PLAN DE CONTINGENCIA INFORMÁTICO Y SEGURIDAD DE INFORMACION 2009, APLICADO EN LA UNIVERSIDAD NACIONAL DE PIURA.

PRESENTACIÓN

El Plan de Contingencia Informático (o Plan de Contingencia Institucional) implica un análisis de los posibles riesgos a cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información. Corresponde aplicar al Centro de Informática y Telecomunicaciones, aplicar medidas de seguridad para proteger y estar preparados para afrontar contingencias y desastres de diversos tipos.

El alcance de este plan guarda relación con la *infraestructura informática*, así como los *procedimientos relevantes asociados con la plataforma tecnológica*. *La infraestructura informática* esta conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función del negocio. *Los procedimientos relevantes a la infraestructura informática*, son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).

El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre. La información como uno de los activos más importantes de la Organización, es el fundamento más importante de este Plan de Contingencia.

Al existir siempre la posibilidad de desastre, pese a todas nuestras medidas de seguridad, es necesario que El Plan de Contingencia Informático incluya el Plan de Recuperación de Desastres con el único objetivo de restaurar el Servicio Informático en forma rápida, eficiente, con el menor costo y perdidas posibles.

El Centro de Procesamiento de Datos o área de Informática, de la Universidad Nacional de Piura, es el Centro de Informática y Telecomunicaciones (CIT). El presente estudio brinda las pautas del Plan de Contingencias Informático y Seguridad de Información 2009 en la Universidad Nacional de Piura.

RESUMEN

La protección de la información vital ante la posible pérdida, destrucción, robo y otras amenazas de una empresa, es abarcar la preparación e implementación de un completo Plan de Contingencia Informático. El plan de Contingencia indica las acciones que deben tomarse inmediatamente tras el desastre. Un primer aspecto importante del plan es la organización de la contingencia, en el que se detallan los nombres de los responsables de la contingencia y sus responsabilidades. El segundo aspecto crítico de un Plan de Contingencia es la preparación de un Plan de Backup, elemento primordial y necesario para la recuperación. El tercer aspecto es la preparación de un Plan de Recuperación. La empresa debe establecer su capacidad real para recuperar información contable crítica en un periodo de tiempo aceptable. Otro aspecto importante del plan de recuperación identificar el equipo de recuperación, los nombres, números de teléfono, asignaciones específicas, necesidades de formación y otra información esencial, para cada miembro del equipo que participa en el Plan de recuperación.

La base del Plan de Contingencia y su posterior recuperación, es establecer prioridades claras sobre que tipo de procesos son los más esenciales. Es necesario por tanto la identificación previa de cuales de los procesos son críticos y cuales son los recursos necesarios para garantizar el funcionamiento de las aplicaciones de gestión.

El Plan de Recuperación del Desastre (PRD) *provee de mecanismos de recuperación para los registros vitales, sistemas alternativos de telecomunicaciones, evacuación de personal, fuente alternativa de provisión de servicios, etc.* Además debe ser comprobado de forma periódica para detectar y eliminar problemas. La manera más efectiva de comprobar si un PRD funciona correctamente, es programar simulaciones de desastres. Los resultados obtenidos deben ser cuidadosamente revisados, y son la clave para identificar posibles defectos en el Plan de Contingencia.

El plan de contingencia informático, debe contemplar los planes de emergencia, backup, recuperación, comprobación mediante simulaciones y mantenimiento del mismo. Un plan de contingencia adecuado debe ayudar a las empresas a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal del negocio.

¿Cual es el grado de preparación de las empresas para estos desastres?. Los desastres han demostrado que la capacidad de recuperarse ante ellos es crucial para la supervivencia de una empresa.

La Dirección General debe comprender los principales riesgos para la empresa y las posibles consecuencias de un desastre. Un Plan de contingencia adecuado identifica las necesidades de todos los departamentos e involucra a TODO el personal de todas las áreas de la compañía.

DEDICATORIA

***A Dios**, Por ser mi guía y luz en mis incertidumbres. Por mantener en mí, el espíritu Superación.*

***A mis padres**, Por su comprensión y apoyo en mis metas, para nunca desmayar ante la adversidad.*

AGRADECIMIENTOS

Al Jefe del Centro de Informática y Telecomunicaciones y compañeros de Trabajo.

PLAN DE CONTINGENCIA INFORMATICO Y SEGURIDAD DE INFORMACION 2009, APLICADO EN LA UNIVERSIDAD NACIONAL DE PIURA.

INDICE

CAPITULO III: PLAN DE RECUPERACIÓN DEL DESASTRE Y RESPALDO DE LA INFORMACION

CAPITULO I. ANALISIS DE LA SITUACION ACTUAL INFORMATICA EN LA UNP

1.1. Introducción

Cualquier Sistema de Redes de Computadoras (ordenadores, periféricos y accesorios) están expuestos a riesgo y puede ser frente fuente de problemas. El Hardware, el Software están expuestos a diversos Factores de Riesgo Humano y Físicos.

Frente a cualquier evento, la celeridad en la determinación de la gravedad del problema depende de la capacidad y la estrategia a seguir para señalar con precisión, por ejemplo: ¿Qué componente ha fallado?, ¿Cuál es el dato o archivo con información se ha perdido, en que día y hora se ha producido y cuan rápido se descubrió? Estos problemas menores y mayores sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información.

Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el disco duro), bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que producen daño físico irreparable. Frente al mayor de los desastres solo queda el tiempo de recuperación, lo que significa adicionalmente la fuerte inversión en recursos humanos y técnicos para reconstruir su Sistema de Red y su Sistema de Información.

1.2. Objetivos e Importancia del Plan de Contingencia

Objetivos

- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.
- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

Importancia

- Garantiza la seguridad física, la integridad de los activos humanos, lógicos y materiales de un sistema de información de datos.
- Permite realizar un conjunto de acciones con el fin de evitar el fallo, o en su caso, disminuir las consecuencias que de el se puedan derivar.
- Permite realizar un Análisis de Riesgos, Respaldo de los datos y su posterior Recuperación de los datos. En general, cualquier desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de una empresa. La probabilidad de que ocurra un desastre es muy baja, aunque se diera, el impacto podría ser tan grande que resultaría fatal para la organización.
- Permite definir contratos de seguros, que vienen a compensar, en mayor o menor medida las pérdidas, gastos o responsabilidades.

1.3. Sistema de Red de Computadoras en la UNP

La Red de la UNP cuenta con Tecnologías de la información (TI) en lo referente a: sistemas de comunicación, sistemas de información, conectividad y servicios Informáticos que se brinda de forma interna y externa a las diferentes Oficinas, Facultades, Dependencias. Se resume que la Administración de Red esta dividido en dos rubros: 1) Conectividad: se encargada de la conexión alambrica e inalámbrica de los equipos de comunicación y 2) Manejo de servidores: se encarga de alojar todos los servicios y sistemas de comunicación e información.

Los servicios de Red implementados en la Universidad Nacional de Piura son, implementados en sus servidores son los siguientes:

- Servidor de Correo Electrónico
- Servidor de seguridad
- Servidor de seguridad – base de datos
- Servidor de telefonía IP.
- Servidor de Políticas de Grupo – Controlador de dominio

1.4. Sistema de Información en la UNP

El Sistema de Información, incluye la totalidad del Software de Aplicación, Software en Desarrollo, conjunto de Documentos Electrónicos, Bases de Datos e Información Histórica registrada en medios magnéticos e impresos en papeles, Documentación y Bibliografía.

El listado de Sistema de Información en la Universidad Nacional de Piura, se detalla en el Anexo V.

CAPITULO II. PLAN DE REDUCCIÓN DE RIESGOS

El presente documento implica la realización de un análisis de todas las posibles causas a los cuales puede estar expuestos nuestros equipos de conectados a la RED de la UNP, así como la información contenida en cada medio de almacenamiento. Se realizara un análisis de riesgo y el Plan de Operaciones tanto para reducir la posibilidad de ocurrencia como para reconstruir el Sistema de Información y/o Sistema de Red de Computadoras en caso de desastres.

El presente Plan incluye la formación de equipos de trabajo durante las actividades de establecimiento del Plan de Acción, tanto para la etapa preventiva, correctiva y de recuperación.

El Plan de Reducción de Riesgos es equivalente a un Plan de Seguridad, en la que se considera todos los riesgos conocidos, para lo cual se hará un *Análisis de riesgos*.

2.1. Análisis de Riesgos

El presente realiza un análisis de todos los elementos de riesgos a los cuales esta expuesto el conjunto de equipos informáticos y la información procesada, y que deben ser protegidos.

Bienes susceptibles de un daño

Se puede identificar los siguientes bienes afectos a riesgos:

a) Personal

b) Hardware

c) Software y utilitarios

d) Datos e información

e) Documentación

f) Suministro de energía eléctrica

g) Suministro de telecomunicaciones

Daños

Los posibles daños pueden referirse a:

a) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.

b) Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

c) Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia.

Fuentes de daño

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

- Acceso no autorizado
- Ruptura de las claves de acceso a los sistema computacionales
- Desastres Naturales: a) Movimientos telúricos b) Inundaciones c) Fallas en los equipos de soporte (causadas por el ambiente, la red de energía eléctrica, no acondicionamiento atmosférico necesario)
- Fallas de Personal Clave: por los siguientes inconvenientes: a) Enfermedad b) Accidentes c) Renuncias d) Abandono de sus puestos de trabajo e) Otros.
- Fallas de Hardware: a) Falla en los Servidores (Hw) b) Falla en el hardware de Red (Switches, cableado de la Red, Router, FireWall)
- Incendios

2.1.1. Características

El Análisis de Riesgos tiene las siguientes características:

- Es posible calcular la probabilidad de que ocurran las cosas negativas.
- Se puede evaluar económicamente el impacto de eventos negativos.
- Se puede contrastar el Costo de Protección de la Informática y medios versus el Costo de volverla a producir.

Durante el estudio Análisis de Riesgo, se define claramente:

- Lo que intentamos proteger
- El valor relativo para la organización
- Los posibles eventos negativos que atentarían lo que intentamos proteger.
- La probabilidad de ataque.

Se debe tener en cuenta la probabilidad de suceso de cada uno de los problemas posibles, de tal manera de tabular los problemas y su costo potencial mediante un Plan adecuado. Los criterios que usaremos para tipificar los posibles problemas son:

Tabla 01. Escala de Valores para Criterios de Posibles Problemas

Criterios	Escala			
Grado de Negatividad	Leve	Moderado	Grave	Muy severo
Posible Frecuencia del Evento negativo	Nunca	Aleatorio	Periódico	Continuo

Grado de impacto o consecuencias	Leve	Moderado	Grave	Muy severo
Grado de Certidumbre	Nunca	Aleatorio	Probable	Seguro

2.1.2. Clases de Riesgo

La tabla 02 proporciona el Factor de Probabilidad por Clase de Riesgo en función a la ubicación geográfica de la institución y a su entorno institucional; por ejemplo, si la institución:

- Se ubica en zona sísmica el factor de probabilidad de desastre por terremotos será alta.
- Se ubica en una zona marginal con alto índice de delincuencia, las probabilidades de robo, asalto o vandalismo será de un sesgo considerablemente alto.
- Se ubica en zona industrial las probabilidades de "Fallas en los equipos" será alto por la magnitud de variaciones en tensiones eléctricas que se generan en la zona.
- Cambia constantemente de personal, las probabilidades de equivocaciones y sabotaje será alto.

Identificación de Amenazas:

Tabla 02. Escala Factor de Probabilidad por Clase de Riesgo

Clase	Factor
Incendio o Fuego	0.40
Robo común de equipos y archivos	0.75
Sabotaje	0.60
Falla en los equipos	0.40
Equivocaciones	0.70
Acción virus informático	0.50
Fenómenos naturales	0.25
Accesos no autorizados	0.75
Robo de datos	0.80
Manipulación y sabotaje	0.80

Estos valores son estimados y corresponden a la apreciación de antecedentes históricos registrados en la UNP durante los últimos años. Corresponde al presente Plan de Contingencia minimizar estos índices con medidas preventivas y correctivas sobre cada caso de Riesgo

En lo que respecta a Fenómenos naturales, nuestra región ha registrado en estos últimos tiempos movimientos telúricos de poca intensidad; sin embargo, las lluvias fuertes producen mayores estragos, originando filtraciones de agua en los edificios de techos, produciendo cortes de luz, cortos circuitos (que podrían desencadenar en incendios).

2.1.2.1. Clase de Riesgo: Incendio o Fuego

Grado de Negatividad:	Muy Severo
Frecuencia de Evento:	Aleatorio
Grado de Impacto:	Grave
Grado de Certidumbre:	Probable

Situación actual	Acción correctiva
El área de Servidores del CIT-UNP cuenta con un extintor cargado, ubicado dentro del Área de Servidores.	Se cumple
En muchos Centros de cómputo de la UNP, no cuenta con un extintor.	Instalar extintores para los centros de cómputo de la UNP.
No se ejecuta un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, lo que no es eficaz para enfrentar un incendio y sus efectos.	Implantar un Programa de Capitación para el manejo de extintores.
Debido al incremento del número de computadores por oficina se hace necesario contar con extintores en las oficinas.	Incrementar el número de extintores por área.

Una probabilidad máxima de contingencia de este tipo en el CIT, puede alcanzar a destruir un 50% de las oficinas antes de lograr controlarlo, también podemos suponer que en el área de Servidores tendría un impacto mínimo, por las medidas de seguridad y ambiente que lo protege. Esta información permite resaltar el tema sobre el lugar donde almacenar los backups. El incendio, a través de su acción calorífica, es más que suficiente para destruir los Dispositivos de almacenamiento, tal como CD's, DV's, cartuchos, Discos duros, las mismas que residen en una caja fuerte (medio de seguridad que nos protege frente a robo o terremoto, pero no del calor). Estos dispositivos de almacenamiento muestran una tolerancia de temperatura de 5°C a 45°C, y una humedad relativa de 20% a 80%.

Para la mejor protección de los dispositivos de almacenamiento, se colocaran estratégicamente en lugares distantes, con una Segunda Copia de Seguridad custodiada en un lugar externo de la UNP.

Las áreas funcionales distribuidas en el campus de la UNP, existe al menos una computadora, por lo que se debe incrementar los elementos y medidas de seguridad contra incendios.

Uno de los dispositivos más usados para contrarrestar la contingencia de incendio, son los extinguidores. Su uso conlleva a colocarlos cerca del las posibles áreas de riesgo que se debe proteger. A continuación se detallan los letreros y símbolos que debe conocer todo el personal en el uso del extinguidor.

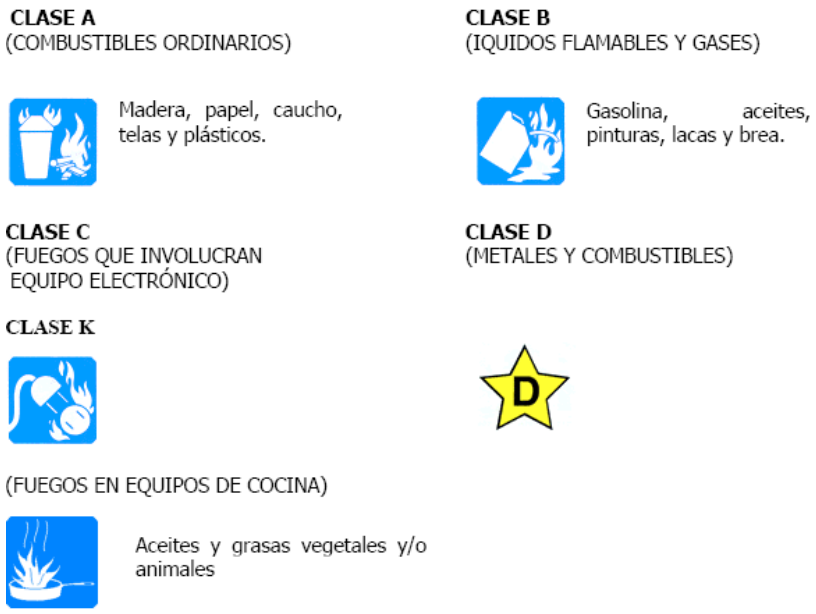


Fig.01 letreros y símbolos usados en los extinguidores.

A continuación se describe gráficamente el procedimiento para el uso de extinguidores en caso de incendio:

Fig.02 procedimiento para el uso de extinguidores.

2.1.2.2. Clase de Riesgo: Robo Común de Equipos y Archivos

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Moderado

Grado de Certidumbre: Aleatorio

Situación actual	Acción correctiva
Vigilancia permanente.	Existe vigilancia. La salida de un equipo informático es registrada por el personal de la Oficina y por el personal de seguridad en turno.
No se verifica si el Personal de Seguridad cumple con la inspección de los usuarios, sobre su obligación de cerrar puertas y ventanas al finalizar su jornada.	Al respecto Personal de Seguridad emite recomendaciones sobre medidas de Alerta y seguridad.
Remitir aviso a la Oficina de Patrimonio y al CIT, para retirar equipo de informático.	Se Cumple

No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización debida entre el Jefe del Área funcional y Jefe de CIT. Esto demuestra que los equipos se encuentran protegidos de personas no autorizadas y no identificables.

Según antecedentes de otras instituciones, es de conocer que el robo de accesorios y equipos informáticos, llegaron a participar personal propio de la empresa en colusión con el personal de vigilancia. Es relativamente fácil remover un disco duro del CPU, una disquetera, tarjeta, etc. y no darse cuenta del faltante hasta días después. Estas situaciones *no se han presentado en nuestro Centro de Informática y Telecomunicaciones, pero se recomienda siempre estar alerta*.

2.1.2.3. Clase de Riesgo: Vandalismo

Grado de Negatividad: Moderado

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual	Acción correctiva
La UNP esta en una zona donde el índice de vandalismo es bajo	Hay vigilancia.
Se presentan casos muy aislados de alumnos, en el Proceso de Inscripción de cursos; que no están conformes con algunas normativas académicas-administrativas, tal que al efectuar sus reclamos personalmente asumen actitudes retroactivas, que muchas veces ofenden al trabajador, y sin medir las consecuencias pueden llegar a dañar alguna instalación de la UNP.	Continuar con la política de Gestión de mejorar la Atención del Cliente, brindando *la información*, previa a Procesos académicos.
Alguna probabilidad de turbas producto de manipulaciones políticas.	Mantener buenos vínculos y coordinaciones permanentes con la Policía Nacional del Perú.

La destrucción del equipo puede darse por una serie de desastres incluyendo el vandalismo, robo y saqueo en simultáneo.

2.1.2.4. Clase de Riesgo: Falla en los Equipos

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual	Acción correctiva
La Red de Servidores en el CIT cuenta con una Red Eléctrica Estabilizada.	Proponer un Estudio para instalar una Red Eléctrica Estabilizada.
No existe un adecuado tendido eléctrico en algunas oficinas de la UNP	Tomar previsiones económicas para implementar un adecuado tendido eléctrico.
Cada área funcional se une a la Red a través Gabinetes, la falta de energía en éstos, origina la ausencia de uso de los servicios de red: los Sistemas Informáticos, Teléfonos IP, mantenimiento remoto.	Proteger los Gabinetes, y su adecuado apagado y encendido, dependen os servicios de red en el Área.
La falla en el hardware de los equipos, requiere un rápido mantenimiento o reemplazo.	Existe Mantenimiento de los equipos de cómputo. Contar con proveedores, en caso de requerir reemplazo de piezas, y de ser posible contar con repuestos.

De ocurrir esta contingencia las operaciones informáticas se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido provocaría un trastorno en las operaciones del día, sin afectar los datos.

El equipo de aire acondicionado y ambiente adecuado en el Área de Servidores, favorece su correcto funcionamiento.

Para el adecuado funcionamiento de las computadoras personales, necesitan de una fuente se alimentación eléctrica fiable, es decir, dentro de los parámetros correspondientes. Si se interrumpe inesperadamente la alimentación eléctrica o varia en forma significativa (fuera de los valores normales), las consecuencias pueden ser muy serias, tal como daño del HW y la información podría perderse.

La fuente de alimentación es un componente vital de los equipos de cómputo, y soportan la mayor parte de las anomalías del suministro eléctrico. Se ha identificado los siguientes problemas de energía mas frecuentes:

- Fallas de energía
- Transistores y pulsos
- Bajo voltaje
- Ruido electromagnético
- Distorsión
- Variación de frecuencia.

Para los cuales existen los siguientes dispositivos que protegen los equipos de estas anomalías:

- Supresores de picos
- Estabilizadores
- Sistemas de alimentación ininterrumpida (UPS)

Existen formas de prever estas fallas, con la finalidad de minimizar su impacto, entre ellas tenemos:

Tomas a Tierra o Puestas a Tierra

Se denomina así a la comunicación entre el circuito Eléctrico y el Suelo Natural para dar seguridad a las personas protegiéndolas de los peligros procedentes de una rotura del aislamiento eléctrico. Estas conexiones a tierra se hacen frecuentemente por medio de placas, varillas o tubos de cobre enterrados profundamente en tierra humedad, con o sin agregados de ciertos componentes de carbón vegetal, sal o elementos químicos, según especificaciones técnicas indicadas para las instalaciones eléctricas.

En la práctica protege de contactos accidentales las partes de una instalación no destinada a estar bajo tensión y para disipar sobretensiones de origen atmosférico o industrial.

La Toma a Tierra tiene las siguientes funciones principales: a) protege a las personas limitando la tensión que respecto a tierra puedan alcanzar las masas metálicas, b) protege a personas, equipos y materiales, asegurando la actuación de los dispositivos de protección como: pararrayos, descargadores eléctricos de líneas de energía o señal, así como interruptores diferenciales., c) facilitar el paso a tierra de las corrientes de defecto y de las descargas de origen atmosférico u otro.

Las inspecciones deben realizarse trimestralmente, con el fin de comprobar la resistencia y las conexiones. Es recomendable que esta labor se realice en los meses de verano o en tiempo de sequía. Es recomendable un mantenimiento preventivo anual dependiendo de las propiedades electroquímicas estables.

Fusibles

Al cablear la computadora, la carcaza normalmente se conecta a la tercera patilla del cable de alimentación. En algunos casos, puede que la tierra se conecte también al neutro. Si la electricidad fugara a través del aislante y llegase a la carcaza, esta derivación de electricidad aumentaría la intensidad de corriente que va por el circuito. Este incremento puede ser detectado por un fusible o un diferencial. Estos dos dispositivos están diseñados para interrumpir un circuito si se sobrecargan (un fusible se debe sustituir tras fundirse, un diferencial se debe restaurar tras saltar).

Si una parte de una computadora funde un fusible o hace saltar un diferencial, primero se debe desconectar el equipo. A continuación debe desconectarse el cable de alimentación que lleva al equipo y buscar la falla que ha hecho saltar el fusible. Arreglado el problema se puede a conectar el equipo.

Al sustituir los fusibles de una computadora, se ha de tener cuidado que todos los equipos deben estar apagados y desconectados antes de cambiar el fusible. No se debe olvidar que algunos elementos del equipo, como es el caso de los monitores, pueden mantener una carga de alto voltaje incluso, después de haberse apagado.

Asegurarse que el fusible de recambio es de la misma capacidad que el fundido. Por ejemplo si el fusible fundido viene marcando 2 amperios, no se debe sustituir por uno de 3 amperios. Un fusible de 3 amperios dejara pasar 1 amperio mas de la intensidad de lo que fijo el diseñador del equipo.

No aprobar las reparaciones de los fusibles, usando hilos de cobre o similares.

Extensiones eléctricas y capacidades

Las computadoras ocupan rápidamente toda la toma de corriente. Pocas oficinas se encuentran equipadas con las suficientes placas de pared. Dado que es necesario conectar además algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples. El uso de estas extensiones eléctricas debe ser controlado con cuidado.

No solo para que no queden a la vista, si no también porque suponen un peligro considerable para aquellos que tengan que pasar por encima. A parte del daño físico que puede provocar engancharse repentinamente con el cable, apaga de forma rápida un sistema completo.

Por razones de seguridad física y de trabajo se recomienda tener en cuenta las siguientes reglas:

Las extensiones eléctricas deben estar fuera de las zonas de paso, siempre que sea posible.

Utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso.

No se debe encadenar sucesivos múltiples, ya que esto puede hacer que pase mas corriente de la que los cables están diseñados para soportar. Se debe utilizar los enchufes de pared siempre que sea posible.

Si es posible, utilizar extensiones eléctricas que incluyan fusibles o diferenciales. Esto puede ayudar limitar el daño ante fallas eléctricas.

Se debe comprobar siempre la carga frente a las extensiones eléctricas. La mayor parte de ellas llevan los amperios que admite cada extensión, no debiendo superar esa cifra el amperaje total de todos los aparatos conectados a ellas.

Adquirir toma de corrientes de pared y/o extensiones eléctricas mixtas, capaces de trabajar con enchufes de espigas planas, como cilíndricas.

Tanto las tomas corrientes de pared como las extensiones eléctricas deben tener toma a tierra.

2.1.2.5. Clase de Riesgo: Equivocaciones

Grado de Negatividad:	Moderado
Frecuencia de Evento:	Periódico
Grado de Impacto:	Moderado
Grado de Certidumbre:	Probable

Situación actual	Acción correctiva
Las equivocaciones que se producen en forma rutinaria son de carácter involuntario.	Capacitación inicial en el ambiente de trabajo. Instruir al nuevo usuario con el Manual de Procedimientos
Cuando el usuario es practicante y tiene conocimientos de informática, tiene el impulso de navegar por los sistemas.	En lo posible se debe cortar estos accesos, limitando su accionar en función a su labor de rutina.
La falta de institucionalizar procedimientos produce vacíos y errores en la toma de criterios para registrar información.	Reuniones y Actas de Trabajo para fortalecer los procedimientos.
El CIT no recibe comunicación del personal de reemplazo por vacaciones por lo tanto supone que es la Oficina usuaria la que capacita al reemplazante.	Se debe informar al CIT del reemplazo para su registro y accesos a la Red y los Sistemas, por el tiempo que

	dure el reemplazo. Al término del periodo de reemplazo se restituye los valores originales a ambos usuarios.
Ante nuevas configuraciones se comunica a los usuarios sobre el manejo, claves, accesos y restricciones, tanto a nivel de Sistemas, Telefonía, Internet	Enviar oficios circulares múltiples comunicando los nuevos cambios y políticas. Convocar reuniones de capacitación antes nuevas opciones en los sistemas.

2.1.2.6. Clase de Riesgo: Acción de Virus Informático

Grado de Negatividad:	Muy Severo
Frecuencia de Evento:	Continuo
Grado de Impacto:	Grave
Grado de Certidumbre:	Probable

Situación actual	Acción correctiva
Se cuenta con un Software Antivirus corporativo. Pero no hay un contrato anual para su actualización.	Se cumple. Se debe evitar que las licencias no expiren, se requiere la renovación de contrato anualmente.
Todo Software (oficina, desarrollo, mantenimiento, drives, etc.) es manejado por personal de CIT, quienes son los encargados de su instalación en las PC's con su respectivo software corporativo.	Se cumple.
Se tiene un programa permanente de bloqueo acciones como cambiar configuraciones de red, acceso a los servidores, etc.	Se cumple a través de políticas de usuarios.
Se tiene instalado el antivirus de red y en estaciones de trabajo. Antes de logear una maquina a la red (dominio) se comprueba al existencia de virus en la PC.	Se cumple
El CIT no recibe comunicación del personal de reemplazo por vacaciones por lo tanto supone que es la Oficina usuaria la que capacita al reemplazante.	Se debe informar al CIT del reemplazo para registrarlo y darle los accesos permitidos a la Red y los Sistemas, por el tiempo que dure el reemplazo. Al término del periodo de reemplazo se restituye los valores originales a ambos usuarios.

En estos últimos años la acción del virus informático ha sido contrarrestada con la diversidad de productos que ofrece el mercado de software. Las firmas y/o corporaciones que proporcionan software antivirus, invierten mucho tiempo en recopilar y registrar virus, indicando en la mayoría de los casos sus características y el tipo de daño que puede provocar, por este motivo se requiere de una actualización periódica del software antivirus.

2.1.2.7. Clase de Riesgo: Fenómenos Naturales

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual	Acción correctiva
La ultima década no se han registrado contingencias debido a fenómenos naturales como: terremotos, inundaciones, aluviones, etc.	Medidas de prevención.
Potencialmente existe la probabilidad de sufrir inundaciones debido a lluvias que ocurren en épocas de verano.	Medidas de prevención.
Tenemos épocas fuertes lluvias (Fenómeno del Niño) que causas estragos en viviendas de material rustico. Las instalaciones de la UNP están adecuadamente protegidas, sin embargo se debe verificar el tema del suministro eléctrico.	Al ocurrir un corte de energía el personal de vigilancia deberá comunicar al personal del CIT, para desconectar el sistema de red de manera preventiva.
El ambiente donde se encuentra los Servidores principales, es apropiado ante las filtraciones.	Ubicación apropiada. Pero ante resultado de posibles filtraciones realizar trabajos de mantenimiento preventivo.

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en la sala de Computación Central, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico 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, dispositivos de almacenamiento, discos con información vital, todo ello como respaldo de aquellos que se encuentren aun en las instalaciones de la institución.

2.1.2.8. Clase de Riesgo: Accesos No Autorizados

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual	Acción correctiva
Se controla el acceso al Sistema de Red mediante la definición de "Cuenta" o "Login" con su respectiva clave	Se cumple
A cada usuario de Red se le asigna los "Atributos de confianza" para el manejo de archivos y acceso a los sistemas.	Se cumple
Cuando el personal cesa en sus funciones y/o es asignado a otra área, se le redefinen los accesos y autorizaciones, quedando sin efecto la primera.	Se cumple de modo extemporáneo, siendo lo indicado actualizar los accesos al momento de producirse el cese o cambio.
Se forman Grupos de usuarios, a los cuales se le asignan accesos por conjunto, mejorando la administración de los recursos	Se cumple
Se acostumbra a confiar la clave de acceso (uso personal) a compañeros de área, sin medir la implicación en el caso de acceso no autorizado. En algunos casos los usuarios escriben su contraseña (Red o de Sistemas) en sitios visibles.	Capacitar al personal sobre la confidencialidad de sus contraseñas, recalcando la responsabilidad e importancia que ello implica.
No se tiene un registro electrónico de Altas/Bajas de Usuarios, con las respectivas claves	Se debe implementar

Todos los usuarios sin excepción tienen un "login" o un nombre de cuenta de usuario y una clave de acceso a la red con un mínimo de cinco (5) dígitos. No se permiten claves en blanco. Además están registrados en un grupo de trabajo a través del cual se otorga los permisos debidamente asignados por el responsable de área.

Cada usuario es responsable de salir de su acceso cuando finalice su trabajo o utilizar un bloqueador de pantalla. Ello se aplica tanto a su autenticación como usuario de Red como usuario de Sistemas en la UNP, si lo tuviere.

2.1.2.9. Clase de Riesgo: Robo de Datos

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual	Acción correctiva
Las Oficinas tienen disponible disqueteras, quemadoras de CD/DVD, puertos USB, pero no se lleva un control sobre la información que ingresa y/o sale del ordenador.	Personal de Planta debe manejar información delicada de la Oficina.
El servicio de Internet es potencialmente una ventaja abierta para el robo de información electrónica	Existen políticas que regulan el uso y acceso del Servicio de Internet.
Los documentos impresos (informes, reportes, contratos, etc.) normalmente están expuestos al robo por que no se acostumbra guardarlos como debe ser. Si no se toma conciencia que esta es una manera de atentar contra el Sistema Informático del UNP el problema persistirá.	Resguardar la información en archivos. Destruir los reportes malogrados, sobre todo de contenido relevante. (existen papeleros que convierten el papel en picadillo).
El acceso a los terminales se controla, mediante claves de acceso, de esta manera se impide el robo de información electrónica. A través de las políticas se seguridad se impide el ingreso a los Servidores.	Se cumple parcialmente

El Robo de datos se puede llevarse a cabo bajo tres modalidades:

- La primera modalidad consiste en sacar “copia no autorizada” a nuestros archivos electrónicos aun medio magnético y retirarla fuera de la institución.
- La segunda modalidad y tal vez la mas sensible, es la sustracción de reportes impresos y/o informes confidenciales.
- La tercera modalidad es mediante acceso telefónico no autorizado, se remite vía Internet a direcciones de Correo que no corresponden a la Gestión Empresarial.

2.1.2.10. Clase de Riesgo: Manipulación y Sabotaje

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual	Acción correctiva
Existe el problema de la inestabilidad laboral, la misma que podría obligar a personas frustradas, o desilusionadas a causar daños físicos y lógicos en el sistema de información de la institución. Esto se puede traducir desde el registro de operaciones incorrectas por parte de los usuarios finales, hasta la operación de borrar registros en el sistema y conductas de sabotaje	La protección contra el sabotaje requiere: Una selección rigurosa del personal. Buena administración de los recursos humanos Buenos controles administrativos Buena seguridad física en los ambientes donde están los principales componentes del equipo. Asignar a una persona la responsabilidad de la protección de los equipos en cada área.
No se comunica el movimiento de personal al CIT, para restringir accesos del personal que es reubicado y/o cesado de la UNP.	Es conveniente la comunicación anticipada del personal que será reubicado y/o cesado con el objeto de retirar los derechos de operación de escritura para otorgarle los derechos de consulta antes de desactivar la cuenta.
Existe el antecedente de origen sabotaje interno. Como es el caso de trabajadores que han sido despedidos y/o están enterados que van a ser rescindidos su contrato, han destruidos o modificado archivos para su beneficio inmediato o futuro.	Hay que protegerse también ante una posible destrucción del hardware o software por parte de personal no honrado.

El peligro mas temido por los centros de Procesamiento de Datos, es el sabotaje. Instituciones que han intentado implementar Programas de Seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un trabajador o un sujeto ajeno a la propia institución. Un acceso no autorizado puede originar sabotajes.

Los riesgos y peligros deben ser identificados y evaluados, para conocer las posibles pérdidas y para que pueda ponerse en práctica los adecuados métodos de prevención.

Una mejora en la seguridad produce, a menudo, importantes beneficios secundarios. Por ejemplo, el cambio de metodología aplicada a determinadas operaciones conduce frecuentemente a una reducción del índice de errores, a una mejora en calidad, a una mejor planificación y a resultados más rápidos.

No existen un plan idóneo o una recomendación simple para resolver el problema de la seguridad. Realmente no es una situación estática u un problema “puntual”, sino que requiere un constante y continuo esfuerzo y dedicación.

Resumen de la Clase de Riesgos

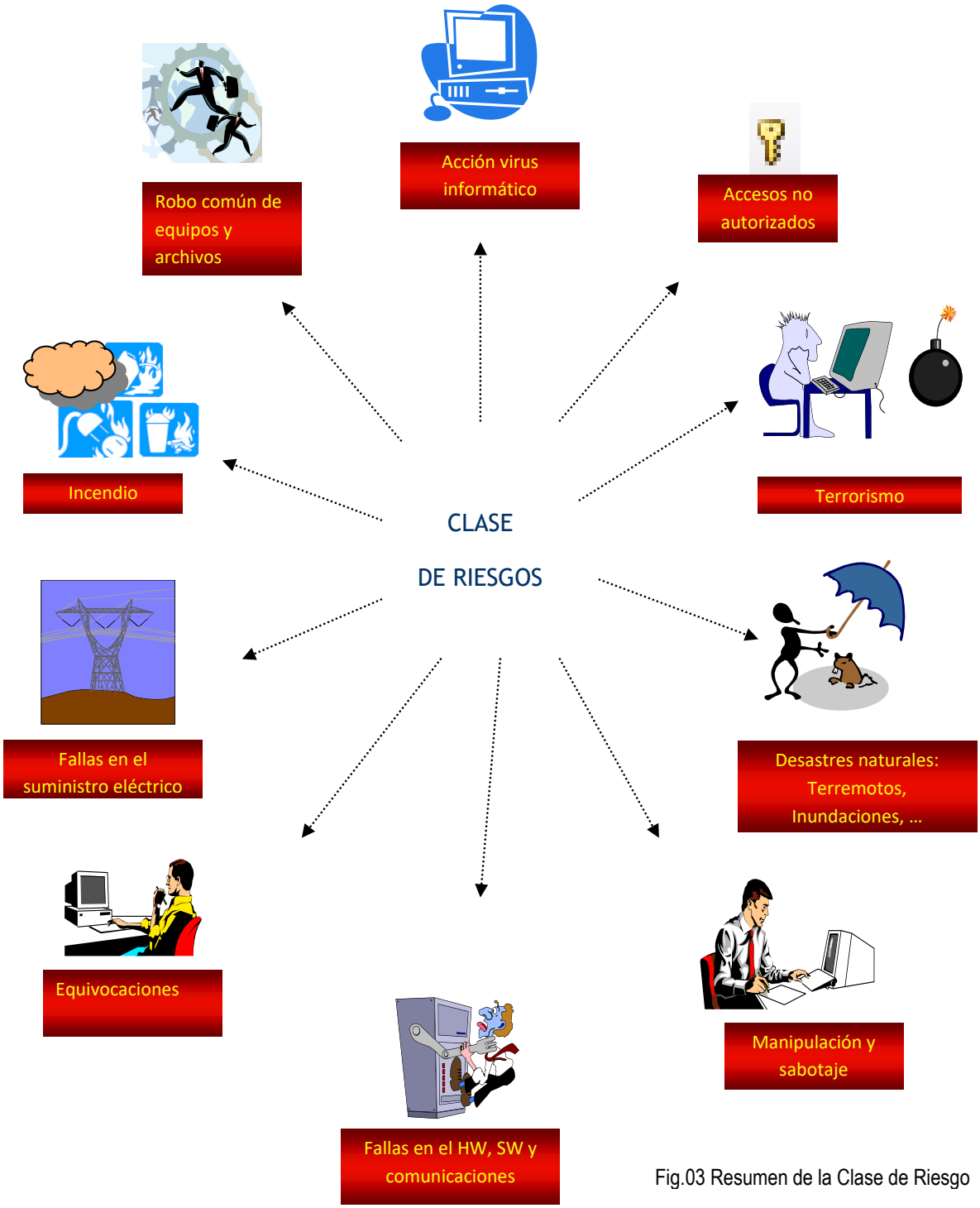


Fig.03 Resumen de la Clase de Riesgo

2.2. Análisis en las fallas en la Seguridad

En este se abarca el estudio del hardware, software, la ubicación física de la estación su utilización, con el objeto de identificar los posibles resquicios en la seguridad que pudieran suponer un peligro.

Las fallas en la seguridad de la información y por consiguiente de los equipos informáticos, es una cuestión que llega a afectar, incluso, a la vida privada de la persona, de ahí que resulte obvio el interés creciente sobre este aspecto. La seguridad de la información tiene dos aspectos importantes como:

- Negar el acceso a los datos a aquellas personas que no tengan derecho a ellos.
- Garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad de proteger los datos que se les ha confiado.

Por ejemplo, en el uso del Servicio Virtual Público de Red (VPN), implica una vía de acceso a la Red Central de UNP, la seguridad en este servicio es la validación de la clave de acceso.

2.3. Protecciones actuales

Se realizan las siguientes acciones:

- Se hace copias de los archivos que son vitales para la institución.
- Al robo común se cierran las puertas de entrada y ventanas
- Al vandalismo, se cierra la puerta de entrada.
- A la falla de los equipos, se realiza el mantenimiento de forma regular.
- Al daño por virus, todo el software que llega se analiza en un sistema utilizando software antivirus.
- A las equivocaciones, los empleados tienen buena formación. Cuando se requiere personal temporal se intenta conseguir a empleados debidamente preparados.
- A terremotos, no es posible proteger la instalación frente a estos fenómenos. El presente Plan de contingencias da pautas al respecto.
- Al acceso no autorizado, se cierra la puerta de entrada. Varias computadoras disponen de llave de bloqueo del teclado.
- Al robo de datos, se cierra la puerta principal y gavetas de escritorios. Varias computadoras disponen de llave de bloqueo del teclado.
- Al fuego, en la actualidad se encuentran instalados extintores, en sitios estratégicos y se brindara entrenamiento en el manejo de los extintores al personal, en forma periódica.

2.3.1. Seguridad de información

La Seguridad de información y por consiguiente de los equipos informáticos, es un tema que llega a afectar la imagen institucional de las empresas, incluso la vida privada de personas. Es obvio el interés creciente que día a días se evidencia sobre este aspecto de la nueva sociedad informática.

Ladrones, manipuladores, saboteadores, espías, etc. reconocen que el centro de cómputo de una institución es su nervio central, que normalmente tiene información confidencial y a menudo es vulnerable a cualquier ataque.

La Seguridad de información tiene tres directivas básicas que actúan sobre la Protección de Datos, las cuales ejercen control de:

- La lectura

  Consiste en negar el acceso a los datos a aquellas personas que no tengan derecho a ellos, al cual también se le puede llamar protección de la privacidad, si se trata de datos personales y mantenimiento de la seguridad en el caso de datos institucionales.

- La escritura

  Es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad que se les ha confiado.

- El empleo de esa información

  Es Secreto de logra cuando no existe acceso a todos los datos sin autorización. La privacidad se logra cuando los datos que puedan obtenerse no permiten el enlace a individuos específicos o no se pueden utilizar para imputar hechos acerca de ellos.

  Por otro lado, es importante definir los dispositivos de seguridad durante el diseño del sistema y no después. Los diseñadores de sistemas deben entender que las medidas de seguridad han llegado a se criterios de diseño tan importantes como otras posibilidades funcionales, así como el incremento de costos que significa agregar funciones, después de desarrollado un Sistema de Información.

2.3.1. 1. Acceso no autorizado

Sin adecuadas medidas de seguridad se puede producir accesos no autorizados:

- Control de acceso al CIT

  La libertad de acceso al CIT puede crear un significativo problema de seguridad. El acceso normal debe ser dado solamente a la gente que trabaja en esta oficina. Cualquier otra persona puede tener acceso únicamente bajo control.

Debemos mantener la seguridad física de la Oficina como primera línea de defensa. Para ello se toma en consideración el valor de los datos, el costo de protección, el impacto institucional por la perdida o daño de la información. La forma propuesta de implantar el Control de Acceso al CIT, seria la siguiente:

- Para personas visitantes, vigilancia otorgara el Credencial de Visitante.
- Para personal de la UNP, con autorización del encargado de la Oficina

- Acceso limitado computadoras personales y/o terminales de la red.

  Los terminales que son dejados sin protección pueden ser mal usados. Cualquier Terminal puede ser utilizado para tener acceso a los datos de un sistema controlado.

- Control de acceso a la información confidencial.

  Sin el debido control, cualquier usuario encontrara la forma de lograr acceso al Sistema de Red, a una base de datos o descubrir información clasificada. Para revertir la posibilidad de ataque se debe considerar:

Programas de control a los usuarios de red

El sistema Operativo residente en los servidores del CIT es Windows 2003 Server. A través del Servicio de "Active Directory" permite administrar a los usuarios y sus derechos de acceso, ya sea por grupos o individualmente.

Palabra de acceso (password)

Es una palabra o código que se ingresa por teclado antes que se realice un proceso.

Constituye un procedimiento de seguridad que protege los programas y datos contra los usuarios no autorizados. La identificación del usuario debe ser muy difícil de imitar y copiar.

El Sistema de Información debe cerrarse después que el usuario no autorizado falle tres veces de intentar ingresar una clave de acceso. Las claves de acceso no deben ser largas puesto que son más difíciles de recordar. Una vez que se obtiene la clave de acceso al sistema, esta se utiliza para entrar al sistema de Red de Información vía Sistema Operativo.

La forma común de intentar descubrir una clave es de dos maneras:

- Observando el ingreso de la clave
- Utilizando un método de ensayo y error para introducir posibles claves de acceso y lograr entrar.

En todo proceso corporativo es recomendable que el responsable de cada área asigne y actualice de forma periódica el "password" a los usuarios.

No se puede depender de un operador o responsable de terminal, que trabe la operatividad normal del UNP, por lo que será necesario establecer

el procedimiento para tener un duplicado de Claves de Acceso, bajo el esquema de niveles jerárquicos en sobre lacrado.

El administrador de Redes deberá entregar al Jefe del CIT, las claves de acceso de su personal en un sobre lacrado, debiendo registrar en un Cuaderno de Control, la fecha y motivo de algún cambio.

Niveles de Acceso

Las políticas de acceso aplicadas, deberá identificar los usuarios autorizados a emplear determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidas a la lectura o modificación en sus diferentes formas. Cada palabra clave deberá tener asignado uno de los niveles de acceso a la información o recursos de red disponibles en la UNP.

La forma fundamental de autoridad la tiene el Administrador de Redes con derechos totales. Entre otras funciones puede autorizar nuevos usuarios, otorgar derechos para modificar estructuras de las Bases de Datos, etc.

De acuerdo a ello se tienen los siguientes niveles de acceso a la información:

Nivel	Concepto
Consulta de la información	El privilegio de lectura esta disponible para cualquier usuario y solo se requiere presentaciones visuales o reportes. La autorización de lectura permite leer pero no modificar la Base de Datos.
Mantenimiento de información	Permite el acceso para agregar nuevos datos, pero no modifica los ya existentes, permite modificar pero no eliminar los datos. Para el borrado de datos, es preferible que sea responsabilidad del CIT.

2.3.1. 2. Destrucción

Sin adecuadas medidas de seguridad la institución puede estar a merced no solo de la destrucción de la información sino también de la destrucción de sus equipos informáticos. La destrucción de los equipos puede darse por una serie de desastres como son: incendios, inundaciones, sismos, posibles fallas eléctricas o sabotaje, etc.

Cuando se pierden los datos y no hay copias de seguridad, se tendrá que recrear archivos, bases de datos, documentos o trabajar sin ellos.

Esta comprobado que una gran parte del espacio en disco esta ocupado por archivos de naturaleza histórica, que es útil tener a mano pero no son importantes para el funcionamiento normal. Un ejemplo típico son las copias de la correspondencia conservados como documentos de referencia o plantilla. Si se guarda una copia de seguridad de estos archivos las consecuencias de organización pueden ser mínimas.

Los archivos Electrónicos Contable son de disposición diferente, ya que volver a crearlos puede necesitar de mucho tiempo y costo. Generalmente la institución recurre a esta información para la toma de decisiones.

Sin los datos al día, si el objetivo se vería seriamente afectado. Para evitar daños mayores se hacen copias de seguridad de la información vital para la institución y se almacenan en lugares apropiados (de preferencia en lugar externo a las instalaciones).

Hay que protegerse también ante una posible destrucción del hardware o software por parte del personal no honrado. Por ejemplo, hay casos en la que, trabajadores que han sido recientemente despedidos o están enterados que ellos van a ser cesados, han destruido o modificado archivos para su beneficio inmediato o futuro. Depende de los Jefes inmediatos de las áreas funcionales dar importancia a estos eventos, debiendo informar al Jefe del CIT para el control respectivo.

2.3.1. 3. Revelación o Deslealtad

La revelación o deslealtad es otra forma que utilizan los malos trabajadores para su propio beneficio. La información de carácter confidencial es vendida a personas ajenas a la institución. Para tratar de evitar este tipo de problemas se debe tener en cuenta lo siguiente:

- Control de uso de información en paquetes/ expedientes abiertos, cintas/disquetes y otros datos residuales. La información puede ser conocida por personal no autorizadas.

- Se deben tomar medidas para deshacerse del almacenaje secundario de información importante o negar el uso de esa a aquellas personas que pueden usar mal los datos residuales de estas.

- Mantener información impresa o magnética fuera del trayecto de la basura. El material de papel en la plataforma de descarga de la basura puede ser la fuente altamente sensitiva de recompensa para aquellos que esperan el recojo de la basura. Para tener una mayor seguridad de protección de la información residual y segregada, esta deberá ser destruida, eliminada físicamente, manualmente o mecánicamente (picadoras de papel).

- Preparar procedimientos de control para la distribución de información. Una manera de controlar la distribución y posible derivación de información, es mantener un rastro de copias múltiples indicando la confidencialidad o usando numeración como “pag 1 de 9”

Desafortunadamente, es muy común ver grandes volúmenes de información sensitiva tirada alrededor de la Oficinas y relativamente disponible a gran número de personas.

2.3.1. 4. Modificaciones

Hay que estar prevenido frente a la tendencia a asumir que “si viene de la computadora, debe ser correcto”.

La importancia de los datos modificados de forma ilícita, esta condicionada al grado en que la institución, depende de los datos para su funcionamiento y toma de dediciones. Esto podría disminuir su efecto su los datos procedente de las computadoras se verificaran antes de constituir fuente de información para la toma de decisiones.

Los elementos en la cual se han establecido procedimientos para controlar modificaciones ilícitas son:

- Los programas de aplicación: adicionalmente a proteger sus programas de aplicación como activos, es a menudo necesario establecer controles rígidos sobre las modificaciones a los programas, para estar seguros de que los cambios no causan daños accidentales o intencionales a los datos o a su uso no autorizado.

- La información en Bases de Datos: como medidas de Seguridad, para proteger los datos en el sistema, efectuar auditorias y pruebas de consistencia de datos en nuestros históricos. Particular atención debe ser dada al daño potencial que pueda efectuar un programador a través de una modificación no autorizada.

- Nuestra mejor protección contra la perdida/modificación de datos consiste en hacer copias de seguridad, almacenando en copias no autorizadas de todos los archivos valiosos en un lugar seguro.

- Los usuarios: los usuarios deben ser concientizados de la variedad de formas en que los datos pueden perderse o deteriorarse. Una campaña educativa de este tipo puede iniciarse con una reunión especial de los empleados, profundizarse con una serie de seminarios y reforzarse con carteles y circulares relacionados al tema.

Para la realización de las Copias de Seguridad se tiene que tomar algunas decisiones previas como:

- ¿Que soporte de copias de seguridad se va utilizar?

- ¿Se van a usar dispositivos especializados para copia de seguridad?

- ¿Con que frecuencia se deben realizar las copias de seguridad?

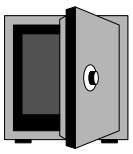
- ¿Cuales son los archivos a los que se le sacara copia de seguridad y donde se almacenara?

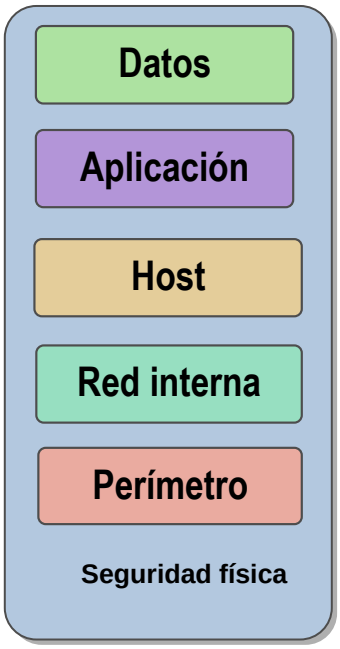
El CIT establecerá Directivas y/o Reglamentos en estas materias, para que los usuarios tomen conocimiento de sus responsabilidades. Tales reglas y normativas deben incorporarse en una campaña de capacitación educativa.

La institución debe tener en cuenta los siguientes puntos para la protección de los datos de una posible contingencia:

- Hacer de la copia de seguridad una política, no una opción.
- Hacer de la copia de seguridad resulte deseable.
- Facilitar la ejecución de la copia de seguridad (equipos adecuados, disponibilidad, suministros).
- Hacer de la copia de seguridad obligatoria.

Procedimientos para controlar modificaciones ilícitas





Física: Fenómenos naturales, fuego, temperatura, …

Instalaciones eléctricas y de datos

Acceso del personal, …

Software y Datos:

Copias de seguridad:

¿Dónde? ¿Cuándo? ¿Cuántas? ¿Tipos? …

Control de fuga de información

Acceso de usuarios:

Categorías, Niveles, …

para las: Aplicaciones, Internet, Correo, …

CAPITULO III: PLAN DE RECUPERACIÓN DEL DESASTRE Y RESPALDO DE LA INFORMACION

El costo de la Recuperación en caso de desastres severos, como los de un terremoto que destruya completamente el interior de edificios e instalaciones, estará directamente relacionado con el valor de los equipos de cómputo e información que no fueron informados oportunamente y actualizados en la relación de equipos informáticos asegurados que obra en poder de la compañía de seguros.

El Costo de Recuperación en caso de desastres de proporciones menos severos, como los de un terremoto de grado inferior a 07 o un incendio de controlable, estará dado por el valor no asegurado de equipos informáticos e información mas el Costo de Oportunidad, que significa, el costo del menor tiempo de recuperación estratégica, si se cuenta con parte de los equipos e información recuperados. Este plan de restablecimiento estratégico del sistema de red, software y equipos informáticos será abordado en la parte de Actividades Posteriores al desastre.

El paso inicial en el desarrollo del plan contra desastres, es la identificación de las personas que serán las responsables de crear el plan y coordinar las funciones. Típicamente las personas pueden ser: personal del CIT, personal de Seguridad.

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

- Actividades Previas al Desastre.
- Actividades Durante el Desastre.
- Actividades Después del Desastre.

3.1. Actividades previas al desastre

Se considera las actividades de planteamiento, preparación, entrenamiento y ejecución de actividades de resguardo de la información, que aseguraran un proceso de recuperación con el menor costo posible para la institución.

3.1.1. Establecimientos del Plan de Acción

En esta fase de planeamiento se establece los procedimientos relativos a:

a. Sistemas e Información.
b. Equipos de Cómputo.
c. Obtención y almacenamiento de los Respaldos de Información (BACKUPS).
d. Políticas (Normas y Procedimientos de Backups).

a. Sistemas de Información

La Institución deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los de desarrollo propio, como los desarrollados por empresas externas (detallada en el anexo V). Los *Sistemas y Servicios críticos* para la UNP, son los siguientes:

Lista de Sistemas

- Sistema Integrado de Administración Financiera (SIAF): Sistema de información asociado a la ejecución del presupuesto anual, de registro único de las operaciones de gastos e ingresos públicos. Lo operan la Oficina Central de Ejecución Presupuestaria.
- *Sistema Integrado de Gestión Académica*: Sistema de información que permite el registro y control de los Procesos académicos, permite al alumno realizar consultas académicas consulta vía WEB. Lo operan las Oficinas Académicas, y los órganos académicos-control.
- Sistema de Tramite Documentario: Sistema de información que permite el registro y seguimiento de los documentos. Lo operan todas las áreas funcionales.
- Sistema de Gestión Administrativa – Ingresos: Sistema de información que permite el registro y control de los ingresos. Lo operan todas las áreas funcionales Administrativas.
- Sistema de Abastecimientos: Sistema de información que permite el registro y control de las Órdenes de Trabajo, almacén. Lo opera la Oficina de Abastecimiento.
- Sistema de Control de Asistencia del personal: Lo opera la Oficina Central de Recursos Humanos.
- Sistema de Banco de Preguntas para la elaboración de Exámenes de admisión

Lista de Servicios

- Sistema de comunicaciones
- Servicio de correo corporativo
- Servicios Web: Publicación de páginas Web, noticias de la UNP, Inscripción comedor universitario, Inscripción de cursos.
- Internet, Intranet.
- Servicios Proxy
- VPN: servicios de acceso privado a la red de la Institución desde cualquier lugar.
- Servicio de Monitoreo de la red: monitorea los equipos de comunicación distribuidos en la red la UNP.
- Servicios de telefonía Principal: teléfonos IP
- Servicios de enseñanza de manera virtual.
- Servicio de Antivirus

b. Equipos de Computo

Se debe tener en cuenta el catastro de Hardware, impresoras, lectoras, scanner, ploters, modems, fax y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional).

Se debe emplear los siguientes criterios sobre identificación y protección de equipos:

- Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.
- Señalización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación. Por ejemplo etiquetar de color rojo los servidores, color amarillo a los PC con información importante o estratégica, y color verde a las demás estaciones (normales, sin disco duro o sin uso).
- Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la institución.

c. Obtención y almacenamiento de Copias de Seguridad (Backups)

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas en la institución. Las copias de seguridad son las siguientes:

- Backup del Sistema Operativo: o de todas las versiones de sistema operativo instalados en la Red.
- Backup de Software Base: (Lenguajes de Programación utilizados en el desarrollo de los aplicativos institucionales).
- Backup del software aplicativo: backups de los programas fuente y los programas ejecutables.
- Backups de los datos (Base de datos, passsword y todo archivo necesario para la correcta ejecución del software aplicativos de la institución).
- Backups del Hardware, se puede implementar bajo dos modalidades:

  Modalidad Externa: mediante el convenio con otra institución que tenga equipos similares o mejores y que brinden la capacidad y seguridad de procesar nuestra información y ser puestos a nuestra disposición al ocurrir una continencia mientras se busca una solución definitiva al siniestro producido.

  En este Caso se debe definir claramente las condiciones del convenio a efectos de determinar la cantidad de equipos, periodos de tiempo, ambientes, etc., que se puede realizar con la entidad que cuente con equipo u mantenga un Plan de Seguridad de Hardware.

  Modalidad Interna: si se dispone de mas de un local, en ambos se debe tener señalado los equipos, que por sus capacidades técnicas son susceptibles de ser usados como equipos de emergencia.

Es importante mencionar que en ambos casos se debe probar y asegurar que los procesos de restauración de información posibiliten el funcionamiento adecuado de los sistemas.

d. Políticas (Normas y Procedimientos)

Se debe establecer procedimientos, normas y determinación de responsabilidades en la obtención de los "Backups" o Copias de Seguridad. Se debe considerar:

- Periodicidad de cada tipo de backup: los backups de los sistemas informáticos se realizan de manera diferente:
  - ⇒ Sistema Integrado de Gestión Académico: en los procesos académicos de Inscripción de curso y registro de Actas se realiza backup diario, para los demás periodos se realiza el backup semanal.
  - ⇒ Sistema de Ingresos: backup diario
  - ⇒ Sistema Integrado de Administración Financiera (SIAF): backup semanal
  - ⇒ Sistema de Tramite Documentario: backup diario.
  - ⇒ Sistema de Abastecimientos: backup semanal
  - ⇒ Sistema de Control de Asistencia del personal: backup semanal.
  - ⇒ Sistema de Banco de Preguntas: backup periodo examen.
- Respaldo de información de movimiento entre los periodos que no se sacan backups: días no laborales, feriados, etc. en estos días es posible programar un backup automático.
- Uso obligatorio de un formulario de control de ejecución del programa de backups diarios, semanales y mensuales: es un control a implementar, de tal manera de llevar un registro diario de los resultados de las operaciones del backups realizados y su respectivo almacenamiento.
- Almacenamiento de los backups en condiciones ambientales optimas, dependiendo del medio magnético empleando.
- Reemplazo de los backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar. No se realiza reemplazos pero se realiza copias de las mismas, considerando que no se puede determinar exactamente el periodo de vida útil del dispositivo donde se ha realizado el backup.
- Almacenamiento de los backups en locales diferentes donde reside la información primaria (evitando la pérdida si el desastre alcanzo todo el edificio o local). Esta norma se cumple con la información histórica, es decir se tiene distribuidos los backups de la siguiente manera: una copia reside en las instalaciones del CIT, y una segunda copia reside en la Oficina que genera la información (OCRCA, OCEP, OCARH).
- Pruebas periódicas de los backups (Restore), verificando su funcionalidad, a través de los sistemas comparando contra resultados anteriormente confiables. Esta actividad se realizara haciendo una comparación entre el contenido de la

primera y segunda copia realizada o con el contenido de la información que se encuentra el Servidor de información histórica.

3.1.2. Formación de equipos operativos

En cada unidad operativa, que almacene información y sirva para la operatividad institucional, se deberá designar un responsable de la seguridad de la información de su unidad. Pudiendo ser el Jefe Administrativo de dicha Área, sus funciones serán las siguientes:

- Contactarse con los autores de las aplicaciones y personal de mantenimiento respectivo.

  El equipo encargado en el CIT- UNP, esta formado por las siguientes unidades:

  - Unidad de Telecomunicaciones
  - Unidad de Soporte Tecnológico.
  - Unidad de Administración de Servidores.
  - Unidad de Desarrollo Tecnológico.
  - Unidad Académica.

- Proporcionar las facilidades (procedimientos, técnicas) para realizar copias de respaldo.

  Esta actividad esta dirigida por el Equipo de Soporte y Mantenimiento.

- Supervisar el procedimiento de respaldo y restauración
- Establecer procedimientos de seguridad en los sitios de recuperación
- Organizar la prueba de hardware y software: el encargado y el usuario final dan su conformidad.
- Ejecutar trabajos de recuperación y comprobación de datos.
- Participar en las pruebas y simulacros de desastres: en esta actividad deben participar el encargado de la ejecución de actividades operativas, y los servidores administrativos del área, en el cumplimiento de actividades preventivas al desastre del Plan de Contingencias.

3.1.3. Formación de Equipos de Evaluación (Auditoria de cumplimiento de los procesos de seguridad)

Esta función debe ser realizada preferentemente por el personal de auditoria o inspectora, de no se posible, lo realizaría el personal del área de informática-CIT, debiendo establecerse claramente sus funciones, responsabilidades y objetivos:

- Revisar que las normas y procedimientos con respecto a backups, seguridad de equipos y data se cumpla.

- Supervisar la realización periódica de los backups, por parte de los equipos operativos, es decir, información generada en el área funcional, software general y hardware.
- Revisar la correlación entre la relación de los Sistemas e información necesarios para la buena marcha de la institución y los backups realizados.
- Informar de los cumplimientos e incumplimientos de las normas para las acciones de corrección necesarias.

3.2. Actividades durante el Desastre

Presentada la contingencia o desastre se debe ejecutar las siguientes actividades planificadas previamente:

a. Plan de Emergencias

b. Formación de Equipos

c. Entrenamiento

a. Plan de Emergencias

La presente etapa incluye las actividades a realizar durante el desastre o siniestros, se debe tener en cuenta la probabilidad de su ocurrencia durante: el día, noche o madrugada. Este plan debe incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro. Solo se debe realizar acciones de resguardo de equipos en los casos en que no se pone en riesgo la vida de personas.

Normalmente durante la acción del siniestro es difícil que las personas puedan afrontar esta situación, debido a que no están preparadas o no cuentan con los elementos de seguridad, por lo que las actividades para esta etapa del proyecto de prevención de desastres deben estar dedicados a *buscar ayuda inmediatamente* para evitar que la acción del siniestro causen mas daños o destrucciones. Se debe tener en toda Oficina los números de teléfono y direcciones de organismos e instituciones de ayuda. Todo el personal debe conocer lo siguiente:

- Localización de vías de Escape o Salida: Las vías de escape o salida para solicitar apoyo o enviar mensajes de alerta, a cada oficina debe señalizar las vías de escape
- Plan de Evaluación Personal: el personal ha recibido periódicamente instrucciones para evacuación ante sismos, a través de simulacros, esto se realiza acorde a los programas de seguridad organizadas por Defensa Civil a nivel local. Esa actividad se realizara utilizando las vías de escape mencionadas en el punto anterior.
- Ubicación y señalización de los elementos contra el siniestro: tales como los extintores, las zonas de seguridad que se encuentran señalizadas (ubicadas normalmente en las columnas), donde el símbolo se muestra en color blanco con fondo verde. De existir un repintado de paredes deberá contemplarse la reposición de estas señales.

- Secuencia de llamadas en caso de siniestro: tener a la mano elementos de iluminación, lista de teléfonos de instituciones como: Compañía de Bomberos, Hospitales, Centros de Salud, Ambulancias, Seguridad.

b. Formación de Equipos

Se debe establecer los equipos de trabajo, con funciones claramente definidas que deberán realizar en caso de desastre. En caso de que el siniestro lo permita (al estar en un inicio o estar en un área cercana, etc.), se debe formar 02 equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y el otro para salvamento de los equipos informáticos, de acuerdo a los lineamientos o clasificación de prioridades.

c. Entrenamiento

Se debe establecer un programa de practicas periódicas con la participación de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo a los roles que se hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se pueden realizar recarga de extintores, charlas de los proveedores, etc.

Es importante lograr que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir; y tomen con seriedad y responsabilidad estos entrenamientos; para estos efectos es conveniente que participen los Directivos y Ejecutivos, dando el ejemplo de la importancia que la Alta Dirección otorga a la Seguridad Institucional.

3.3. Actividades después del desastre

Estas actividades se deben realizar inmediatamente después de ocurrido el siniestro, son las siguientes:

a. Evaluación de Daños.
b. Priorización de Actividades del Plan de Acción.
c. Ejecución de Actividades.
d. Evaluación de Resultados.
e. Retroalimentación del Plan de Acción.

a. Evaluación de daños

El objetivo es evaluar la magnitud del daño producido, es decir, que sistemas se están afectando, que equipos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo.

En el caso de la UNP se debe atender los procesos de contabilidad, tesorería, administrativo-académicos, documentarios; que son las actividades que no podrían dejar de funcionar, por la importancia estratégica. La recuperación y puesta en marcha de los servidores que alojan dichos sistemas, es prioritario.

b. Priorizar Actividades del Plan de Acción

La evaluación de los daños reales nos dará una lista de las actividades que debemos realizar, preponderando las actividades estratégicas y urgentes de nuestra institución. Las actividades comprenden la recuperación y puesta en marcha de los equipos de cómputo ponderado y los Sistemas de Información, compra de accesorios dañados, etc.

c. Ejecución de actividades

La ejecución de actividades implica la creación de equipos de trabajo para realizar actividades previamente planificadas en el Plan de Acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar el avance de los trabajos de recuperación y, en caso de producirse un problema, reportarlo de inmediato a la Jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas:

- La primera la restauración del servicio usando los recursos de la institución o local de respaldo.
- La segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta ultima etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución y el buen servicio de nuestro sistema e Imagen Institucional.

d. Evaluación de Resultados

Una vez concluidas las labores de Recuperación de los sistemas que fueron afectado por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, con que eficacia se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del Plan de Acción, como se comportaron los equipos de trabajo, etc.

De la evaluación de resultados y del siniestro, deberían de obtenerse dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencias y Seguridad de Información, y otra una lista de recomendaciones para minimizar los riesgos y perdida que ocasionaron el siniestro.

e. Retroalimentación del Plan de Acción

Con la evaluación de resultados, debemos de optimizar el Plan de Acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionan adecuadamente.

El otro elemento es evaluar cual hubiera sido el costo de no contar con el Plan de Contingencias en la institución.

3.3.6. Acciones frente a los tipos de riesgo.

3.3.1.1. Clase de Riesgo: Incendio o Fuego.

Cuando el daño del edificio ha sido mayor, evaluar el traslado a un nuevo local, hasta considerar la posibilidad del traslado. El procedimiento de respuesta a esta emergencia se ve en la figura A1.

Cuando el daño ha sido menor:

a) Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable encargado de Soporte y Mantenimiento

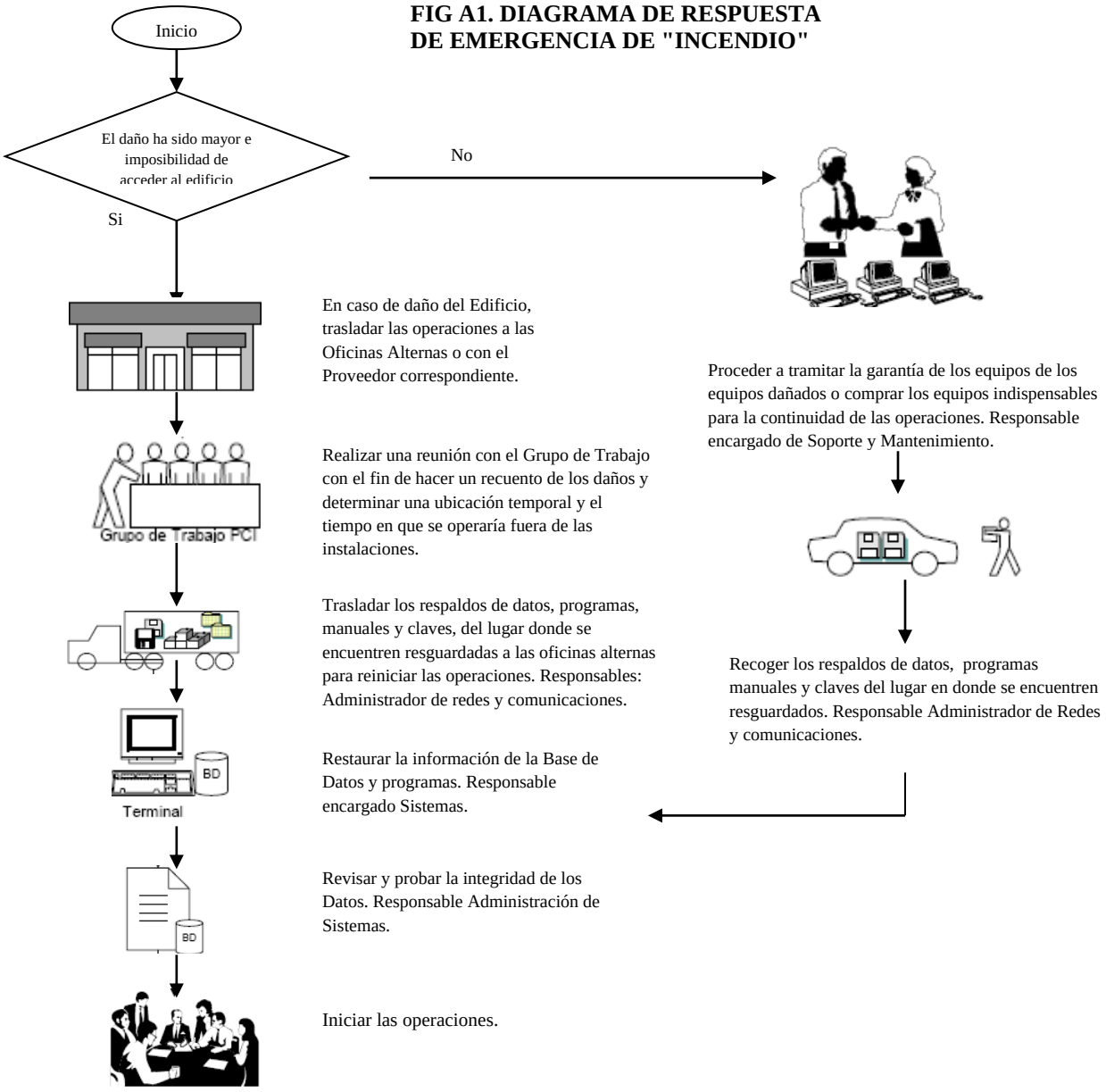
b) Se recoge los respaldos de datos, programas, manuales y claves. Responsable encargado de Redes.

c) Instalar el sistema operativo. Responsable encargado de Soporte y Mantenimiento

d) Restaurar la información de las bases de datos y programas. Responsable encargado de Desarrollo.

e) Revisar y probar la integridad de los datos. Responsable encargado de Desarrollo.

FIG A1. DIAGRAMA DE RESPUESTA DE EMERGENCIA DE "INCENDIO"



¿QUE HACER? Antes, Durante y Después de un INCENDIO.

ANTES:

- Verificar periódicamente que las instalaciones eléctricas estén en perfecto estado.
- No concentrar grandes cantidades de papel, ni fumar cerca de químicos o sustancias volátiles.
- Verificar las condiciones de extintores e hidratantes y capacitar para su manejo.
- Si se fuma, procurar no arrojar las colillas a los cestos de basura, verificar que se hayan apagado bien los cigarrillos y no dejarlos en cualquier sitio, utilizar ceniceros.
- No almacenar sustancias y productos inflamables.
- No realizar demasiadas conexiones en contactos múltiples, evitar la sobrecarga de circuitos eléctricos.
- Por ningún motivo mojar las instalaciones eléctricas, recordar que el agua es un buen conductor de la electricidad.
- Si se detecta cualquier anomalía en los equipos de seguridad (extintores, hidratantes, equipo de protección personal, etc.) y en las instalaciones eléctricas, reportar de inmediato a Seguridad.
- Mantener siempre el área de trabajo limpia y en orden, ya que no hacerlo es una de las causas que provocan incendios.
- Tener a la mano los números telefónicos de emergencia.
- Portar siempre el fotocheck de identificación.

DURANTE

- Ante todo se recomienda conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.
- En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Computador Principal, se deberá (si el tiempo lo permite) "Salir de Red y Apagar Computador": Down en el (los) servidor(es), apagar (OFF) en la caja principal de corriente del CIT.
- Si se conoce sobre el manejo de extintores, intenta sofocar el fuego, si este es considerable no trates de extinguirlo con los propios medios, solicitar ayuda.
- Si el fuego esta fuera de control, realizar evacuación del inmueble, siguiendo las indicaciones del Personal de bomberos.
- No utilizar elevadores, descender por las escaleras pegado a la pared que es donde posee mayor resistencia, recuerda: No gritar, No empujar, No correr y dirigirse a la zona de seguridad.
- Si hay humo donde nos encontramos y no podemos salir, mantenernos al ras del piso, cubriendo tu boca y nariz con un pañuelo bien mojado y respira a través de el, intenta el traslado a pisos superiores.
- Las personas que se encuentren en los últimos pisos, deberán abrir ventanas para que el humo tenga una vía de salida y se descongestionen las escaleras.
- Si es posible mojar la ropa.
- Verifica si las puertas están calientes antes de abrirlas, si lo están, busca otra salida.

DESPUES

- Retirarse inmediatamente del área incendiada y ubícate en la zona de seguridad externa que te corresponda.
- No obstruir las labores del personal especializado, dejar que los profesionales se encarguen de sofocar el incendio.
- El personal calificado realizara una verificación física del inmueble y definirá si esa en condiciones de ser utilizado normalmente.
- Colaborar con las autoridades.

3.3.1.2. Clase de Riesgo: Robo común de equipos y archivos.

Analizar las siguientes situaciones:

- En qué tipo de vecindario se encuentra la Institución
- Las computadoras se ven desde la calle
- Hay personal de seguridad en la Institución y están ubicados en zonas estratégicas
- Cuánto valor tienen actualmente las Bases de Datos
- Cuánta pérdida podría causar en caso de que se hicieran públicas
- Asegurarse que el personal es de confianza, competente y conoce los procedimientos de seguridad.
- Trabajo no supervisado, especialmente durante el turno de noche, malas técnicas de contratación, evaluación y de despido de personal.

3.3.1.3. Clase de Riesgo: Vandalismo.

- Si el intento de vandalismo es mayor, se presenta un grave riesgo dentro del área del Centro de Cómputo ya que puede dañar los dispositivos perdiendo toda la información y por consecuencia las actividades se verían afectadas en su totalidad, así como el servicio proporcionado.
- A continuación se menciona una serie de medidas preventivas:
  - Establecer vigilancia mediante cámaras de seguridad en el Site, el cual registre todos los movimientos de entrada del personal.
  - Instalar identificadores mediante tarjetas de acceso.
  - Determinar lugares especiales, fuera del centro de datos, para almacenar los medios magnéticos de respaldo y copia de la documentación de referencia y procedimientos de respaldo y recuperación (se puede contratar una caja de seguridad bancaria donde se custodiaran los datos e información crítica).
- Los principales conflictos que pudieran presentarse son:
  - En cuanto a la red, si el sistema llegará a presentar una falla no habría personal que atendiera la problemática y por consecuencia se detendrían las operaciones a falta del monitoreo a los distintos sistemas.
  - Respecto a los dispositivos de almacenamiento, si se mantienen los respaldos únicamente dentro de la Delegación Miguel Hidalgo, sería imposible reanudar las actividades que un momento dado fueran críticas, como la nómina, contabilidad, etc; en un sitio alterno, ya que no contarían con copia de la información.

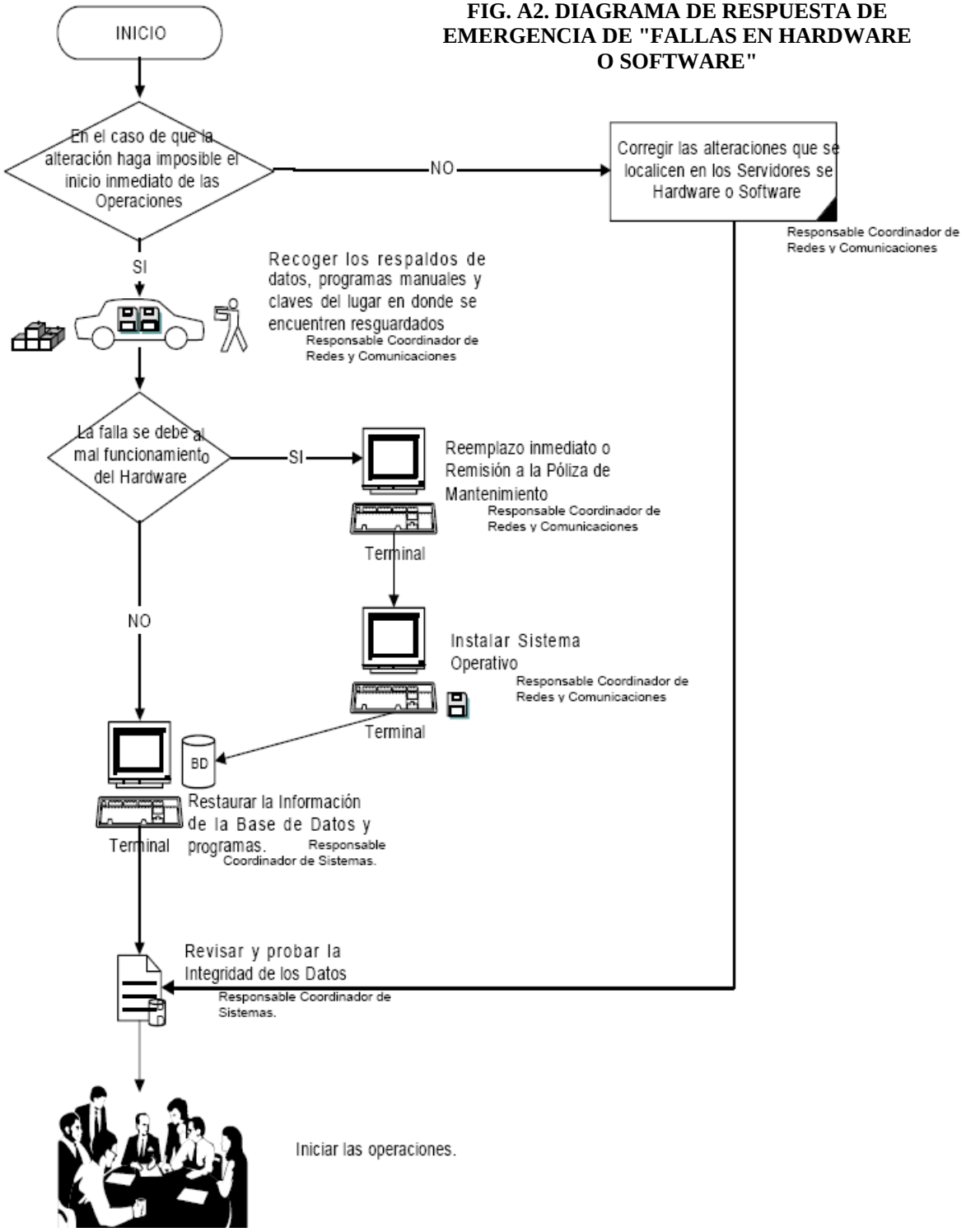
3.3.1.4. Clase de Riesgo: Equivocaciones.

- Cuánto saben los empleados de computadoras o redes.
- Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?
- Difusión de Manuales de Usuario y operación del correcto uso del software y el hardware a todo el personal que labora de manera directa con los equipos informáticos.

3.3.1.5. Clase de Riesgo: Fallas en los equipos.

Las fallas del sistema de red pueden deberse al mal funcionamiento de los equipos ó a la pérdida de configuración de los mismos por lo que se deben evaluar las fallas para determinar si estas se derivan del mal funcionamiento de un equipo ó de la pérdida de su configuración. El procedimiento de respuesta a esta emergencia se ve en la figura A2.

FIG. A2. DIAGRAMA DE RESPUESTA DE EMERGENCIA DE "FALLAS EN HARDWARE O SOFTWARE"



Casos

- **Error Físico de Disco de un Servidor (Sin RAID).**
  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 teléfono a 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, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
  7. Verificación el buen estado de los sistemas.
  8. Habilitar las entradas al sistema para los usuarios.

- **Error de Memoria RAM y Tarjeta(s) Controladora(s) de Disco**
  En el caso de las memorias RAM, se dan los siguientes síntomas:
  - El servidor no responde correctamente, por lentitud de proceso o no rendir ante el ingreso masivo de usuarios.
  - Ante procesos mayores se congela el proceso.
  - Arroja errores con mapas de direcciones hexadecimales.
  - Es recomendable que el servidor cuente con ECC (error correct checking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.

  Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la compañía, a menos que la dificultad apremie, cambiarlo inmediatamente.

  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, utilizar mensajes por red y teléfono a jefes de área.
  2. El servidor debe estar apagado, dando un correcto apagado del sistema.
  3. Ubicar las memorias malogradas.
  4. Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
  5. Retirar la conexión del servidor con el concentrador, 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.

3.3.1.6. Clase de Riesgo: Acción de Virus Informático.

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidor:

- Se contará con antivirus para el sistema; aislar el virus para su futura investigación.
- El antivirus muestra el nombre del archivo infectado y quién lo usó.
- Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras fuera de red:

- Utilizar los discos de instalación que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado.
- Insertar el disco de instalación antivirus, luego instalar el sistema operativo, de tal forma que revise todos los archivos y no sólo los ejecutables. De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, recomendará borrar el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del Scaneado. Finalizado el scaneado, reconstruir el Master Boot del disco duro.

3.3.1.7. Clase de Riesgo: Accesos No Autorizados.

Enfatiza los temas de:

- **Contraseñas.** Las contraseñas son a menudo, fáciles de adivinar u obtener mediante ensayos repetidos. Debiendo implementarse un número máximo (3) de intentos infructuosos. El CIT implementa la complejidad en sus contraseñas de tal forma que sean mas de siete caracteres y consistentes en números y letras.

- **Entrampamiento al intruso.** Los sistemas deben contener mecanismos de entrampamiento para atraer al intruso inexperto. Es una buena primera línea de detección, pero muchos sistemas tienen trampas inadecuadas.

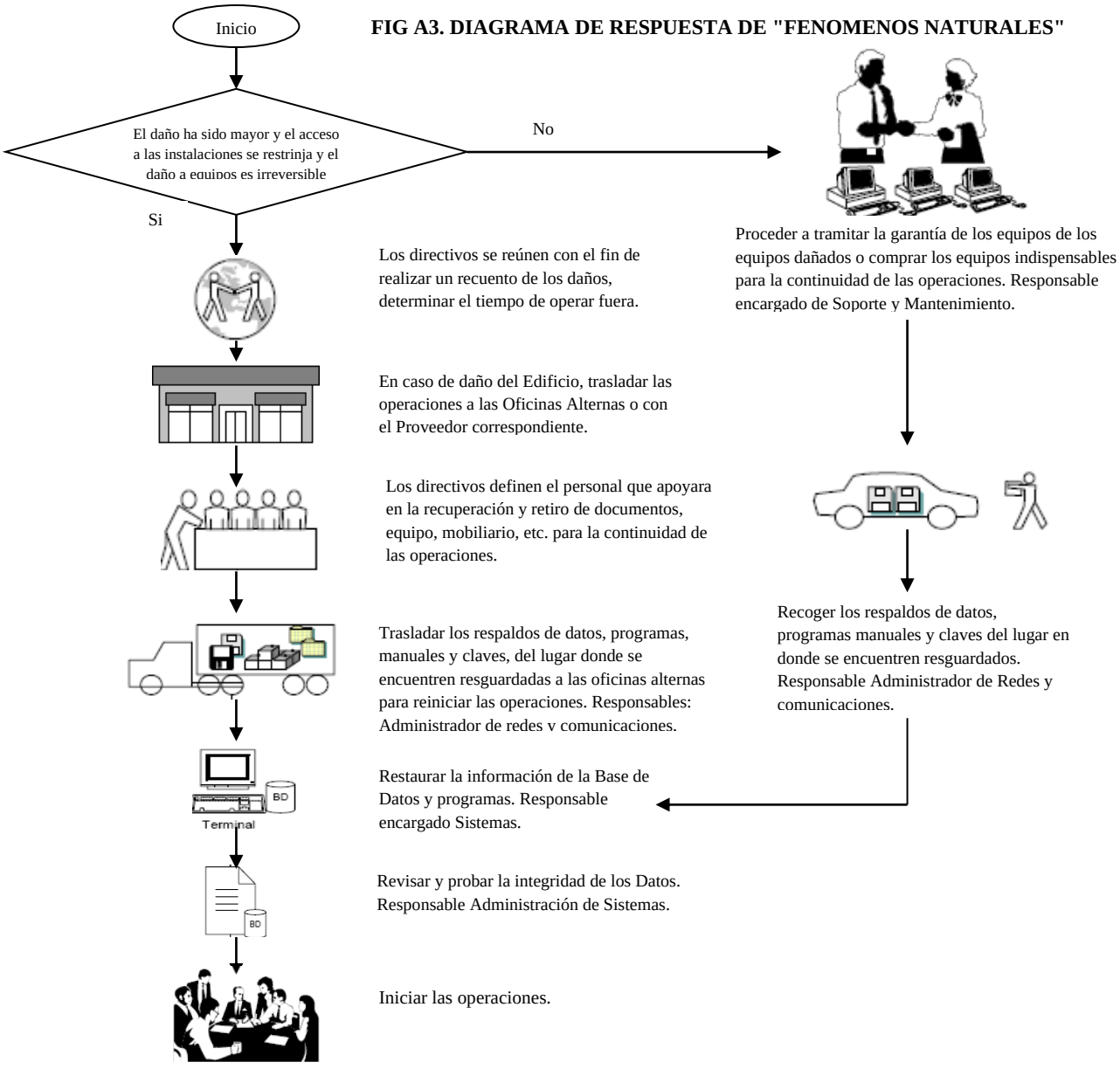
- **Privilegio.** En los sistemas informáticos de la UNP, cada usuario se le presenta la información que le corresponde. Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Estas se deben proteger con cuidado. Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella, e incluso imprimirla. Por supuesto, una red deja de ser eficiente si se convierte en una fortaleza inaccesible. En este punto el administrador de la red ha clasificado a los usuarios de la red en “Grupos” con el objeto de adjudicarles el nivel de seguridad y perfil adecuado.

3.3.1.8. Clase de Riesgo: Fenómenos naturales.

a) Terremoto e Inundación

- Para evitar problemas con inundaciones ubicar los servidores a un promedio de 50 cm de altura.
- En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.
- Cuando el daño del edificio ha sido mayor, evaluar el traslado a un nuevo local, hasta considerar la posibilidad del traslado.
- Cuando el daño ha sido menor se procede:
  a) Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable encargado de Soporte y Mantenimiento
  b) Recoger los respaldos de datos, programas, manuales y claves. Responsable encargado de Redes.
  c) Instalar el sistema operativo. Responsable encargado de Soporte y Mantenimiento
  d) Restaurar la información de las bases de datos y programas. Responsable encargado de Desarrollo.
  e) Revisar y probar la integridad de los datos. Responsable encargado de Desarrollo.

FIG A3. DIAGRAMA DE RESPUESTA DE "FENOMENOS NATURALES"



3.3.1.9. Clase de Riesgo: Robo de Datos.

Se previene a través de las siguientes acciones:

- **Acceso no Autorizado:** Sin adecuadas medidas de seguridad se puede producir accesos no autorizados a:
  - Área de Sistemas.
  - Computadoras personales y/o terminales de la red.
  - Información confidencial.
- **Control de acceso al Área de Sistemas:** El acceso al área de Informática estará restringido:
  - Sólo ingresan al área el personal que trabaja en el área.
  - El ingreso de personas extrañas solo podrá ser bajo una autorización.
- **Acceso Limitado a los Terminales:** Cualquier terminal que puede ser utilizado como acceso a los datos de un Sistema, las siguientes restricciones pueden ser aplicadas:
  - Determinación de los períodos de tiempo para los usuarios o las terminales.
  - Designación del usuario por terminal.
  - Limitación del uso de programas para usuario o terminales.
  - Límite de tentativas para la verificación del usuario, tiempo de validez de las señas, uso de contraseñas, cuando un terminal no sea usado pasado un tiempo predeterminado (5 - 10 minutos).
- **Niveles de Acceso:** Los programas de control de acceso deberán identificar a los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidos a la lectura o modificación en sus diferentes formas.
  - Nivel de consulta de la información.- privilegio de lectura.
  - Nivel de mantenimiento de la información.- El concepto de mantenimiento de la información consiste en: Ingreso, Actualización, Borrado.

3.3.1.10. Clase de Riesgo: Manipulación y Sabotaje.

- La protección contra el sabotaje requiere:
  1. Una selección rigurosa del personal.
  2. Buena administración de los recursos humanos.
  3. Buenos controles administrativos.
  4. Buena seguridad física en los ambientes donde están los principales componentes del equipo.
  5. Asignar a una persona la responsabilidad de la protección de los equipos en cada área.

- A continuaciones algunas medidas que se deben tener en cuenta para evitar acciones hostiles:
  1. Mantener una buena relación de trabajo con el departamento de policía local.
  2. Mantener adecuados archivos de reserva (backups).
  3. Planear para probar los respaldos (backups) de los servicios de procesamiento de datos.
  4. Identificar y establecer operaciones criticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otras actividades.
  5. Usar rastros de auditorias o registros cronológicos (logs) de transacción como medida de seguridad.

- Cuando la información eliminada se pueda volver a capturar, se procede con lo siguiente:
  - Capturar los datos faltantes en las bases de datos de los sistemas. Responsable: Áreas afectadas
  - Revisar y probar la integridad de los datos. Responsable: Desarrollo de Sistemas.

La eliminación de la información, puede volverse a capturar en la mayoría de los casos, sin embargo en algunas ocasiones, las pérdidas demandan demasiado tiempo requerido para el inicio de las operaciones normales, por tal motivo es recomendable acudir a los respaldos de información y restaurar los datos pertinentes, de esta forma las operaciones del día no se verían afectados.

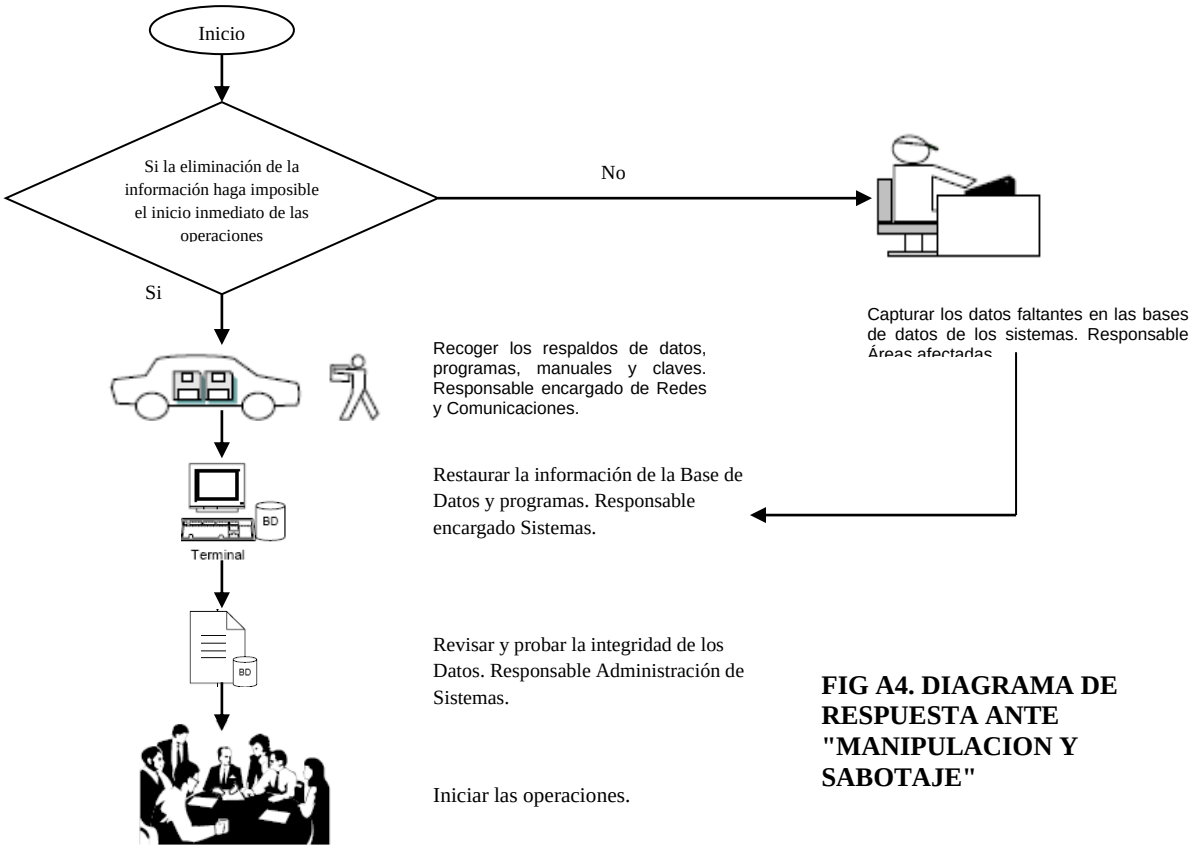


FIG A4. DIAGRAMA DE RESPUESTA ANTE "MANIPULACION Y SABOTAJE"

CONCLUSIONES

- El presente Plan de contingencias y Seguridad en Información de la UNP, tiene como fundamental objetivo el salvaguardar la infraestructura de la Red y Sistemas de Información extremando las medidas de seguridad para protegernos y estar preparados a una contingencia de cualquier tipo.

- Las principales actividades requeridas para la implementación del Plan de Contingencia son: Identificación de riesgos, Evaluación de riesgos, Asignación de prioridades a las aplicaciones, Establecimiento de los requerimientos de recuperación, Elaboración de la documentación, Verificación e implementación del plan, Distribución y mantenimiento del plan.

- Un Plan de Contingencia es la herramienta que la institución debe tener, para desarrollar la habilidad y los medios de sobrevivir y mantener sus operaciones, en caso de que un evento fuera de su alcance le pudiera ocasionar una interrupción parcial o total en sus funciones. Las políticas con respecto a la recuperación de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.

- No existe un plan único para todas las organizaciones, esto depende de la infraestructura física y las funciones que realiza en Centro de Procesamiento de Datos mas conocido como Centro de Cómputo.

- Lo único que realmente permite a la institución reaccionar adecuadamente ante procesos críticos, es mediante la elaboración, prueba y mantenimiento de un Plan de Contingencia.

RECOMENDACIONES

- Programar las actividades propuestas en el presente Plan de Contingencias y Seguridad de Información.

- Hacer de conocimiento general el contenido del presente Plan de Contingencias y Seguridad de Información, con la finalidad de instruir adecuadamente al personal de la UNP.

- Adicionalmente al plan de contingencias se debe desarrollar reglas de control y pruebas para verificar la efectividad de las acciones en caso de la ocurrencia de los problemas y tener la seguridad de que se cuenta con un método seguro.

- Se debe tener una adecuada seguridad orientada a proteger todos los recursos informáticos desde el dato más simple hasta lo más valioso que es el talento humano; pero no se puede caer en excesos diseñando tantos controles y medidas que desvirtúen el propio sentido de la seguridad, por consiguiente, se debe hacer un análisis de costo/beneficio evaluando las consecuencias que pueda acarrear la pérdida de información y demás recursos informáticos, así como analizar los factores que afectan negativamente la productividad de la empresa.

BIBLIOGRAFIA

- *R.J. N° 340-94-INEI*[1], Normas Técnicas para el procesamiento y respaldo de la información que se procesa en entidades del Estado.
- *R.J. N° 076-95-INEI*, Recomendaciones Técnicas para la seguridad e integridad de la información que se procesa en la administración pública.
- *R.J. N° 090-95-INEI*, Recomendaciones Técnicas para la protección física de los equipos y medios de procesamiento de la información en la administración pública.
- *R.J. Nº 070-2007-J-CONIDA,* Comisión Nacional de Investigación y Desarrollo Aeroespacial – CONIDA.
- Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información. INEI.

- Manual de Operación y Funciones del Centro de Informática y Telecomunicaciones.
- Manual de Reglamento Interno del Centro de Informática y Telecomunicaciones.

[1] INEI, son las siglas del Instituto Nacional de Estadística e Informática

ANEXO I: ESTRUCTURA ORGANICA DEL CIT

Unidad	Función General
Telecomunicaciones	Mantener y Monitorear los Servicios red.
Soporte Tecnológico	Mantenimiento y Reparación de Computadoras y equipos tecnológicos.
Administración de Servidores	Velar por la integridad y buen funcionamiento de los Servidores.
Desarrollo Tecnológico	Desarrollar e implementar las necesidades de los usuarios en los Sistemas de Información.
Académica	Verificar y garantizar el correcto funcionamiento de los sistemas implementados.

ANEXO II: FORMATO PARA RELACION DE PROVEEDORES DE HARDWARE / SOFTWARE Y/O SERVICIOS

Razón Social	Dirección	Observación	Teléfono
		Hardware/ Software	

ANEXO III: FORMATO PARA EL REGISTRO DE BACKUPS

Anexo de Periodicidad para la Realización de Backup o Copias de Seguridad	**Código:**
	Versión:
	Fecha de actualización:
	Elaborado por:

Sistema de Información	**Tipo de Backup**	**Periodicidad del Backup**	**Medio de Almacenamiento**	**Lugar de Almacenamiento**	**Persona que lo genera**

ANEXO IV: MEDIDAS DE PRECAUCIÓN Y RECOMENDACIÓN [2]

1. En el Área de Servidores:

- Es recomendable que no esté ubicado en áreas de alto tráfico de personas o con un alto número de invitados.
- Evitar, en lo posible, los grandes ventanales por el riesgo de terrorismo y sabotaje; además de que permiten la entrada del sol y calor (inconvenientes para los equipos).
- En su construcción, no debe existir materiales altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no quedan perfectamente selladas y despidan polvo.
- Su acceso debe estar restringido al personal autorizado. El personal de la Institución deberá tener su carné de identificación siempre en un lugar visible.
- Establecer un medio de control de entrada y salida al *Área de Servidores*.
- Se recomienda que al personal, de preferencia, se les realice exámenes psicológicos y médico, y tener muy en cuenta sus antecedentes de trabajo, ya que el *Área de Servidores* depende en gran medida, de la integridad, estabilidad y lealtad del personal.
- El acceso a los Sistemas de Información, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.
- Establecer controles para una efectiva disuasión y detección, de intentos de acceso no autorizados a los sistemas de información.
- Se recomienda establecer políticas para la creación de los password y establecer periodicidad de cambios.
- Establecer políticas de autorizaciones de acceso físico al ambiente y de revisiones periódicas de dichas autorizaciones.
- Establecer políticas de control de entrada y salida del personal, en el caso de visitas, verificar los paquetes u objetos que portan.
- La seguridad de las terminales de un sistema en red podrán ser controlados por medio de anulación del disk drive, anulación de Compartir Discos duros, cubriéndose de esa manera la seguridad contra robos de la información y el acceso de virus informáticos.
- La ubicación de los controles de acceso (vigilancia) y el acceso en sí deben estar ubicados de tal manera que no sea fácil el ingreso de una persona extraña.
- Las cámaras fotográficas no se permitirán en el *Área de Servidores*, sin permiso por escrito de la Jefatura.

2. En la Administración de las Impresiones:

- Todo listado que especialmente contenga información confidencial, debe ser destruido, así como el papel carbón de los formatos de impresión especiales.
- Establecer controles de impresión, respetando prioridades de acuerdo a la cola de impresión.
- Establecer controles respecto a los procesos remotos de impresión.

[2] Referencia "Guía Practica para el Desarrollo de Planes de contingencia de Sistemas de Información". Instituto Nacional de Estadística e Informática (INEI).

3. En los Niveles de Control:

- Existen dos tipos de activos en un Centro de Cómputo (*Área de Servidores*): los equipos físicos y la información contenida en dichos equipos. Estos activos son susceptibles de robo, daño del equipo, revelación y/o destrucción no autorizada de la información, que interrumpen el soporte a los procesos del negocio.
- El valor de los activos a proteger, está determinado por el nivel de clasificación de la información y por el impacto en el negocio, causado por pérdida o destrucción del Equipo o información. Hay que distinguir los activos en nivel clasificado y no clasificado. Para los de nivel no clasificado, no será necesario control. Para el nivel clasificado, deben observarse todas las medidas de seguridad de la información que estos equipos contengan.

4. Recomendaciones para los Medios de Almacenamientos

- **Mantenimiento de Medios Magnéticos:**
  Deben guardarse bajo ciertas condiciones, con la finalidad de garantizar una adecuada conservación de la información almacenada. Medidas a considerar:
  - ⇒ La temperatura y humedad relativa del ambiente de almacenamiento, debe ser adecuada.
  - ⇒ Las cintas deben colocarse en estantes o armarios adecuados.
  - ⇒ Deberá mantenerse alejados de los campos magnéticos.
  - ⇒ Dar un mantenimiento preventivo en forma periódica a fin de desmagnetizar impurezas.

- **Recomendaciones para el Mantenimiento de los Discos Duros**
  - ⇒ Aunque el conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores.
  - ⇒ El ordenador debe colocarse en un lugar donde no pueda ser golpeado.
  - ⇒ Se debe evitar que la computadora se coloque en zonas donde haya acumulación de calor. Esta es una de las causas más frecuentes de las fallas de los discos duros.
  - ⇒ No se debe mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.

- **Respecto a los Monitores**
  - ⇒ La forma más fácil y común de reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día, es el uso de medidas contra la refección. Se recomienda no mirar directamente a la pantalla, si no mirar con una inclinación.
  - ⇒ Se recomienda sentarse por lo menos a 60 cm. (2 pies) de la pantalla. No sólo esto reducirá su exposición a las emisiones, sino que puede ayudar a reducir el esfuerzo visual.
  - ⇒ También manténgase por lo menos a 1 m. o 1.20 m. del monitor de su vecino, ya que la mayoría de los monitores producen más emisiones por detrás, que por delante.
  - ⇒ Finalmente apague su monitor cuando no lo esté usando

- **Recomendación para el cuidado del Equipo de Cómputo**
  - ⇒ Teclado: mantener fuera del teclado grapas y clips pues, de insertarse entre las teclas, puede causar un cruce de función.
  - ⇒ Cpu: mantener la parte posterior del cpu liberado en por lo menos 10 cm. Para asegurar así una ventilación mínima adecuada.
  - ⇒ Mouse: poner debajo del mouse una superficie plana y limpia.

- ⇒ Protectores de pantalla: para evitar la radiación de las pantallas que causan irritación a los ojos.
- ⇒ Impresora: el manejo de las impresoras, en su mayoría, es a través de los botones, tanto para avanzar como para retroceder el papel. Por Ejemplo:
  - Caso Epson FX-11xx/LQ-10xx no usar rodillo cuando esté prendido.
  - Caso Epson DFX-50xx/80xx tratar con cuidado los sujetadores de papel y no apagar de súbito, asegurarse que el ON LINE esté apagado, así evitaremos problemas de cabezal y sujetador.
  - Caso de mala impresión, luego de imprimir documentos o cuadros generados, apagar por unos segundos la impresora para que se pierda el set dejado.

- **Mantener las Áreas Operativas Limpias y Pulcra**

  Todas las razones para mantener las áreas operativas limpias y pulcras son numerosas. Sin embargo, algunos de los problemas que podemos evitar son: el peligro de fuego generado por la excesiva acumulación de papeles, el daño potencial al equipo por derramar líquidos en los componentes del sistema, el peligro por fumar y las falsas alarmas creadas por detectores de humo.

ANEXO V: SISTEMAS DE INFORMACION EN LA UNP, CRITICOS PARA LA CONTINUIDAD DEL NEGOCIO.

La relación de los sistemas de información deberá detallar los siguientes datos:

Nombre del sistema	Lenguaje de Programación / Sw Base de datos	Área que genera la información base	Áreas que usan la información	Tamaño promedio del archivo	Volumen de transacciones	Equipamiento necesario	Fechas en que la infor. se necesita urgente
Sistema Integrado de Administración Financiera (SIAF) Uso obligatorio en Instituciones públicas, por el MEF.		La Oficina Central de ejecución Presupuestaria.	OCEP, Oficina de Presupuesto			Conexión a Internet.	Diario
Sistema Integrado de Gestión Académico. Desarrollo CIT		Las Oficinas de Secretarias Académicas, OCRCA.	Las Oficinas Académicas, OCRCA, Autoridades Académicas-Administrativas-Control.		Proceso de Inscripción de cursos y Entrega de Actas.		Diario.
Sistema de Gestión Administrativa - Ingresos Desarrollo CIT		Todas las Unidades Operativas– Area Administrativa	Todas las Unidades Operativas – Of. Adminis., Autoridades Administrativas.		Descarga diario de los archivos del banco.		Diario
Sistema de Trámite Documentario Desarrollo CIT		Todas las Unidades Operativas – Tramite documentario	Todas las Unidades Operativas – Tramite documentario, Autoridades		Registro diario de los documentos.		Diario
Sistema de Abastecimientos. Desarrollo Externo		Oficina de Abastecimientos	Oficina de Abastecimientos		Registro diario de Ordenes de Trabajo.		Diario
Sistema de Control de Asistencia del personal Desarrollo CIT		Oficina de Recursos Humanos-Control de Asistencia	Oficina de Recursos Humanos-Control de Asistencia		Registro diario de las Asistencias de los trabajadores.		Diario
Sistema de Banco de Preguntas. Desarrollo CIT		Comisión de Exámenes de Idepunp	Comisión de Exámenes de Idepunp		Periodo de promedio cada cinco semanas		Exámenes Admisión

ANEXO VI: ESTADOS DE EMERGENCIA

Permiten identificar cuáles pueden ser los eventos que se pueden presentar que afecten el normal funcionamiento de la plataforma y afecte el ingreso de datos y la operación de los Sistemas de Información.

Evento	Descripción	Proceso alterno que debe realizar el usuario del sistema	Proceso alterno que debe realizar el personal de sistemas
Caída De Los Sistemas	Se produce cuando: Ninguna estación de trabajo funciona, el computador no ingresa a las aplicaciones o no hay comunicación con la red. Algunos de los elementos principales que impiden que la red funcione adecuadamente, pueden ser: Servidor, UPS del servidor, concentrador o swiches, puntos de red.	Mientras se restablece el sistema se debe realizar las operaciones de registro de manera manual. Solicitar soporte a la Coordinación Administrativa del CIT - UNP.	Informar del problema a la Coordinación Administrativa, para asignar al personal del soporte. Los mismos que identifican cual de los elementos no están funcionando y se procede a hacer el reemplazo.
Estación de trabajo no funciona	Se produce cuando: No hay energía en el toma, Cables de energía flojos o mal conectados, punto de red deteriorado, patchcord flojo en la conexión de equipo o la caja de punto de red, clave de acceso a la red bloqueada, problemas con el Hardware.	En la toma de energía no hay corriente eléctrica o el cable de energía esta flojo o mal conectado: Los usuarios deben verificar que estos elementos estén bien conectados, o utilizar otra estación de trabajo disponible. Solicitar soporte a la Coordinación Administrativa del CIT - UNP. Si los elementos del equipo están dañados: Solicitar soporte a la Coordinación Administrativa del CIT - UNP.	Verificar cada uno de los elementos que describen el problema y corregir el elemento en conflicto o reemplazarlo. La Coordinación Administrativa del CIT - UNP y de Soporte debe apoyar.
El programa o aplicación transaccional no ingresa al sistema	Se puede producir porque la conexión de red esta deshabilitada, borraron acceso directo o icono al programa, archivos de	Utilizar otra estación de trabajo para realizar sus tareas diarias, sino es posible realizarlas manualmente de acuerdo a las instrucciones dadas en caída de sistemas, reportar a la Coordinación Administrativa del CIT - UNP.	Verificar el caso mencionado y restaurar los elementos que están en conflicto. La Coordinación Administrativa del CIT - UNP y Desarrollo de

	configuración del programa fueron borrados, servidor fuera de servicio		Sistemas debe apoyar.
Pérdida de datos en el programa o aplicación transaccional	Ocurre cuando se pierden datos de registro diario del área operativa que ingresa a las aplicaciones transaccionales para realizar las operaciones.	Mientras se restablece el sistema se debe reportar a la Coordinación Administrativa del CIT – UNP.	Restauración de archivos del backup si se realizo entre las fechas indicadas. Revisar tabla de referencia de realización de backup y las políticas de seguridad de la información.
Errores de realizar: advertencia de los programas o aplicaciones transaccionales	Los mensajes de error de la aplicación expresan alguna anomalía dentro de los procesos normales que se realizan. Cada mensaje de error dentro de la aplicación emite un código con el que se puede identificar la causa, con el código del error que aparece en la pantalla, indica que puede estar pasando, es muy importante reconocer cual es el código del error y el mensaje completo para poder identificar y realizar el proceso de corrección de dicha falla.	Tomar nota del mensaje de error y comunicar a la Coordinación Administrativa del CIT – UNP, para que sea analizado y se establezca una posible solución. Mientras se restablece el sistema se debe realizar lo siguiente de acuerdo a la actividad que necesite realizar:	Se debe reportar al personal de Soporte de la Coordinación Administrativa del CIT – UNP y de Sistemas, sí el error persiste y no permite realizar o continuar con el proceso.

ANEXO VII: CONCEPTOS GENERALES

- **Privacidad**
  Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros.

- **Seguridad**
  Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.
  En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.
  El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

- **Integridad**
  Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

- **Datos**
  Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc.

- **Base de Datos**
  Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan. También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System - DBMS).
  Las características que presenta un DBMS son las siguientes:
  • Brinda seguridad e integridad a los datos.
  • Provee lenguajes de consulta (interactivo).
  • Provee una manera de introducir y editar datos en forma interactiva.
  • Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación.

- **Acceso**
  Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

- **Ataque**
  Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

- **Ataque Activo**
  Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

- **Ataque Pasivo**
  Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

- **Amenaza**
  Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

- **Incidente**
  Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

- **Golpe (Breach)**
  Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

ANEXO VIII: PROBABILIDAD DE QUE TENGA EFECTO ALGUNO DE LOS RIESGOS MENCIONADOS

PREGUNTA	RESPUESTA
Fallas eléctricas, que dañen los equipos	
¿La Institución cuenta con grupo electrógeno ?	No
¿Se cuenta con Planos Eléctricos de la distribución del cableado?	No
¿Esta falla cuánto daño puede ocasionar?	10%
El fuego que destruyen los equipos y los archivos	
¿La institución cuenta con protección contra incendios?	No
¿Se cuenta con sistema de aspersión automática?	No
¿Diversos Extintores?	Sí
¿Detectores de Humo?	No
¿Los empleados están preparados para un posible incendio?	No
Robo común, llevándose los equipos	
¿En que tipo de vecindario se encuentra la institución?	poco peligroso
¿Hay venta de drogas?	No
¿Las computadoras se ven desde la calle?	No
¿Hay personal de seguridad en la institución?	Si
¿Cuántos vigilantes hay?	2 por turno
Fallas en los equipos, que dañen los archivos	
¿Los equipos tienen mantenimiento continuo por parte de personal calificado?	Sí, según un plan de mantenimiento
¿Cuáles son las condiciones actuales de Hardware?	Bueno
¿Es posible predecir las fallas a que están expuestos los equipos?	Sí, es posible saberlo
Errores de los usuarios que dañen los archivos	
¿Cuánto saben los empleados de computadoras o redes?	Un nivel medio
Los que no conocen de manejo de computadoras, ¿Saben a quien pedir ayuda?	Si
Durante el tiempo de vacaciones de los empleados, ¿Qué tipo de personal los sustituye y que tanto saben del manejo de computadoras?	Con conocimientos similares
La acción de virus que dañen los archivos	
¿Se prueba software sin hacer un examen previo?	No
¿Esta permitido el uso de dispositvo de almacenamiento en la oficina?	Si
¿Todas las máquinas tienen dispositvo de almacenamiento?	Si
¿Se cuenta con procedimientos contra virus?	Si
Terremotos que destruyan los equipos y archivos	
¿La institución se encuentra en zona sísmica?	No
¿El local cumple con las normas antisísmicas?	Si

Un terremoto, ¿Cuánto daño podría causar?	75%
Accesos no autorizados, filtrando datos importantes	
¿Cuánta competencia hay para la institución?	
¿Qué probabilidad hay que un competidor intente hacer un acceso no autorizado?	
¿El módem se usa para llamar fuera y también se puede utilizar para comunicarse hacia dentro?	
¿Contamos con sistema de seguridad en el servidor?	
¿Contamos con seguridad en internet?	
Robo de Datos: difundiéndose los datos	
¿Cuánto valor tiene actualmente la Base de Datos?	Muy importante
¿Cuánta pérdida podría causar en caso de que se hicieran públicas?	
¿Se ha elaborado una lista de los posibles sospechosos que pudieran efectuar el robo?	
Fraude desviando fondos merced a la computadora.	
¿Cuántas personas se ocupan de la contabilidad de la institución?	
¿El sistema de contabilidad es confiable?	Si
Las personas que trabajan en el departamento de contabilidad ¿Qué tipo de antecedentes laborales tiene?	
¿Existe acceso al Sistema de Contabilidad desde otros sistemas o personas?	No, únicamente los encargados
¿Existen sistemas que manejen cuentas corrientes?	
¿Existen posibles manipulaciones en los archivos de cuentas corrientes?	
¿Existen algún sistema de seguridad para evitar manipulaciones en determinados archivos?	