**
  - Acceder a la configuración de la transmisión de datos del SIAF.
  - Pruebas.
  - Luz verde

10. Ralentización o intermitencia de la interacción entre los usuarios y las aplicaciones

- **Reconocimiento:**
  - Interacción con las aplicaciones demasiado pesadas.
- **Severidad:** Moderada
- **Posibilidad de ocurrencia:** Baja
- **Rol(es):**
  - Responsable del Centro de Informática
  - Personal autorizado de apoyo.
- **Recursos:**
  - Utilitarios de la misma aplicación para mantenimiento y/o depuración de la BD y recreación de índices.
  - Otros utilitarios para el mantenimiento de las BDs.
  - Experiencia.
- **Acciones:**
  - Llevar a cabo el fin de sesión de los usuarios de la aplicación.
  - Si es necesario, en el servidor cerrar todas las conexiones.

- Si es necesario, realizar una copia de respaldo de la BD.
- Si es necesario y dable, revisar el directorio de la aplicación y borrar todos los archivos temporales.
- Si es necesario, ejecutar los utilitarios.
- Pruebas.
- Luz verde

11. Incendio en las instalaciones del Centro de Informática

- **Reconocimiento:**
  - Fuego, humo y/o emanación de gases tóxicos.
- **Severidad**: Crítica
- **Posibilidad de ocurrencia:** Baja
- **Rol(es):** odo el personal de la Oficina de Informática
- **Recursos:**
  - Extintores.
  - Capacitación en el uso de extintores a todo el personal de la Oficina de Informática
- **Acciones:**
  - Tomar el extintor y usarlo en la zona del incendio.
  - Desconectar y retirar los equipos críticos de la zona del incendio (si posible).
  - Si es necesario, llamar a los bomberos.
  - Una vez controlado el incendio, llevar a cabo una evaluación de daños.
  - Estimar el tiempo de recuperación de la operatividad de la zona siniestrada.
  - Llevar a cabo las acciones del caso, para restaurar la operatividad de la zona siniestrada.
  - Luz verde.

12. Caso de Virus en la PC o Estación Cliente

- **Reconocimiento:**
  - Mensajes de virus detectado y no eliminado emitido por el software antivirus instalado.
  - Ralentización de la interacción del usuario con el equipo.
  - Cambios inesperados en los directorios de archivos.
  - Grupos de archivos de documentos que muestran el mismo tipo de corrupción.
  - Cambio del año del sistema, mientras la fecha aparentemente permanece correcta.
  - Al intentar ejecutar la aplicación del antivirus mensaje que "*otro programa está utilizando este archivo*".
  - Al intentar ejecutar alguna utilidades del sistema que "*otro programa está utilizando este archivo*".
  - Cambio inesperado en la página Web por defecto al iniciar un navegador, comúnmente página en idioma "chino".
  - Opcionalmente mensajes de ataques de virus en la PC de monitoreo del Responsable del Centro de Informática.
- **Severidad**: Moderada
- **Posibilidad de ocurrencia:** Medio
- **Rol(es):**
  - Responsable del Centro de Informática
- **Recursos:**
  - Software antivirus diferente al instalado y en el cual se tenga confianza.
  - Experiencia.
- **Acciones:**
  - Verificar si la PC cliente tiene actualizado su registro de virus a la fecha del día.

- Verificar si el antivirus ya no actualiza el registro de virus:
  - Por caducidad de la licencia
  - Por Usuario y contraseña inválidos
  - Clave o llave en la "lista negra".
- Si es necesario, desconectar físicamente la PC cliente de la red.
- Instalar el software antivirus alternativo.
- Actualizar el registro de virus vía Internet (si posible) ó a través de la copia de sus files de actualización en la PC cliente.
- Ejecutar el software antivirus.
- Evaluar los resultados de desinfección mostrados por el software antivirus.
- Llevar a cabo las siguientes evaluaciones:
  - Evaluar el QUIÉN y el CÓMO de estos eventos.
  - Evaluar el porqué el software antivirus originalmente instalado no cumplió a cabalidad su trabajo.
  - Evaluar la posibilidad de que la fuente de la infección esté fuera del control de la red administrativa.
- Hacer seguimiento a la capacidad de desinfección del antivirus originalmente instalado.
- Tomar las decisiones del caso, en base a los resultados de las diferentes evaluaciones llevadas a cabo.

13. Caso de Robo común

- **Reconocimiento:**
  - Falta comprobada del dispositivo o accesorio informático, o útil de oficina.
- **Severidad**: Moderada
- **Posibilidad de ocurrencia:** Muy Bajo
- **Rol(es):**
  - Usuario afectado
  - Responsable del Centro de Informática

- **Recursos:**
  - Ninguno.
- **Acciones:**
  - Reportar el robo al Jefe inmediato superior y a la Dirección del Centro de Informática
  - De acuerdo con la magnitud del robo, solicitar la investigación correspondiente.
  - En caso de que se trate de elementos informáticos, evaluar las medidas de seguridad física y de control del acceso físico a las oficinas. Tomar las decisiones del caso en base a los resultados de las evaluaciones llevadas a cabo.

PLAN DE RECUPERACIÓN DE DESASTRES

Es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre en el área Informática, considerando como tal todas las áreas de los usuarios que procesan información por medio de la computadora.

Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

La elaboración de los procedimientos que se determinen como adecuados para un caso de emergencia deben ser planeados y probados fehacientemente.

Las actividades a realizar en un Plan de Recuperación de Desastres se pueden clasificar en tres etapas:

1. ACTIVIDADES PREVIAS AL DESASTRE

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, que nos aseguren un proceso de Recuperación con el menor costo posible a nuestra Institución.

Podemos detallar las siguientes Actividades Generales:

1.1. Establecimiento del Plan de Acción.

En esta fase de Planeamiento se establecen los procedimientos relativos a:

a) Sistemas e Información.

La Institución tiene una relación de los Sistemas de Información con los que cuenta, tanto los realizados por el Centro de Informática como los hechos por las áreas usuarias.

Se identifica toda información sistematizada o no, que sea necesaria para la buena marcha Institucional.

La relación de Sistemas de Información tiene detallados los siguientes datos:

Nombre del Sistema:

SIGA

Lenguaje o Paquete con que fue creado:

Power Builder 10

Dueño del Sistema:

UNE-Oficina de Informática

Oficinas que usan el Sistema:

- Planificación y Desarrollo Institucional
- Adquisiciones y Contrataciones
- Administración y Desarrollo de Personal
- Economía y Finanzas
- Servicios Generales
- Bienestar Universitario
- Oficina de Informática

Equipamiento usuario mínimo necesario:

- Windows 7 o superior
- 2 GB de RAM
- 80 GB de disco duro
- Tarjeta de red 10/100/1000

❖ **Nombre del Sistema:**

Sistema Académico

Lenguaje o Paquete con que fue creado:

PHP

Dueño del Sistema:

UNE-Oficina de Informática

Oficinas que usan el Sistema:

- Oficina Central de Registro y Servicios Académicos
- Facultades

Equipamiento usuario mínimo necesario:

- Windows 7 o superior
- 2 GB de RAM
- 80 GB de disco duro
- Tarjeta de red 100/1000

❖ **Nombre del Sistema:**

SIAF

Lenguaje o Paquete con que fue creado:

Visual Fox Pro

Dueño del Sistema:

MEF

Oficinas que usan el Sistema:

- Planificación y Desarrollo Institucional
- Adquisiciones y Contrataciones
- Administración y Desarrollo de Personal
- Economía y Finanzas

Equipamiento usuario mínimo necesario:

- Windows 7 o superior
- 2 GB de RAM
- 100 GB de disco duro
- Tarjeta de red 100/1000

❖ **Nombre del Sistema:**

Sistema de Incidencias

Lenguaje o Paquete con que fue creado:

PHP

Dueño del Sistema:

UNE-Oficina de Informática

Oficinas que usan el Sistema:

- Oficina de Informática

Equipamiento usuario mínimo necesario:

- Windows 7 o superior
- 2 GB de RAM
- 100 GB de disco duro
- Tarjeta de red 10/100/1000

b) Actividades a realizar para volver a contar con la Base de Datos

Se debe recuperar el Sistema del backup que se encuentra en el Centro de Informática. Si fuera necesario, se procederá recuperar el Sistema del backup actual. De haber tenido problemas con todos los backups, se utilizará el backup almacenado en la sala de Servidores, siguiendo el orden de ubicación del (los) servidor (es) como a continuación se detalla:

1.- SERVIDOR DE BD ORACLE 11G

NOMBRE

ATENEA

HARDWARE

- PROCESADOR. Intel Xeon E5320 1.86Ghz.
- MEMORIA: 16GB
- DISCO DURO: (04) X 400 GB. 10K SAS

SOFTWARE

- Windows 2008R2 Enterprise SP1 64 Bits

2.- SERVIDOR DE CORREO EXCHANGE CAS (Virtualizado)

NOMBRE

HERA01

HARDWARE

- PROCESADOR. Intel Xeon X5667 3.07Ghz.
- MEMORIA: 12GB
- DISCO DURO: (01) X 80 GB

SOFTWARE

- Windows 2012R2 STD 64 Bits

3.- SERVIDOR DE CORREO EXCHANGE BD (Virtualizado)

NOMBRE

HERA02

HARDWARE

- PROCESADOR. Intel Xeon X5667 3.07Ghz.
- MEMORIA: 12GB
- DISCO DURO: (01) X 80 GB
  (01) X 1 TB

SOFTWARE

- Windows 2012R2 STD 64 Bits

4.- DIRECTORIO ACTIVO PRIMARIO (Virtualizado)

NOMBRE

ADONIS01

HARDWARE

- PROCESADOR. Intel Xeon X5667 3.07Ghz.

- MEMORIA: 6GB
- DISCO DURO: (01) X 80 GB

SOFTWARE

- Windows 2012R2 STD 64 Bits

5.- DIRECTORIO ACTIVO SECUNDARIO (Virtualizado)

NOMBRE

ADONIS02

HARDWARE

- PROCESADOR. Intel Xeon X5667 3.07Ghz.
- MEMORIA: 6GB
- DISCO DURO: (01) X 80 GB

SOFTWARE

- Windows 2012R2 STD 64 Bits

6.- AULA VIRTUAL PRINCIPAL MOODLE (Virtualizado)

NOMBRE

QUIMERA

HARDWARE

- PROCESADOR. Intel Xeon E5320 1.86Ghz.
- MEMORIA: 4GB
- DISCO DURO: (01) X 100 GB

SOFTWARE

- Linux CentOS 5 32 Bits

7.- SERVIDOR WEB (Virtualizado)

NOMBRE

HADES

HARDWARE

- PROCESADOR. Intel Xeon E5-2403 1.86Ghz.
- MEMORIA: 6GB
- DISCO DURO: (01) X 100 GB

SOFTWARE

- Linux CentOS 6 64 Bits

8.- SERVIDOR DE ARCHIVOS (Virtualizado)

NOMBRE

THOT

HARDWARE

- PROCESADOR. Intel Xeon X5667 3.07Ghz.
- MEMORIA: 8GB
- DISCO DURO: (01) X 100 GB
  (02) X 800 GB

SOFTWARE

- Windows 2008R2 Enterprise SP1 64 Bits

9.- SERVIDOR SIAF (Virtualizado)

NOMBRE

POSEIDON

HARDWARE

- PROCESADOR. Intel Xeon X5667 3.07Ghz.
- MEMORIA: 6GB
- DISCO DURO: (01) X 120 GB

SOFTWARE

- Windows 2008R2 Énterprise SP1 64 Bits

c) Actividades a realizar para volver a contar con la Información

Se debe recuperar la información de los backups generados. Si se ha perdido Sistema e Información hay que tratar de que los backups que se usen pertenezcan al mismo periodo o fecha para evitar conflictos y equivocación en los datos.

Hay que tener en cuenta que el Sistema de Backups debe estar lo suficientemente estructurado para poder identificar rápida y eficientemente la información que se necesita.

d) Actividades para volver a contar con los Servidores

Una vez evaluado el daño se procederá a reparar o adquirir un Nuevo equipo manteniendo su configuración original y restaurando la data de los sistemas de backup.

Determinados los Servidores vitales para el mínimo desenvolvimiento de la Universidad Nacional de Educación, procedemos a indicar sus características actuales:

1. **Servidor Base de Datos Oracle:**
   - Sistema Operativo:
     Windows Server 2008R2 SP1 64 BITS.
   - Sistema Base de Datos:
     Oracle 11G
   - Modelo:
     Dell PowerEdge 2950
   - Procesador:
     Intel Xeon E5320 1.86Ghz.
   - Almacenamiento Magnético:
     DISCO DURO: (04) X 400 GB. 10K SAS
     Memoria Ram: 16 GB
     Lector/Grabador DVD RW.

2. **Servidor de Correo CAS:**
   - Sistema Operativo Virtualizado:
     Windows Server 2012R2 STD 64 BITS.
   - Sistema Base de Datos:

   - Modelo:
     Dell PowerEdge R710
   - Procesador:
     Intel Xeon X5667 3.07Ghz.
   - Almacenamiento Magnético:
     Disco duro: (01) X 80 GB.
     Memoria Ram: 12 GB

3. **Servidor de Correo BD:**
   - Sistema Operativo Virtualizado:
     Windows Server 2012R2 STD 64 BITS.
   - Sistema Base de Datos:

   - Modelo:
     Dell PowerEdge R710
   - Procesador:
     Intel Xeon X5667 3.07Ghz.
   - Almacenamiento Magnético:
     Disco duro: (01) X 80 GB.
     (01) X 1 TB.
     Memoria Ram: 12 GB

4. **Directorio Activo Principal:**
   - Sistema Operativo Virtualizado:
     Windows Server 2012R2 STD 64 BITS.
   - Sistema Base de Datos:

   - Modelo:
     Dell PowerEdge R710
   - Procesador:
     Intel Xeon X5667 3.07Ghz.
   - Almacenamiento Magnético:
     Disco duro: (01) X 80 GB.
     Memoria Ram: 6 GB

5. **Directorio Activo Secundario:**
   - Sistema Operativo Virtualizado:
     Windows Server 2012R2 STD 64 BITS.
   - Sistema Base de Datos:

   - Modelo:
     Dell PowerEdge R710
   - Procesador:
     Intel Xeon X5667 3.07Ghz.
   - Almacenamiento Magnético:

Of. de Organización y Procesos - UNE - | OFICINA DE ASESORÍA LEGAL V°B° | OFICINA DE INFORMÁTICA V°B° | SECRETARÍA GENERAL - UNE - | Univ. Nac. de Educ. - RECTOR

Disco duro: (01) X 80 GB.

Memoria Ram: 6 GB

6. **Aula Virtual:**
   - Sistema Operativo Virtualizado:
     Linux Centos 5 de 32 bits.
   - Sistema Base de Datos:
     MySql
   - Modelo:
     Dell PowerEdge 2950
   - Procesador:
     Intel Xeon E5320 1.86Ghz.
   - Almacenamiento Magnético:
     Disco duro: (01) X 100 GB.
     Memoria Ram: 4 GB

7. **Servidor Web:**
   - Sistema Operativo Virtualizado:
     Linux Centos 6 64 bits.
   - Sistema Base de Datos:
     MySql
   - Modelo:
     Dell PowerEdge R520
   - Procesador:
     Intel Xeon E5-2403 1.86Ghz.
   - Almacenamiento Magnético:
     Disco duro: (01) X 100 GB.
     Memoria Ram: 6 GB

8. **Servidor de Archivos:**
   - Sistema Operativo Virtualizado:
     Windows Server 2008 R2 SP1 de 64 BITS.
   - Sistema Base de Datos:

   - Modelo:
     Dell PowerEdge R710
   - Procesador:
     Intel Xeon X5667 3.07Ghz.

- Almacenamiento Magnético:
  Disco duro: (01) X 80 GB.
  (02) X 800 GB.
  Memoria Ram: 8 GB

e) Prácticas Habituales

Se debe considerar la práctica de reposición de equipos:

- **Por tiempo de vida**, al deterioro natural de los componentes internos que sufre el equipo informático. En ese caso el Centro de Informática elaborará un informe Técnico del equipo en atención al requerimiento hecho por el Área solicitante.
- **Por falla de Hardware**, al presentarse esta situación primero se deberá verificar si el equipo cuenta con garantía para ser enviado al proveedor. De no ser así, el Centro de Informática o el Proveedor elevará un informe Técnico, el cual determinará la atención al requerimiento que será hecho por el Área solicitante.
- **Por Pérdida**, en este caso se aplicará el ítem 7.1. de la Directiva Nº 018-2009-R-UNE "Inventario físico de bienes muebles, equipos y otros activos de la UNE", aprobado con ResoluciónNº 3617-2009-R-UNE.

Los usuarios deberán seguir las siguientes recomendaciones sobre el cuidado de los equipos de cómputo:

- **Teclado.** Mantener fuera del teclado grapas y clips; así como elementos líquidos que puede causar un cruce de función.
- **CPU.** Mantener la parte posterior del CPU liberado en por lo menos 10cm. para asegurar así una ventilación adecuada.
- **Mouse**. Poner debajo del mouse una superficie plana y limpia, de tal manera que no se ensucie la base y evitar los golpes.
- **Impresora**. El manejo de las impresoras en general es a través de los botones o rodillos. En caso de mala impresión luego de imprimir documentos o cuadros generados, apagar por unos segundos la impresora para que se pierda el set dejado. Según la tecnología se tienen:
  - **Matriciales**: no usar rodillo cuando esté prendido, tratar con cuidado los sujetadores de papel y no apagar de súbito. Asegurarse que el ONLINE esté apagado, así evitaremos problemas de cabezal y sujetador.

- **Inyección**: al cambiar la tinta asegurarse de sacar la cinta de seguridad, mantenerla libre de polvo, grapas, clips, etc; usar las guías de papel correctamente, usar papeles no arrugados y no exponerla a la luz solar.
- **Láser**: al cambiar el tóner agitar suavemente para distribuir el polvo uniformemente y retirar la cintilla de seguridad. Antes de cargar el papel flexionar las hojas hacia los dos lados y airearlas, usar las guías de papel correctamente, mantenerla libre de polvo, grapas, clips, agua, comida, etc.

Mantener las áreas limpias y pulcras

Todas las razones para mantener las áreas operativas limpias y pulcras son numerosas. Algunos de los problemas que se pueden evitar son: el daño potencial al equipo por derramar el café, gaseosa, agua, etc en los componentes del sistema, el peligro de fuego que se presentan por el excesivo almacenamiento de hojas continuas, papel desechado, el peligro por fumar.

El usuario es responsable de la limpieza externa y cuidado de los equipos informáticos, quien, además de lo indicado líneas arriba, deberá recurrir a elementos de limpieza y protección como cremas limpiadoras, sprays, fundas, etc.

f) Equipos Operativos.

En cada unidad operativa de la Universidad Nacional de Educación se deberá designar un responsable de la seguridad de la Información de su área. Esta tarea puede ser desempeñada por el Jefe de dicha Área Operativa.

Funciones:

- Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.
- Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas.
- Supervisar procedimientos de respaldo y restauración.
- Participar en las pruebas y simulacros de sistemas.

2. ACTIVIDADES DURANTE EL DESASTRE

2.1. Equipos

Los equipos deben tener un Jefe elegido por los mismos integrantes. Él es el responsable de coordinar con los superiores los recursos y medidas necesarias para la mejor realización de su tarea.

Estos equipos deberán estar compuestos por tres o cuatro personas cada uno y se definen de la siguiente manera:

2.2.1. Para combatir siniestro.

Los criterios para la elección de este equipo no incluyen conocimientos de Sistemas mas sí un grado de madurez, criterio, confianza con el personal y de preferencia con características de liderazgo.

Funciones:

Realizar las llamadas correspondientes para el pedido de auxilio. Los teléfonos a considerar son:

- Central Policial: 105
- Central de Bomberos: 116
- Comisaría de Chosica: 3603127
- Escuadrón de Emergencia: 4828988
- Bomberos de Chosica 32: 3610260
- Serenazgo de Chosica 3603171
- ESSALUD: 4118000

Los datos que generalmente se piden por teléfono son:

- Dirección y lugar exacto donde ocurre u ocurrió el problema.
- Referencia del tipo de Emergencia.
- Número telefónico de donde se realiza la llamada.
- Nombre de la persona que realiza la llamada.

Accciones:

- Realizar un recuento del Personal y prestar los servicios de primeros auxilios hasta que llegue el personal de Rescate.
- Evaluar la situación y tomar las medidas convenientes. Si es posible combatir el siniestro (fuego, cortocircuito, etc.), se debe actuar (uso de

extintores, corte del suministro eléctrico, etc.), pero no si esto pone en riesgo la vida de alguien.

- Si la situación lo amerita, se debe proceder a la evacuación del personal. Esto se debe realizar por las escaleras y en orden. Los miembros del equipo deben proporcionar confianza y calma al personal.
- No se debe olvidar que la razón principal de la formación de este equipo es reducir al máximo las posibles pérdidas de vidas en el caso de un desastre o emergencia.

2.2.2. **Para salvar Recursos Informáticos**

En este caso, para la elección de este equipo, se deben tener en cuenta ciertas características tales como: cierto conocimiento de informática (sobre todo el jefe del equipo), condiciones físicas apropiadas que le permitan hacer transporte de equipo, alto grado de responsabilidad, etc.

Funciones:

- Coordinar con el Equipo para combatir Siniestro y evaluar la posibilidad de salvar recursos informáticos sin arriesgar la vida.
- De ser posible esto, el Jefe del equipo determinará, según la emergencia el modo y los equipos que se procederá a salvar.
- No se debe olvidar que la prioridad básica es la protección de la integridad del personal.
- Si no existiera forma de salvar el equipo informático, los integrantes de este equipo tendrán que ponerse a disposición del equipo para combatir el Siniestro.

2.2.3. **Entrenamiento**

Se debe establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo con los roles que se les haya asignado en los planes de evacuación del personal o equipos. Para minimizar se puede aprovechar fechas de recarga de extintores, charlas de los proveedores, etc.

Es necesario que los elementos directivos participen de estas actividades para que el personal tome conciencia de la importancia que la Alta Dirección otorga a la Seguridad Institucional.

Para ayudar al entrenamiento y capacitación de los equipos, el responsable de la implantación del Plan de Contingencias deberá solicitar la ayuda y colaboración de ciertas Instituciones o áreas:

- Cuerpo de Bomberos Voluntarios del Perú, sede Chosica.
- Comandante de la Comisaría de Chosica.
- Serenazgo de la Municipalidad de Chosica.
- Jefe de Defensa Civil de la Municipalidad de Chosica.

3. ACTIVIDADES DESPUÉS DEL DESASTRE

CUADRO N° 1: MEDIDAS DESPUÉS DEL DESASTRE

DESCRIPCION DE CAUSAL	MEDIDA A TOMAR
SINIESTROS	
Incendio	Utilizar los extintores, cortar el suministro eléctrico, llamar al Cuerpo de Bomberos de Chosica, Centros de Salud de acuerdo con la magnitud del daño.
Vandalismo	Comunicar a la Policía de Chosica, Unidad de Control Patrimonial y Seguridad según tipo de daño.
Corto Circuito	Utilizar los extintores, cortar el suministro eléctrico, llamar al Cuerpo de Bomberos de Chosica, Centros de Salud de acuerdo con la magnitud del daño.
Terremoto	Coordinar con el Cuerpo de Bomberos, Centros de Salud y Defensa civil.
Atentado terrorista	Comunicar a la Policía Nacional, Unidad de Control Patrimonial y Seguridad según el tipo de daño.
ROBOS	
Fraude	Comunicar a la Unidad de Control Patrimonial y Seguridad.
Robo de Equipo	Comunicar a la Unidad de Control Patrimonial y Seguridad.
Robo de Información	Comunicar a la Unidad de Control Patrimonial y Seguridad.
FALLAS DE HARDWARE	
Falla de la Tarjeta Principal	Diagnóstico y Mantenimiento correctivo o reemplazo.
Falla Equipo de Comunicación	Diagnóstico y Mantenimiento correctivo o reemplazo.
Falla de Disco duro	Diagnóstico y Mantenimiento correctivo o reemplazo.
Falla de Tarjeta de Red	Diagnóstico y Mantenimiento correctivo o reemplazo.
Falla de la Fuente de Alimentación	Diagnóstico y Mantenimiento correctivo o reemplazo.

FALLAS DE SOFTWARE	
Falla del Sistema Operativo	Diagnóstico y Mantenimiento correctivo.
Falla de Software Base	Diagnóstico y Mantenimiento correctivo.
Falla de Software Aplicativo	Diagnóstico y Mantenimiento correctivo.
Falla de Base de Datos	Diagnóstico y Mantenimiento correctivo.
ERRORES HUMANOS	
Borrado de Datos	Restaurar archivos con copias de seguridad.
Apagado de Equipos	Solicitar soporte técnico.
Perdida de Claves de Acceso	Solicitar reposición al Administrador de Red.
Perdida de Llaves de Acceso	Solicitar copias de la llave a Administración.
ACCESOS NO AUTORIZADOS	
Accesos Físicos no autorizados	Evaluación del área a cargo de cada jefatura para las acciones del caso.
Accesos Lógicos no autorizados	Bloqueo de la clave de acceso y supervisión.
MALWARE INFORMÁTICO	
Infecciones por Virus informaticos	Desinfección o eliminación con antivirus actualizado.
VANDALISMO INFORMÁTICO	
Borrado de Información	Evaluación de restauración con copias de seguridad.
Deterioro de Equipos	Ver política de reposición de equipos.
Hackers	Evaluación de daño y restauración de backups

Cada funcionario es responsable de su área y deberá aplicar o comunicar al órgano competente para que tome las medidas indicadas en el anterior cuadro.

3.1. Evaluación de Daños

Este punto permitirá definir el universo de daños sobre los que hay que recuperarse. Además es un documento básico para iniciar la Priorización de Actividades, ver cuadro N° 1.

La realización de este punto es responsabilidad de la Dirección General de Administración.

3.2. Priorización de Actividades

Dado que el Plan se logra imaginando un escenario de pérdida total, la evaluación de los daños reales ocurridos y su comparación con el Plan de Contingencia arrojará la lista de las actividades que se deben realizar, siempre priorizándola de

acuerdo con las actividades estratégicas y urgentes de la Universidad Nacional de Educación.

A este nivel se tomarán decisiones tales como asignar temporalmente personal de alguna área que no resultó seriamente dañada con el apoyo del personal de Informática.

3.3. Ejecución de Actividades.

La ejecución de actividades implica la creación de equipos de trabajo, en el momento de la contingencia, para realizar las actividades previamente planificadas en el Plan de Acción.

Cada uno de estos equipos deberá contar con un Coordinador que deberá reportar diariamente el avance de los trabajos de recuperación a la Jefatura a cargo del Plan de Contingencias.

El Jefe a cargo del Plan de Contingencias debe orientar las actividades diferenciando dos etapas:

- Restauración del Servicio usando los recursos de la Universidad Nacional de Educación.
- Volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información.

3.4. Evaluación de Resultados

La realización de este punto permitirá tener un registro para llevar un archivo histórico de las contingencias.

De la evaluación de resultados y del siniestro en sí, deberían de salir dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

3.5. Retroalimentación del Plan

El Plan de Contingencias tiene que tener una constante revisión ya sea por parte de la Dirección General de Administración y la Oficina de Central de Planificación y Desarrollo Institucional, vigilando la correspondencia entre la relación de Sistemas de Información necesarios para la operatividad de la Universidad Nacional de Educación, optimizando el Plan de Contingencias original luego de sufrida una contingencia o por cambios tecnológicos, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

Glosario de Términos

- **Análisis de riesgo**:

  Estudio sistemático para analizar cuáles son los riesgos relativos a la calidad y a la seguridad a los que se encuentra sometido un proceso en una organización, sus costes asociados y las contramedidas más eficientes para reducir o eliminar los riesgos identificados.

- **Confidencialidad**:

  Condición que asegura que la información no pueda estar disponible o ser descubierta por las personas, las entidades o los procesos no autorizados.

- **Contraseña**:

  Palabra clave que identifica al usuario para proteger el acceso a un equipo, a una aplicación o a un módulo de una aplicación.

- **Copia de seguridad**:

  Replicación periódica y almacenamiento externo (usualmente en discos, CDs, memorias USB, etc.) de datos y programas en previsión de posibles contingencias. Reproducción de los datos actuales guardados en un soporte informático, para tenerlos disponibles en caso de que un desastre del sistema impida recuperar los datos con los que se está trabajando.

- **Dispositivo de almacenamiento**:

  Elemento físico que almacena información de forma permanente.

- **Experiencia**:

  La capacidad, conocimiento y "know how" que poseen los expertos en un determinado dominio que les permite llevar a cabo eficientemente una tarea.

- **Parche**:

  Código que aplicado a un programa, modifica el funcionamiento de este, bien para solucionar un problema, o bien para dotarlo de funcionalidad adicional.

- **Plan de contingencias**:

  Es un documento que establece una estrategia de respuesta para atender en forma oportuna, eficiente y eficaz, un desastre, evento natural u otros, por culpa de algún incidente tanto interno como externo a la Institución. En él se definen las responsabilidades de las entidades y persona que intervienen en la operación, se provee información básica sobre posibles áreas afectadas y recursos susceptibles de

Of. de Organización y Procesos · OFICINA DE ASESORÍA LEGAL V°B° · V°B° · SECRETARÍA GENERAL · Univ. Nac. de Ucayali

sufrir interrupción en el funcionamiento. También sugiere cursos de acción para hacer frente al evento presentado, de manera que se permita racionalizar el empleo de personal, equipos e insumos disponibles, para proteger en su orden: la vida humana (empleados), la infraestructura, bienes (de la Institución y de terceros) y el ambiente (recursos: agua, aire, suelo, flora y fauna).

- **Política de seguridad**:

  Conjunto de principios y reglas, propias de la organización, que declaran cómo se especificará y gestionará la protección de los activos de información de una manera consistente y segura.

- **Recuperación de desastres**

  Cuando ocurre una contingencia, es esencial que se conozca a detalle el motivo que la originó y el daño producido. En ese sentido, es importante definir los procedimientos y los planes de acción para el caso de una posible falla, siniestro o desastre en el área informática.